



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at wvOASIS.gov. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at WVPurchasing.gov with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 2

List View

General Information | [Contact](#) | [Default Values](#) | [Discount](#) | [Document Information](#) | [Clarification Request](#)

Procurement Folder: 1369290

Procurement Type: Central Master Agreement

Vendor ID: VS0000003342

Legal Name: Securance LLC

Alias/DBA:

Total Bid: \$333,234.00

Response Date: 03/27/2024

Response Time: 16:06

Responded By User ID: securancelc

First Name: Paul

Last Name: Ashe

Email: supplydiv@securancecon

Phone: 877-578-0215

SO Doc Code: CRFQ

SO Dept: 0705

SO Doc ID: LOT2400000009

Published Date: 3/21/24

Close Date: 3/28/24

Close Time: 13:30

Status: Closed

Solicitation Description: Network Penetration Testing and Cybersecurity Assessments

Total of Header Attachments: 2

Total of All Attachments: 2



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder: 1369290
Solicitation Description: Network Penetration Testing and Cybersecurity Assessments
Proc Type: Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2024-03-28 13:30	SR 0705 ESR03272400000005463	1

VENDOR
VS0000003342
Securance LLC

Solicitation Number: CRFQ 0705 LOT2400000009
Total Bid: 333234
Response Date: 2024-03-27
Response Time: 16:06:21
Comments:

FOR INFORMATION CONTACT THE BUYER
Brandon L Barr
304-558-2652
brandon.l.barr@wv.gov

Vendor Signature X	FEIN#	DATE
---------------------------	--------------	-------------

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	External Network Penetration Testing				121176.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Website Penetration Testing				30294.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Internal/Client-Side Network Penetration Testing				131274.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Wireless Penetration Testing				50490.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

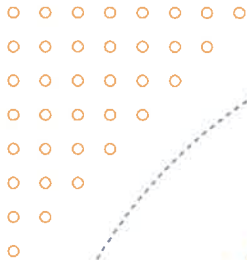
See Attached Specifications and Exhibit - A Pricing Page



MARCH 28, 2024

TECHNICAL PROPOSAL

RFQ #CRFQ 0705 LOT2400000009 NETWORK PENETRATION TESTING AND CYBERSECURITY ASSESSMENTS



Contact for RFP Response:
Patrick Swere
Proposal Manager
pswere@securanceconsulting.com
P: 877.578.0215 ext. 118
www.securanceconsulting.com

TABLE OF CONTENTS

1	REQUIREMENTS MATRIX
2	ABOUT SECURANCE
3	THE SECURANCE DIFFERENCE
4	WE UNDERSTAND GOVERNMENTS AND QUASI-GOVERNMENT AGENCIES
5	Case Studies and References
8	Similar Clients
9	PROJECT TEAM
10	Consultant Resumes — Key Personnel
21	APPROACH AND METHODOLOGIES
53	PROJECT MANAGEMENT
55	LOTTERY RESOURCES NEEDED TO COMPLETE THE PROJECT
59	REPORTING
62	REQUIRED FORMS
72	APPENDIX: SAMPLE REPORT

22+ YEARS

Securance has more than 22 years of experience providing cybersecurity services similar to those requested by the Lottery.

EXECUTIVE-LEVEL CONSULTANTS

Our executive-level consultants have provided comprehensive vulnerability assessments and penetration tests for more than 400 clients in multiple industries.

EXTRA VALUE

Few firms are as dedicated to their clients as Securance will be to you. We will invest the time and effort necessary to learn the Lottery's IT environment and organizational objectives. Then, we will use that understanding to identify vulnerabilities and help the Lottery implement effective security measures.

This proposal contains confidential material proprietary to Securance Consulting. The material, ideas, and concepts contained herein are to be used solely and exclusively to evaluate the capabilities of Securance Consulting to provide assistance to the State of West Virginia The Lottery (The Lottery). This proposal does not constitute an agreement between Securance Consulting and the Lottery. Any services Securance Consulting may provide to the Lottery will be governed by the terms of a separate written agreement signed by both parties. All offers to provide professional services are valid for sixty (60) days.



March 28, 2024

Brandon Barr, Buyer
Department of Administration, Purchasing Division
West Virginia The Lottery
2019 Washington Street East
Charleston, WV 25305-0130

Dear Brandon:

Thank you for considering Securance Consulting for the State of West Virginia Lottery's (The Lottery's) upcoming network penetration tests and cybersecurity assessments. As a full-service IT risk management firm with more than 22 years as an industry leader, we have the knowledge and experience to help the Lottery identify threats, remediate vulnerabilities, and implement effective security measures to protect its data and networks.

Email: jennifer.adkins@wv.gov
Hashed Password: \$2a\$08\$ywkph6cwEEZKVFerqCa
Sourced from dark web

Bad actors can strike at any moment, and the Lottery is already at risk. It took Securance less than a minute to find sensitive information about the Lottery on the dark web. In the wrong hands, this type of information could be the starting point of a cyber attack.

The Lottery needs a partner that can find security gaps like this and determine their impact. **Securance wants to be your partner.** We are committed to driving long-term improvements in your network security posture by:

- ▶ Performing the Lottery's engagement with methodologies enriched by the use of generative artificial intelligence (GenAI) and large language models (LLMs), as well as manual testing techniques.
- ▶ Providing value-added services at no cost to the Lottery, including:
 - External network vulnerability assessment and penetration testing.
 - Project management.
 - Status reporting.
 - The virtual findings presentations to the Lottery's management team.
 - Knowledge transfer sessions to appropriate staff.
- ▶ Leveraging the assigned team's years of experience performing network testing and cybersecurity assessments for clients in nearly every industry. Our proposed team of consultants, which I will lead, has a combined **80 years of cybersecurity experience**, and they are experts in providing the services the Lottery is requesting.

13916 Monroes Business Park, Suite 102 • Tampa, Florida 33635

877.578.0215

www.seuranceconsulting.com

Client	Project	Description	Performance Period
Oregon State Treasury (OST)	Information Technology Security Assessment	Conducted vulnerability assessments and penetration tests of OST's internal, external, and wireless networks.	April–June 2023
Peach State Bank & Trust (PSB&T)	Cybersecurity Assessment	Conducted vulnerability assessments and penetration tests of its internal and external networks, reviewed the configuration of its firewalls, and identified weaknesses in its user security awareness program.	February–April 2023
Texas Municipal Retirement System (TMRS)	Information Technology Security Assessment	Perform regular cybersecurity assessments and technical testing of external internal networks and web applications, firewall reviews, and social engineering campaigns.	Annually since 2017

We acknowledge that Securance may not be the lowest-priced bidder of the services required by the Lottery. However, our services represent a superior value when compared to those offered at a lower cost by our competitors. From the detailed nature of our assessment to the comprehensiveness of our deliverables and the in-depth knowledge transfer we will provide, The Lottery will not find a firm whose analyses and results are more accurate and exhaustive than ours. Discussions with our clients over the past 22 years have confirmed that our slightly higher upfront costs represent significant long-term savings.

Thank you for including Securance in your evaluation process. If you have any questions after reviewing our proposal, please do not hesitate to contact me.

Professional regards,

Paul Ashe, CPA, CISA, CISSP, CMMC-AB RP, HCISPP

President

We Want To Partner With You!

13916 Monroes Business Park, Suite 102 • Tampa, Florida 33635

877.578.0215

www.securanceconsulting.com

CONFIDENTIAL —

REQUIREMENTS MATRIX

Securance has formatted our proposal according to the The Lottery's requirements. Below, we summarize the contents of our proposal:

RFP Section	Requirement	Page No.
3.1	The vendor must have been in business for at least 15 years, performing and delivering information technology cybersecurity assessments. Vendor should provide with their bid a general company overview that must include information regarding the professional services offered and the number of dedicated security staff resources.	2
3.2	Vendor should provide, with their bid, a minimum of 3 references for projects of similar or greater size and scope of the assessments to be performed for the Lottery. References shall include contact information and brief details of the services performed for each reference.	4
3.3	Vendor should provide, with their bid, an overview of the project team and documentation of qualifications for each project team member assigned to the Lottery cybersecurity assessments. Documentation shall consist of information regarding the prior security assessments completed, resumes, and documentation of certifications.	9
3.4	Vendor staff performing information technology cybersecurity assessments must hold a current certification from a source of accreditation and should provide the certification credentials with their bid response. Allowable certifications include: CISSP, GPEN, OSCP, CEH, CPTE, CEPT, CRTOP, ECSA, CPPT, CWSF, CMWAPT.	13
3.5	Vendor must comply with the Center for Internet Security methodology and employ techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide.	21
3.6	Background Checks: Prior to award and upon request, the Vendor must provide names, addresses, and fingerprint information for a law enforcement background check for any Vendor staff working on the Lottery project team.	71
3.7	Prior to award both parties, the Vendor and The Lottery must sign a mutual Non-Disclosure Agreement (NDA), attached as Exhibit – B, to ensure the confidentiality of the information exposed and proprietary tools and techniques used during these assessments.	67
4.1	External network penetration testing requirements.	24
4.2	Website penetration testing requirements.	33
4.3	Internal client-side network penetration testing requirements.	24
4.4	Wireless penetration testing requirements.	36
5.2	Pricing page (included in separate cost proposal): Vendor should complete the Pricing Page by entering the unit cost per assessment and reports as a fixed amount for all penetration testing, vulnerability assessments, reports and findings presentation to calculate the extended amount. Then add all extended amount line items together to get the total bid amount. Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.	-

ABOUT SECURANCE

Two Decades of Network Penetration Testing and Cybersecurity Assessment Services

Securance is a 100-percent minority-owned limited liability company, certified as an 8(a), Small Disadvantaged Business (SDB), and Minority Business Enterprise (MBE). Since the firm was founded in March 2002, we have performed more than 2,500 cybersecurity assessments for clients in nearly every industry, including numerous government and financial agencies, helping them to align their cybersecurity postures with their cyber risk appetites.

Exclusively Staffed with Senior-Level IT Security Professionals

In order to provide the highest quality services, Securance only hires IT security consultants with more than 15 years of professional experience. Their expertise in a wide array of assessments, technical testing, and industry needs is our foundation, allowing us to perform each project we undertake to the unique specifications required by our clients' IT environments, security and control standards, and business requirements. **We are proposing three of Securance's most experienced security consultants for the The Lottery's engagement and maintain a dedicated staff of 39 W-2 consultants across the U.S.**

Securance's consultants excel in assessing and evaluating clients' IT infrastructures, identifying vulnerabilities, exploiting those vulnerabilities to gain privileged access, and developing actionable remediation recommendations. They are committed to clear and proactive communication and will work with all relevant Lottery departments and staff to achieve the project objectives.

THE SECURANCE DIFFERENCE

HANDS-ON
EXECUTIVE
LEADERSHIP ON
EVERY PROJECT

TECHNICAL RISK
TRANSLATED TO
BUSINESS RISK

Powered
by



THE SECURANCE DIFFERENCE

HANDS-ON EXECUTIVE LEADERSHIP ON EVERY PROJECT

A niche IT consulting firm, Securance was founded more than two decades ago by a group of executives from Big 4 accounting firms. Their vision was to provide highly specialized IT consulting services to clients in a wide range of industries, with unique advantages that only a small business could offer. Among these benefits are the caliber of our professional staff and the hands-on involvement of our executive team in client projects.

Larger firms use senior resources to lead their businesses, but often turn much of the fieldwork on client projects over to less experienced consultants. This is not the case with Securance.

Our professional staff is limited to senior IT consultants with at least 15 — and, often, 30 or more — years of experience.

Senior staff do not just lead our projects; they execute them

from cradle to grave. In addition, members of our executive team, including founder and president Paul Ashe and security lead Ray Resnick, work alongside our staff consultants on every project.

We have worked with hundreds of clients over the years and understand the disconnect that can occur when IT speaks one language and business another. An assessment report filled with technical jargon may be useful to a system administrator or engineer, but it provides little, if any, value to the C-suite.

Securance's reports are written in plain English that both technical and non-technical executives can understand. We explain the potential adverse effect of each finding on business operations. This approach extends the value of our analysis beyond the IT department, helping senior management understand the risks and making our recommendations truly actionable.

IT PROCESS RISK TRANSLATED TO BUSINESS RISK

Powered by



Securance is the *only* IT consulting firm that uses generative artificial intelligence (GenAI) and large language models (LLMs) to enhance its approach to assessing its clients' IT risk and security profiles. Our proprietary GenAI technology uses OpenAI's GPT-4 model, an LLM with 1 trillion parameters, to analyze large amounts of multimodal data, identify patterns and potential risks within a client's technology environment and IT processes, and, even, predict security breaches and failures. Armed with this insight, Securance tailors its assessment approach to fit each client's organization, address industry concerns, and target technology-specific threats.

WE UNDERSTAND GOVERNMENTS AND QUASI-GOVERNMENT AGENCIES

Government and quasi-government agencies, including the Lottery's systems, have complex requirements and needs when it comes to cybersecurity. The stakes are high, given the sensitive financial and personal data that needs to be protected. Consequences from a successful breach can include hefty fines, loss of critical data, and reputational damage. For this reason, the Lottery needs a cybersecurity partner who understands the evolving threats to its technologies, proven security measures to protect the types of systems and data it controls, and the risks that technical vulnerabilities present to its overall operations. Securance is that partner, and our experience and expertise proves this.

Our Experience at a Glance

- ▶ 22 years of experience serving government agencies and financial institutions.
- ▶ 400+ clients.
- ▶ 2,500+ cybersecurity projects completed.

We will bring specific value to the Lottery's project, including:

- ▶ A desire and ability to learn the Lottery's unique environment and customize our approach accordingly.
- ▶ Cybersecurity assessments that leverage AI to enhance technical testing and produce more accurate results.
- ▶ An awareness of specific issues facing agencies like the Lottery, such as the:
 - Need to thoroughly test new hardware and software installed by third-party vendors, such as International Game Technology.
 - Potential for exploiting software weaknesses to hack the Lottery terminals and manipulate the results.
- ▶ Efficient project execution with clear and actionable remediation recommendations.

WE UNDERSTAND GOVERNMENTS

Case Studies and References



CLIENT NAME: Oregon State Treasury (OST)

SECURANCE TEAM: Paul Ashe, Chris Bunn, Ray Resnick

PROJECT DURATION AND TIMEFRAME: Seven Weeks, 2023

PROJECT OUTCOME

Identified multiple critical vulnerabilities in OST's internal network security and provided detailed remediation instructions.

Documented opportunities to improve physical security of OST's facilities.

REFERENCE CONTACT

Josh Woodmansee
Procurement | Contract
Specialist

Josh.Woodmansee@ost.state.or.us
503.378.6785

CYBERSECURITY ASSESSMENT

CLIENT OBJECTIVES

OST sought a vendor to conduct a cybersecurity assessment that included:

- ▶ Reviewing IT governance against best practices.
- ▶ Evaluating the security of its web applications.
- ▶ Performing vulnerability scans of its internal and external networks.
- ▶ Conducting social engineering testing.

SECURANCE SOLUTION

The Securance team:

- ▶ Conducted vulnerability assessments and penetration tests of OST's internal, external, and wireless networks.
- ▶ Performed social engineering exercises, including email phishing, vishing, and physical security reviews of two locations.
- ▶ Tested the security of 10 web applications.
- ▶ Prioritized remediation recommendations based on severity and risk of each vulnerability.



WE UNDERSTAND GOVERNMENTS

Case Studies and References



CLIENT NAME: Peach State Bank and Trust (PSB&T)

SECURANCE TEAM: Paul Ashe, Ray Resnick, Jerry Bruggeman

PROJECT DURATION AND TIMEFRAME: Three Months, 2023

PROJECT OUTCOME	CYBERSECURITY ASSESSMENT
<p>Prioritized vulnerabilities by level of severity.</p> <p>Provided actionable recommendations to mitigate risks.</p> <p>Evaluated the effectiveness of PSB&T's end-user security awareness training.</p> <p>Identified opportunities to improve and streamline PSB&T's firewall configuration.</p>	<p>CLIENT OBJECTIVES</p> <p>PSB&T sought a vendor to:</p> <ul style="list-style-type: none">▶ Conduct vulnerability assessments and penetration tests of its internal and external networks.▶ Review the configuration of its firewalls.▶ Identify weaknesses in its user security awareness program. <p>SECURANCE SOLUTION</p> <p>The Securance team:</p> <ul style="list-style-type: none">▶ Scanned PSB&T's internal and external networks and identified critical, high, and medium-priority vulnerabilities.▶ Performed a detailed configuration analysis of PSB&T's firewalls.▶ Designed an email phishing campaign to test the effectiveness of PSB&T's internal user security awareness training.
<p>REFERENCE CONTACT</p> <p>Steve Pettit Senior Vice President</p> <p>Spettit@peachstatebank.com 770.531.2755</p>	

WE UNDERSTAND GOVERNMENTS

Case Studies and References



CLIENT NAME: Texas Municipal Retirement System (TMRS)

SECURANCE TEAM: Paul Ashe, Ray Resnick

PROJECT DURATION AND TIMEFRAME: Securance has performed cybersecurity reviews and quarterly vulnerability assessments for TMRS since 2017.

PROJECT OUTCOMES

Improved end-user security awareness by 70 percent.

Supported TMRS staff in the remediation of identified vulnerabilities.

Reduced technical threats in TMRS's IT environment by over 50 percent.

Provided detailed technical reports that included customized recommendations.

REFERENCE CONTACT

Gordon James
Manager Information Security

Gjames@tmrs.com
512.225.3861

INFORMATION TECHNOLOGY SECURITY ASSESSMENT

CLIENT OBJECTIVES

TMRS sought a vendor to:

- ▶ Conduct an assessment of its network architecture.
- ▶ Assess its security controls designed to protect endpoints against cyber attacks.
- ▶ Perform regular vulnerability scans and penetration testing of its internal and external networks.
- ▶ Conduct social engineering testing, including email phishing and phone pretexting.
- ▶ Perform penetration testing of web applications.
- ▶ Review firewall configurations.

SECURANCE SOLUTION

The Securance team:

- ▶ Tested endpoint security and ransomware preparedness.
- ▶ Analyzed firewall configurations, including the intrusion prevention system modules.
- ▶ Conducted external and internal network penetration tests and quarterly external network vulnerability assessments.
- ▶ Performed detailed security assessments of Internet-facing web applications and the web application firewall (WAF).
- ▶ Tested user security awareness via email phishing and other social engineering activities.
- ▶ Assessed workstation security controls.

WE UNDERSTAND GOVERNMENTS

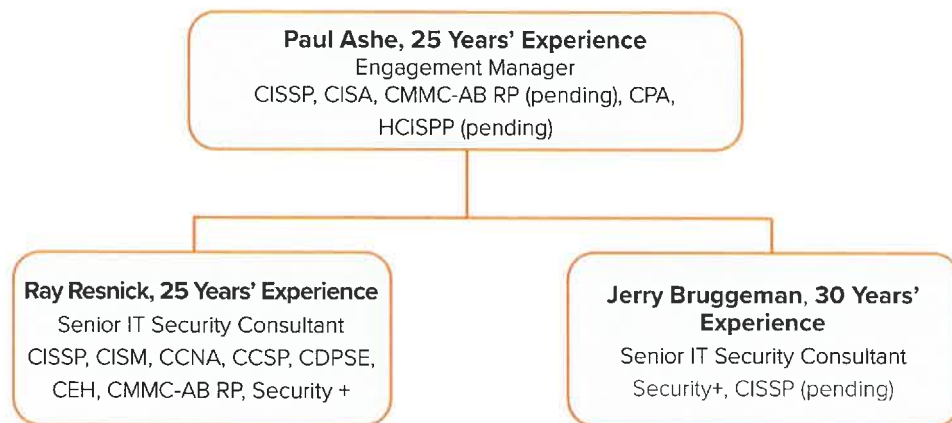
Similar Clients

Below is a sample list of clients with whom we have worked with scopes of work and requirements similar to the Lottery's.



PROJECT TEAM

The expertise and experience of the consultants listed on the following pages align with the Lottery's scope of work and RFQ requirements. If any of these consultants is unavailable when the project starts, Securance will propose an equally experienced substitute for approval. Securance only employs senior-level consultants; no junior-level consultants will be assigned to the Lottery's project.



PROJECT TEAM

Consultant Resumes — Key Personnel

PAUL ASHE

25 YEARS OF CYBERSECURITY EXPERIENCE

President and Engagement Manager | Securance Consulting



EDUCATION

Master of Science

Accounting Information Systems

Bachelor of Science

Accounting and Management
Information Systems

PROFESSIONAL CREDENTIALS

- ▶ Certified Public Accountant (CPA)
- ▶ Certified Information Systems Security Professional (CISSP)
- ▶ Certified Information Systems Auditor (CISA)
- ▶ Healthcare Information Security and Privacy Practitioner (HCISPP)
- ▶ Cybersecurity Maturity Model Certification Registered Practitioner (CMMC RP)

Paul has provided hands-on project management to lead Securance engagements over the past 22 years. A former IT consultant for Ernst & Young, he translates his knowledge and experience into an effective, time- and budget-conscious project management style. Paul conducts cybersecurity assessments, penetration tests, and social engineering for clients in every industry. He is an expert in configuring security devices and tools to safeguard critical IT assets.

RELEVANT EXPERIENCE

- ▶ Web application testing
- ▶ External vulnerability assessments and penetration tests
- ▶ Internal vulnerability assessments and penetration tests
- ▶ Wireless network security assessments
- ▶ Social engineering campaigns
- ▶ Project management
- ▶ Automated and manual testing techniques
- ▶ Advanced penetration testing
- ▶ Firewall, router, and switch configuration reviews
- ▶ Virtual private network (VPN) testing

RELEVANT EXPERTISE

- ▶ **Project Management:** Paul has led Securance engagements from kick-off to final report for 22 years.
- ▶ **Virtual Chief Information Security Officer (vCISO):** Collaborating closely with an organization's chief information officer, Paul develops and implements cybersecurity strategies and initiatives to manage risks, deter breaches, and meet compliance obligations.
- ▶ **Cyber Resilience:** Paul helps organizations identify threats, risks, and vulnerabilities, and establish full-scale cyber resilience programs to harden their security postures.
- ▶ **Cybersecurity Assessments:** Paul helps clients identify threats, strengthen security, and develop reports that allow organizations to gain insight into their current security posture and remediate vulnerabilities.

PROJECT TEAM

Consultant Resumes — Key Personnel

RELEVANT ACHIEVEMENTS

- ▶ **City of St. Charles** Improved logging and monitoring, change management, patch management, and disaster recovery processes and reduced network and database vulnerabilities by 60 percent.
- ▶ **City of Durham** Reduced urgent, critical, and high risk vulnerabilities associated with the internal network, enterprise application, and database environment by 50 percent; managed the recovery process after the City suffered a major ransomware attack; currently serves as the City's vCISO; oversees the cybersecurity program and security operations center (SOC); and achieved a 100-percent reduction in cybersecurity breaches and incidents.
- ▶ **City of Gilroy** Streamlined the City's IT operations by improving governance documentation and implementing a cyber resilience plan, which facilitated a sustainable reduction in vulnerabilities.
- ▶ **City of Modesto** Improved governance documentation and reduced key person risk.
- ▶ **City of New Haven** Identified vulnerabilities and opportunities to improve policies, procedures, and security configurations; provided extensive remediation support to address identified vulnerabilities, including incident response tabletop exercises and plans to train IT staff and standard users in security awareness; developed a three-year plan to implement all new security program items.
- ▶ **City of Pasadena** Reviewed IT operations and processes against the NIST CSF and provided a roadmap to improve the City's security and control posture.
- ▶ **City of Phoenix** In addition to identifying and help remediate vulnerabilities in the City's networks, servers, databases, firewalls, and routers, secured funding for a 24 | 7 | 365 SOC.
- ▶ **City of Richmond** Facilitated a significant reduction in technical risks across the internal network following remediation.
- ▶ **Riverside University Health System** Reduced vulnerabilities within the internal network, web application, operating system, and databases and developed a remediation plan that prioritized risks, estimated costs, timelines, and resources needed to attain full HIPAA compliance.
- ▶ **State of Wyoming** Identified critical-, high-, and medium-risk vulnerabilities to decrease technical threats in the IT environment and improved IT governance to decrease future vulnerabilities.
- ▶ **Texas Municipal Retirement System** Improved end user security awareness by 70 percent and reduced technical risk across the environment by more than 50 percent.
- ▶ **Village of Niles** Spearheaded development of policies, procedures, cross-training, and a technology steering committee and reduced key person risk by matching staff to appropriate tasks.
- ▶ **Village of Orland Park** Mapped assessment findings to CJIS requirements and NIST CSF controls; then streamlined IT operations by improving the Village's governance documentation.
- ▶ **Washington State Investment Board** Reduced key person risk by 90 percent and reduced financial exposure from non-compliance with the Washington State Office of the CIO's standards.



PROJECT TEAM

Paul Ashe CISSP Certification

International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

Paul Ashe

the credential of

Certified Information Systems Security Professional

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.



Zachary Tudor - Chairperson



Yiannis Pavlosogiou - Secretary



[Redacted]

Certification Number

Aug 1, 2021 - Aug 31, 2024

Certification Cycle

Certified Since 2015

1952

(ISC)²



PROJECT TEAM

Consultant Resumes — Key Personnel

RAY RESNICK

25 YEARS OF CYBERSECURITY EXPERIENCE

Senior IT Security Consultant | Securance Consulting



EDUCATION

Bachelor of Science

Accounting

PROFESSIONAL CREDENTIALS

- ▶ Certified Information Security Manager (CISM)
- ▶ Certified Information Systems Security Professional (CISSP)
- ▶ Certified Cloud Security Professional (CCSP)
- ▶ Certified Data Privacy Solutions Engineer (CDPSE)
- ▶ Certified Ethical Hacker (CEH)
- ▶ Cisco Certified Network Associate (CCNA)
- ▶ CompTIA Security + Certified
- ▶ Cybersecurity Maturity Model Certification Registered Practitioner (CMMC RP)

Ray, a retired Commander and Special Operations Officer for the U.S. Navy, specializes in analyzing organizational security needs, assessing existing security posture, and implementing plans to mitigate risks to an acceptable level. Ray has the ability to work with IT staff at all levels to address risks, vulnerabilities, and gaps that hamper security in the IT environment.

RELEVANT EXPERIENCE

- ▶ Advanced persistent threat simulation testing
- ▶ Enterprise and web application security
- ▶ Firewall, router, and switch configuration reviews
- ▶ Information security awareness training
- ▶ Internal | external | wireless network security
- ▶ Vulnerability assessment and penetration testing
- ▶ Web application testing
- ▶ Social engineering campaigns
- ▶ Project management
- ▶ Automated and manual testing techniques
- ▶ VPN testing

RELEVANT EXPERTISE

- ▶ **Advanced Persistent Threat Simulation Testing (APT):** Ray is an expert in simulating realistic APT scenarios, gaining increased access through exfiltration, privilege escalation, evasion, and persistence.
- ▶ **Cybersecurity Assessments:** Ray helps clients identify threats, strengthen security, and develop reports that allow organizations to gain insight into their current security posture and remediate vulnerabilities.
- ▶ **Advanced Penetration Testing:** Ray is an experienced ethical hacker, skilled in advanced penetration testing techniques and performing configuration reviews of firewalls and other critical technologies to help organizations protect against potential threats.
- ▶ **Ransomware Readiness:** Ray has extensive experience training staff in ransomware readiness and helping organizations prepare to respond to breaches quickly and efficiently, minimizing mean time to recovery.

PROJECT TEAM

Consultant Resumes — Key Personnel

RELEVANT ACHIEVEMENTS

- ▶ **City of Durham** Reduced urgent, critical, and high risk vulnerabilities associated with the internal network, enterprise application, and database environment by 50 percent; managed the recovery process after the City suffered a major ransomware attack; serves as backup vCISO to Paul Ashe for the City; helps oversee the cybersecurity program and security operations center (SOC); and achieved a 100-percent reduction in cybersecurity breaches and incidents.
- ▶ **City of Kenai** Improved operating effectiveness of critical IT processes.
- ▶ **City of Modesto** Improved governance documentation and reduced key person risk.
- ▶ **City of New Haven** Identified vulnerabilities and opportunities to improve policies, procedures, and security configurations; provided extensive remediation support to address identified vulnerabilities, including incident response tabletop exercises and plans to train IT staff and standard users in security awareness; developed a three-year plan to implement all new security program items.
- ▶ **City of Phoenix** In addition to identifying and assisting to remediate vulnerabilities in the City's networks, servers, databases, firewalls, and routers, secured funding for a 24 | 7 | 365 SOC.
- ▶ **City of Richmond** Facilitated a significant reduction in technical risks across the internal network following remediation.
- ▶ **Emergence Health Network** Improved the organization's cybersecurity posture by recommending several improvements, including implementation of a disaster recovery plan and a change management process.
- ▶ **North Dakota Public Employee Retirement System** Identified medium-risk vulnerabilities and offered actionable remediation recommendations and recommended the implementation of a program management policy to solidify program change policies.
- ▶ **Riverside University Health System** Reduced vulnerabilities within the internal network, web application, operating system, and databases and developed a management plan that prioritized risks, estimated costs, timelines, and resources needed for to attain full HIPAA compliance.
- ▶ **Texas Municipal Retirement System** Improved end user security awareness by 70 percent and reduced technical risk across the environment by more than 50 percent.
- ▶ **Village of Orland Park** Mapped assessment findings to CJIS requirements and NIST CSF controls; streamlined IT operations by improving the Village's governance documentation.
- ▶ **Washington State Investment Board** Reduced key person risk by 90 percent and reduced financial exposure from non-compliance with Washington State Office of the CIO's standards.

PROJECT TEAM

Consultant Resumes — Key Personnel

PRIOR ACHIEVEMENTS

- ▶ **Copper Collar Enterprises, LLC** | 2012–2018 | Information Security Engineer | Conducted vulnerability scanning, attack and penetration studies, analyzed information and physical security vulnerability assessments; analyzed data security controls to identify weaknesses; designed remediation strategies.
- ▶ **Verizon Communications** | 1998–2003 | Database Administrator | Performed database installs, loads, and data conversions. Tuned and altered databases and tables to increase performance. Prepared custom database reports with SQL and shell scripts. Wrote stored procedures, triggers, and database views to increase efficiency and security. Scheduled and performed database back-ups. Troubleshoot application code for SQL errors and potential SQL injection vulnerabilities.
- ▶ **Verizon Communications** | 1998–2003 | Senior Systems Engineer | Developed automated tools to improve system reliability and disk and CPU utilization; planned, coordinated, and performed application testing, installation, and patch management; responsible for installing, managing, and administering servers, providing training and technical support to end users, and maintaining system documentation.
- ▶ **United States Navy Reserve** | 2002–2003 | Commander | Served as Executive Officer, Operations Department Head (N3), Inspector General, Information Technology and Physical Security Department Head (N6), and Intelligence Department Head (N2); responded to crisis management situations in the United States Central Command Area of Responsibility (USCENTCOM AOR). Supervised Crisis Action Team (CAT cell), Joint Personnel Adjudication System (JPAS), and internal badging systems for U.S. Naval Forces Central Command (NAVCENT); prepared and delivered briefings to Flag Level officers regarding political, military, security, and terrorism matters.
- ▶ **United States Navy** | 1991–2007 | Deputy Assistant Chief of Staff Naval Liaison Officer | Performed high-level negotiations with senior governmental officials and military officers from 53 coalition nations; responsible for operational planning efforts of U.S. and coalition maritime assets during wartime environment.

PROJECT TEAM

Ray Resnick CISSP Certification



PROJECT TEAM

Ray Resnick CEH Certification



PROJECT TEAM

Consultant Resumes — Key Personnel

JERRY BRUGGEMAN

30 YEARS OF CYBERSECURITY EXPERIENCE

Senior IT Security Consultant | Securance Consulting



EDUCATION

Bachelor of Science

Cybersecurity

PROFESSIONAL CREDENTIALS

- ▶ CompTIA Security + Certified
- ▶ Certified Information Systems Security Professional (CISSP) pending

Jerry is a versatile cybersecurity expert with a strong background in risk management, networking, IT administration and IT security. He has helped create and maintain robust information security programs for large organizations in both the private and public sectors, including the U.S. military. Jerry has significant experience developing conducting network penetration tests and cybersecurity assessments.

RELEVANT EXPERIENCE

- ▶ Advanced persistent threat simulation testing
- ▶ Cybersecurity assessments
- ▶ Cybersecurity program development
- ▶ Enterprise and web application security
- ▶ Firewall reviews
- ▶ Router | switch configuration reviews
- ▶ Information security awareness training
- ▶ Network assessments, e.g., internal | external | wireless
- ▶ Vulnerability assessment and penetration testing

RELEVANT EXPERTISE

- ▶ **Advanced Penetration Testing:** Jerry is an ethical hacker with a passion for penetration testing, cyber security, and information security. His exceptional ability to think like a hacker and probe for security vulnerabilities helps organizations enhance their security postures and protect against potential threats.
- ▶ **Advanced Persistent Threat (APT) Simulation Testing:** Jerry is an expert in simulating APT attacks that use exfiltration, privilege escalation, evasion, and persistence to move laterally and access increasingly sensitive information.
- ▶ **Network Security** Jerry excels at identifying and exploiting vulnerabilities in networks, routers, switches, and firewalls and providing actionable remediation recommendations to address each vulnerability



PROJECT TEAM

Consultant Resumes — Key Personnel

RELEVANT ACHIEVEMENTS WITH SECURANCE

- ▶ **Emergence Health Network** Improved the organization's cybersecurity posture by recommending several improvements, including implementation of a disaster recovery plan and a change management process.
- ▶ **Riverside University Health System** Reduced vulnerabilities within the internal network, web applications, operating systems, and databases; developed a remediation plan that prioritized risks, estimated costs, timelines, and resources needed to attain full HIPAA compliance.
- ▶ **Village of Oak Park** Improved the Village's cybersecurity posture by reducing technical risks associated with vulnerabilities in the internal and external networks and provided actionable remediation recommendations to reduce compliance risks within the environment.
- ▶ **Village of Schaumburg** Identified urgent-, high-, and medium-risk vulnerabilities to decrease technical threats in the Village's IT environment.

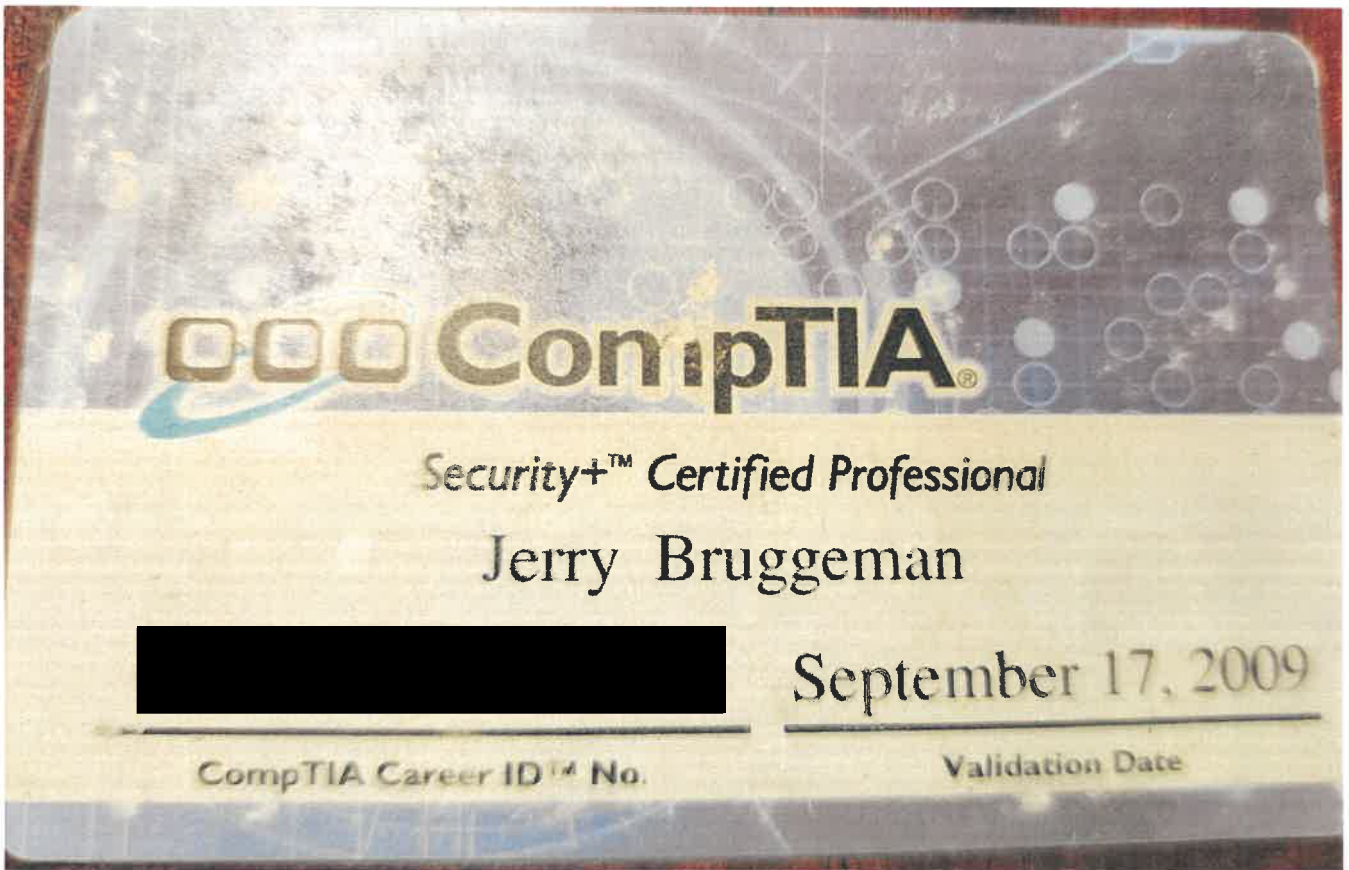
PRIOR ACHIEVEMENTS

- ▶ **Healthplan Services (WIPRO)** | 2020–2023 | Director of Information Security | Provided subject matter expertise in risk assessment, compliance, and technical security.
- ▶ **VASTEC** | 2013–2020 | Director of Information Security | Spearheaded IT security program, developed disaster recovery and incident response plans, conducted IT risk assessments, performed and analyzed vulnerability scans, and administered virtual environments.
- ▶ **U.S. Air Force, 52d Combat Communications Squadron** | 2010–2013 | Chief of Cyber Systems Operations | Managed a 120-person team across five work centers, conducted vulnerability and risk assessments, tracked and reported KPIs, and developed and deployed tactical networks.
- ▶ **U.S. Air Force, 14th Weather Squadron** | 2005–2010 | Manager, Information Assurance | Managed unit network security programs and assessments; conducted vulnerability and risk assessments.
- ▶ **U.S. Air Force Weather Agency** | 2002–2005 | Lead Infrastructure /Information Assurance Technician | Led and trained team responsible for administering and managing the weather network.

PROJECT TEAM

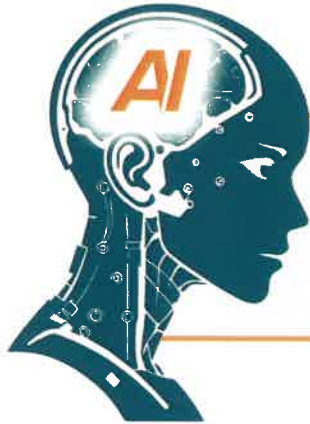
Jerry Bruggeman CISSP Certification

Jerry's CISSP certification is currently pending. He will have his official certification by July 2024. Below is Jerry's current certification for CompTIA Security+.



APPROACH AND METHODOLOGIES

Cybersecurity Powered by AI



Securance is **the first and only cybersecurity firm** to use generative AI (GenAI) and large language models (LLMs) to enhance its approach to client-focused assessments.

GenAI and LLMs can transform the ways in which businesses across industries gather and analyze information, predict outcomes, and make better decisions. Cybersecurity is no exception. At Securance, we use LLMs to identify potential risks based on a client's technologies, IT processes, and industry. We apply this information to focus our approach and methodologies when conducting cybersecurity assessments.



LLMs consider billions of parameters and ingest massive amounts of data from sources such as the Internet, Common Crawl, which collects data from more than 50 billion web pages, and Wikipedia, with approximately 57 million pages. While not perfect, LLMs have a remarkable ability to make predictions based on a relatively small number of prompts, or inputs. GenAI uses LLMs to produce content based on human-language prompts that provide clarity and context.

APPROACH AND METHODOLOGIES

Cybersecurity Powered by AI

Securance's program leverages OpenAI's GPT-4 model. With 1 trillion parameters, GPT-4 can identify patterns from multimodal data, generate natural and readable output, and perform complex tasks. We use GPT-4 to deliver maximal value to our clients via customized methodologies, targeted assessments, and actionable recommendations to prevent security breaches. During an initial co-development and planning session, we gather information about the client, its technology environment, and its IT organization.

We use this data to adjust our input prompts, which include:

- ▶ The organization's industry.
- ▶ The organization's size.
- ▶ The security framework(s) in place.
- ▶ The security tools in place.
- ▶ Whether the organization has a security operations center (SOC) monitoring its network.

Securance does not include confidential, proprietary, or sensitive data from our clients in our prompts.

Based on the input prompts, our LLMs and GenAI produce information that informs our assessment approach. Securance's model can even predict cyber breaches, events, and failures and their consequences. Predictions may include the potential for:

- ▶ Failures in IT process controls.
- ▶ Network, system, and/or application breaches based on the client's cybersecurity profile.
- ▶ End-user security failures and phishing attacks.
- ▶ Inappropriate access to data or systems by end users.

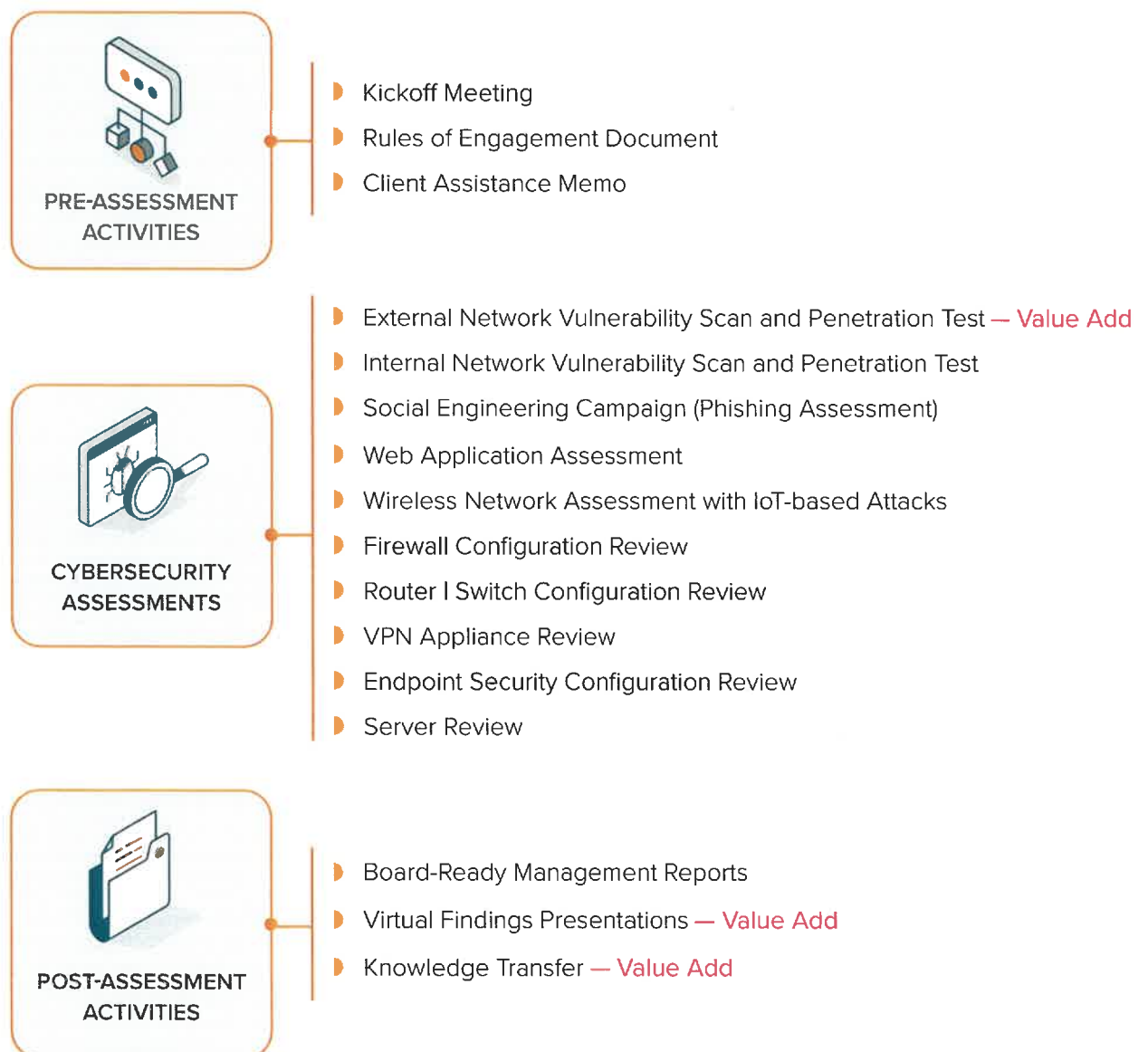
Harnessing the power of GenAI, Securance provides clients with accurate results, tailored recommendations, and unique advantages that other security firms cannot match. The benefits of a Securance assessment include:

- ▶ Comprehensive security profile.
- ▶ Predictive risk analysis, including industry- and technology-specific risks.
- ▶ Recommendations to prevent costly network and system breaches.

APPROACH AND METHODOLOGIES

Scope of Work

Below, we summarize our understanding of the Lottery's expectations for this project and the deliverables. We have included methodologies for the assessment tasks on the following pages. Securance's methodologies align with the Center for Internet Security (CIS) Controls and configuration standards, the Open Web Application Security Project (OWASP) Top 10, and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115, Information Security Testing and Assessment.





APPROACH AND METHODOLOGIES

Internal | External Network Vulnerability Assessment and Advanced Penetration Test

Vulnerability assessments and penetration tests are fundamental to an organization’s security against internal and external cyber threats. With over 22 years of experiencing conducting these assessments for clients in every industry, Securance understands how to maximize the value and efficiency of every step in the testing process. Our team will consider the Lottery’s unique digital landscape and adjust our practices to meet the Lottery’s needs, including which method of testing best aligns with the Lottery’s security objectives:



- ▶ **Black Box:** The Lottery does not provide Securance any internal knowledge of the target system that is not publicly available.
- ▶ **Gray Box:** The Lottery provides Securance some knowledge of the network’s internals, which may include design and architecture documentation and an account internal to the network.
- ▶ **White Box:** The Lottery provides Securance all information about target network.

Securance will utilize a combination of industry-leading techniques during this engagement, including the National Institute of Standards and Technology (NIST) Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment), Information Systems Security Assessment Framework (ISSAF), Open-Source Security Testing Methodology Manual (OSSTMM), Open Worldwide Application Security Project (OWASP), and Penetration Testing Execution Standard (PTES).



- ▶ **Plan the Assessment**
- ▶ **Information Gathering**
- ▶ **Vulnerability Assessment**
- ▶ **Advanced Penetration Testing**
- ▶ **Identify and Remove False Positives**

PLAN THE ASSESSMENT

- ▶ Identify client resources.
- ▶ Develop rules of engagement.
 - Securance will work closely with the Lottery to confirm and agree upon clear rules of engagement for the Lottery’s project, including Securance’s authorization to perform certain items:

<ul style="list-style-type: none"> • Project Scope of Effort. • Tool Configuration. • The Lottery’s IT Environment Uniqueness. • Privileged Testing Authority. • VoIP Solution Scan. • 3rd Party Hosted IP Scans. • How to handle Scope 	<ul style="list-style-type: none"> Creep. • The Lottery Lab’s IP Address. • Approved Dates, Times, and Tools. • Interest in Whitelisting Lab’s IP. • Communication Ground Rules. 	<ul style="list-style-type: none"> • Escalation Plan. • The Lottery and Securance Contact Information. • Lottery’s Specific Concerns.
--	---	--

APPROACH AND METHODOLOGIES

Internal | External Network Vulnerability Assessment and Advanced Penetration Test (cont.)

- ▶ Develop specific scope that addresses which systems (if any) should not be assessed.

INFORMATION GATHERING

External Assessment

- ▶ Search for public information about the Lottery's Internet presence using the American Registry for Internet Numbers (ARIN), social media, the surface web, and the dark web.
- ▶ Identify weaknesses in the registration process, like publishing internal staff contact information.

Internal Assessment

- ▶ Connect to a "hot" port on the internal network, if applicable for selected testing method.
- ▶ Obtain internal IP information about approved targets.
- ▶ In stealth mode, perform a port sweep to develop a map of the internal network structure.
- ▶ Attempt to identify servers, applications, network infrastructure devices, database systems, web applications, and other technologies based on ports and services.
- ▶ Assess fingerprint information.
- ▶ Review information with the The Lottery's PM.

VULNERABILITY ASSESSMENT

- ▶ Analyze information gathered in previous section.
- ▶ Our testing techniques scale from soft to aggressive. Below are examples of soft and aggressive techniques we will utilize:

Soft Techniques

- Passive port scanning to identify open ports and listening services.
- Default password identification.
- "Safe check" vulnerability scanning.
- Software version identification.
- Firmware version identification.
- Multiple-tool scanning.

Aggressive Techniques

- Multi-location network sniffing.
 - Applying a denial of service attack.
 - Aggressive vulnerability scanning.
- ▶ Identify modes of access.
 - ▶ Locate trusted hosts.
 - ▶ Identify sensitive data flows.



APPROACH AND METHODOLOGIES

Internal | External Network Vulnerability Assessment and Advanced Penetration Test (cont.)

- ▶ Perform vulnerability scans using various tools and cross-reference available services against a comprehensive listing of vulnerability databases.
- ▶ The Securance vulnerability assessment and penetration test performs a series of checks to discover methods to breach your systems. Here is a summary list of checks we include in our methodology:

- Buffer Overflows
- Hard Coded Secrets
- Router Vulnerability Detection
- Bypass Authentication
- HTML Source Code Analysis
- Look for Sensitive Error Messages
- Case Studies and Presentations Info
- Integer Overflows
- Server | Service Fingerprinting
- Cross Site Tracing
- Open Relay Scan
- SSL Configuration
- Database Scan
- OS Fingerprinting
- Trade Publications Info
- Default Passwords
- Password Cracking and Guessing
- Command Injection
- Job Postings Info
- Session ID Prediction
- Cross Site Request Forgery
- LDAP Injection
- SNMP Scan
- Cross Site Scripting
- Mailing Lists Info
- SQL Injection
- Validate Cryptographic Strength
- Directory Traversal
- Ping Sweep
- Vulnerable Sample Applications
- DNS Records Info
- Port Scanning
- Web Server Vulnerability Scan
- Fire Walking

ADVANCED PENETRATION TESTING

- ▶ Develop penetration testing rules of engagement.
- ▶ Determine the approved target systems for penetration testing.
- ▶ Utilize information gathered, including user names and passwords.
- ▶ Perform exploit testing.
- ▶ Collect and clean up evidence of exploitation.

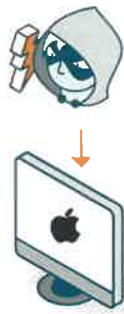
Our advanced penetration methodology makes use of automated tools, such as Core Impact, Metasploit, and Canvas, to exploit common security vulnerabilities throughout an organization. We leverage tools like Cobalt Strike to perform lateral testing, gain control of other systems on the network, and attempt to exfiltrate sensitive data. In addition to automated testing, Securance will also perform manual penetration testing to find weaknesses missed by the automated tools.

APPROACH AND METHODOLOGIES

Internal | External Network Vulnerability Assessment and Advanced Penetration Test (cont.)

Our manual testing techniques include:

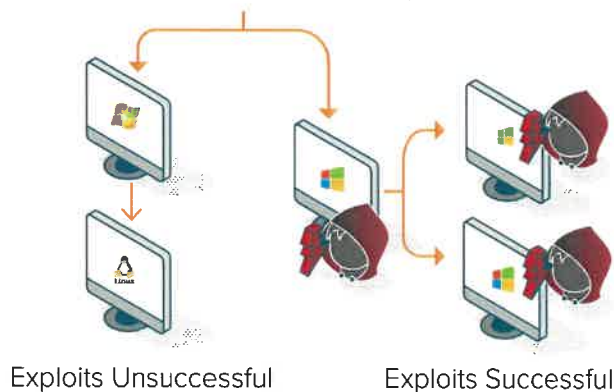
- ▶ Modification of scripts used in automated tools.
- ▶ Threat hunting on compromised hosts.
- ▶ Use of manual scripts available in the wild.
- ▶ Installation of security tools on compromised hosts.
- ▶ Keyboard entry on compromised hosts.
- ▶ Exploit of risk found based on newly installed security tools on compromised hosts.



Our penetration testing will involve:

- ▶ Moving laterally in the environment.
- ▶ Escalating account privileges.
- ▶ Attempting to exfiltrate data.
- ▶ Leaving a trophy.
- ▶ Cleaning up the environment.

Execute Automated and Manual Exploits.



IDENTIFY AND REMOVE FALSE POSITIVES

The following manual testing methods will be used to identify false positives:

- ▶ Tools will be configured specifically to the operating system or firmware version of the network device or system being tested.
- ▶ Our staff will rely on the experience of the subject matter expert to identify false positives, including those caused by backporting.
- ▶ Prior to reporting, we will validate our technical findings with IT Management.



APPROACH AND METHODOLOGIES

Internal | External Network Vulnerability Assessment and Advanced Penetration Test (cont.)

THEIR APPROACH

- ▶ Use of automated tools with limited manual tests and no false positive checks.

THE SECURANCE WAY...

- ▶ Securance will remain flexible to the Lottery's larger goals and potentially changing needs as the engagement unfolds.
- ▶ Results are investigated to ensure that no "false positives" are left with the The Lottery.
- ▶ Automated tools are paired with manual testing to provide the The Lottery a thorough, accurate assessment.

... DELIVERS EXTRA VALUE TO YOU.

- ▶ The Lottery will receive an exact depiction of how a bad actor would breach its network, and, more importantly, the specific steps required to prevent a future network breach.

Software Tools

Securance may use these tools during the penetration testing engagements, depending on the Lottery's needs:

▶ Web Application Scanning Tools:

- WebInspect – Dynamic application security testing (DAST) tool used to identify vulnerabilities in web applications and services. It scans the web application and uses audit engines to perform an attack, then generates a vulnerability report to aid remediation.
- ZAP (Zed Attack Proxy) – Stands between the tester's browser and a web application to intercept requests, modify contents, and forward packets.
- Nikto – Works with command lines to identify common web flaws, such as server misconfigurations. It performs tests against multiple items, checks for outdated versions of servers, checks for configuration items, and tests intrusion detection systems.
- w3af (Web Application Attack and Audit Framework) – A scanner with a framework to analyze applications and generate reports with its findings.
- WPScan – A security tool for WordPress. It can reveal flaws in WordPress installations, such as the use of the XML-RPC protocol or outdated dependencies. It can also perform brute-force attacks efficiently.
- NStalker – An automated scanning tool that provides a comprehensive assessment of web service vulnerabilities. It scans websites for security issues including SQL injection and cross-site scripting.

APPROACH AND METHODOLOGIES

Internal | External Network Vulnerability Assessment and Advanced Penetration Test (cont.)

▶ Network Scanning and Enumeration Tools:

- NMAP Scanner – Used for network exploration, host discovery, and security auditing, NMAP can map an entire network to find its open ports and services and fingerprint an operating system. It can adapt to network conditions, including latency and congestion, during a scan.
- NESSUS Scanner – Network vulnerability assessment tool for measuring system risks. Nessus is used to probe systems and report vulnerabilities that might create an exposure.
- GFI LANguard – Designed specifically for Windows. It enables users to manage and maintain end-point protection across a network, provides visibility into all the elements in a network, and helps assess where there may be potential vulnerabilities.
- Netcat – A UNIX utility that reads and writes data across network connections, using TCP or UDP protocol. It can be used for network troubleshooting, port scanning, and file transferring.
- Wireshark – Allows users to capture and browse the traffic running on a computer network. It supports hundreds of protocols and can analyze encrypted traffic if the encryption keys are provided.
- Gobuster – Efficient software that can be used to enumerate hidden directories and files quickly. Many web applications use default directories and file names that are relatively easy to spot. This tool can use brute-force techniques to discover them.
- Amass – Efficient for DNS (Domain Name System) and subdomain enumeration. It is actively maintained and updated to keep up with the latest techniques and methodologies, and combines various reconnaissance and gathering techniques.
- SAINT – A vulnerability scanner approved by the Payment Card Industry (PCI). It scans networks, servers, and applications for weaknesses and provides detailed reports and remediation recommendations.

▶ Wireless Network Scanning Tools:

- Hashcat – Provides advanced password recovery features and lets testers crack Wi-Fi passwords or password-protected documents such as ZIP files.
- Aircrack-ng – Tool for analyzing and cracking wireless networks. Aircrack-ng's main focuses include packet capture and export of data to text files for further processing, replay attacks, de-authentication, fake access points, and others via packet injection, and Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) for WPA and WPA2 cracking.
- Wifite – A wireless network auditor that deals with current or legacy attacks against WEP and WPA2. It is good for retrieving the password of a wireless access point such as a router.



APPROACH AND METHODOLOGIES

Internal | External Network Vulnerability Assessment and Advanced Penetration Test (cont.)

▶ Password Cracking Tools:

- John the Ripper – Supports hundreds of hash and cipher types, including for user passwords of Unix flavors, macOS, Windows, web apps, groupware, database servers, network traffic captures, encrypted private keys, filesystems and disks, archives, and document files.
- Medusa – A powerful brute-force tool that supports thread-based parallel testing like simultaneous brute-force attack.
- Ncrack – Can test all hosts and devices in a network for weak passwords. It's a set of command lines that can scan large networks, allowing sophisticated brute-force attacks.
- Rubeus – A tool used in penetration testing for Kerberos sessions. It exploits the identified vulnerabilities and performs functions such as crafting keys and granting access using forged certificates.

▶ Penetration Testing Tools:

- AppDetective – Designed to identify potential security risks and compliance violations in relational database management systems (RDBMS). It can also perform penetration testing support, configuration management, and privileged escalation detection.
- Cobalt Strike – A threat emulation software to create targeted attacks for penetration testing. It simulates real-world attacks and tests the security defenses of organizations' networks and systems.
- Burp – A software suite that can perform advanced scans. It is typically used for traffic interception, such as for HTTP requests.
- Metasploit – Contains a vast collection of exploit modules that target known vulnerabilities in various operating systems, applications, and network services. These modules automate the process of exploiting vulnerabilities to gain unauthorized access to target systems.
- Fiddler – Collection of manual tools for dealing with web debugging, web session manipulation, and security and performance testing.

▶ Exploitation Tools:

- SolarWinds – A powerful combination of network discovery, system and security management, monitoring and attack tools.
- Metasploit Framework – An advanced open-source platform for developing, testing and using exploit code, as well as identifying vulnerabilities and testing the effectiveness of security controls.
- Core Impact – A powerful exploitation tool that can use access from one exploit to further exploit other devices.

APPROACH AND METHODOLOGIES

Internal | External Network Vulnerability Assessment and Advanced Penetration Test (cont.)

- BeEF (Browser Exploitation Framework) – Aids in enumeration, phishing, and social engineering. It provides GUI and practical client-side attack vectors to target different contexts and achieve various tasks, such as stealing credentials.
 - SQLmap – Automates the process of detecting and exploiting SQL injection flaws and database server takeovers. It can detect various types of SQL injections, and supports an extensive range of databases.
 - SET (Social Engineer Toolkit) – Performs advanced social engineering attacks. Users will be able to create payloads, phishing pages like Google login, and other web attacks.
- ▶ **Sniffing Tools:**
- Wireshark – A network sniffer and TCP | IP analysis tool. It can capture and display the data traveling back and forth on a network in real-time or by analyzing saved capture files. It supports hundreds of protocols and can analyze encrypted traffic.
 - Ettercap – A packet sniffer that allows users to modify data on the fly and run man-in-the-middle (MITM) attacks. Commonly used to intercept passwords with ARP (Address Resolution Protocol) poisoning or spoofing.
 - Tcpdump – A powerful command-line packet analyzer. It prints out a description of the contents of packets on a network interface, preceded by a timestamp.
 - Wfuzz – Runs brute-force attacks on various elements such as directories, scripts, or forms.





APPROACH AND METHODOLOGIES

Social Engineering (Phishing)

The human element is often the most overlooked aspect of an organization’s security program. Social engineering assessments measure employee adherence to the Lottery’s cybersecurity program and identify weaknesses in security awareness training.

Our process for performing social engineering engagements can include remote and on-site testing activities. Securance performs all methods of social engineering testing and will tailor the exercises for this project to the Lottery’s requirements.



Remote Social Engineering Exercises

Phishing

- ▶ Our IT security consultants design a targeted phishing message that appears to come from a trusted source. Then, they identify the number of employees that inadvertently reveal sensitive information, such as usernames and passwords.
 - Trackable information includes the numbers of opens (unique and total), bounces, forwards, registrations, spam reports, and clicks on links in the email.
 - Examples of phishing campaign topics include:
 - Local discounts.
 - Gas cards.
 - O365 Webmail access.
 - O365 password reset | expiration.
 - HR policy update.
 - LinkedIn password reset.
 - LinkedIn recruiter invite.
 - LinkedIn access code.
 - Zoom call.
 - Suspicious activity notices.
 - Employee rewards and recognitions.
 - Company holidays
 - Termination letter
 - Client appreciation
 - Billing information.
 - Requests for IT support.
 - Software updates.
 - Requests from an authority figure.
 - Brand impersonation.
 - Tax refunds.
- ▶ **Spear Phishing:** While most phishing attempts cast a wide net, spear phishing activities are more targeted. Our consultants craft messaging tailored to employees who may have privileged access to critical systems and data.
- ▶ **Whaling:** Our consultants target a “big fish” in the executive suite such as a CEO, company owner, or president to coerce them into revealing sensitive data.



APPROACH AND METHODOLOGIES

Web Application Testing

Web applications are pieces of software that run in a web browser to exchange information and deliver services. Organizations use web applications to connect with customers conveniently and securely. The Securance approach to testing web applications covers more than just OWASP Top 10 risks. We evaluate web applications against the following risk categories:



- ▶ **Data Protection:** Because web applications often handle sensitive user data such as personal information, login credentials, and financial details, we assess the security and controls implemented to prevent unauthorized access and protect user data from theft or misuse.
- ▶ **User Privacy:** We assess how the Lottery protects users' personal information to maintain user privacy and build trust.
- ▶ **Preventing Cyber Attacks:** We perform automated and manual testing against the categories of attack listed below.

- Boolean parameter tampering
- Broken access control
- Broken authentication session management
- Buffer and integer overflow
- CGI attacks
- Common HTTP device attacks
- Cross site request forgery
- Cross site scripting (XSS)
- Directory | file traversal
- Failure to restrict URL access
- Format string
- Generic HTTP attacks
- Information leakage and improper error handling
- Injection flaws (e.g., SQL, CRLF)
- Insecure communications
- Insecure components
- Insecure cryptographic storage
- Insecure deserialization
- Insufficient logging and monitoring
- Malicious file | remote execution
- Microsoft CGI attacks
- Microsoft IIS attacks
- Parameter deletion
- PHP file include
- Security misconfiguration
- Sensitive data exposure
- Special parameter addition
- XML external entity

Our approach includes unauthenticated as well as authenticated testing. We will obtain a test credential set to log into the web application, uncover hidden input fields, test input parameters, crawl the portal and identify exploratory features, attempt to discover sensitive and private information, uncover common software writing errors, identify common injection vulnerabilities that may allow malicious code execution, and assess error handling that may expose the application.

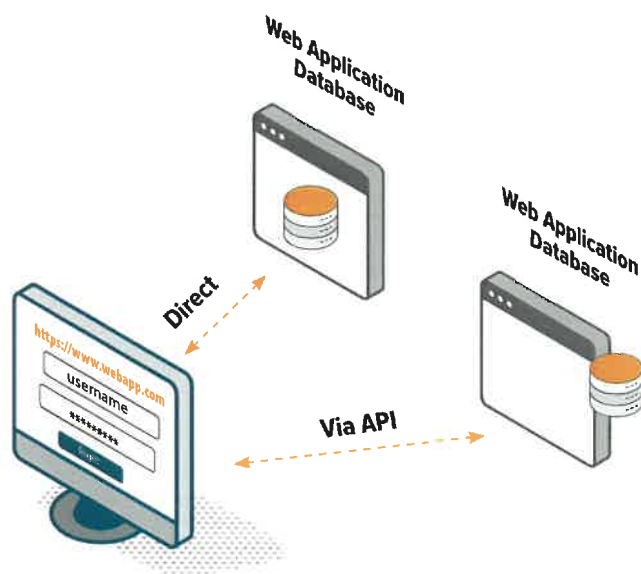


APPROACH AND METHODOLOGIES

Web Application Testing (cont.)

Our testing techniques are not only automated; we perform manual testing as well. Our manual testing includes:

- ▶ URL manipulation
- ▶ Input field character testing
- ▶ Input field string sanitization testing
- ▶ Remote site return validation
- ▶ Software version vulnerability testing



API Testing

Application programming interfaces (API) act as an intermediary layer that processes data transfers between systems allowing companies to open their application data and functionality to external third-party developers, business partners, and internal departments within their companies. Our API assessment includes:

- ▶ Evaluating the security of both ends of the Lottery's API connection.
- ▶ Performing manual manipulation testing.
- ▶ Assessing the Lottery's data integrity controls.

APPROACH AND METHODOLOGIES

Web Application Testing (cont.)

Database Assessment

In addition to the operating system-level procedures, we perform a comprehensive security analysis against the portal's back-end database. Initial attempts are made to access the database without credentials. Pending success, we perform a database-specific vulnerability scan using commercial tools (e.g., Application Detective, Tenable).

- ▶ **Compliance with Regulations:** We determine if there are specific Federal, State or local compliance requirements to protect user data and assess compliance with them to ensure the Lottery will avoid legal consequences.
- ▶ **Financial Impact:** As web applications are supporting many financial functions of the Lottery's operations, we assess the financial impact due to a security breach, or legal actions. This includes fines, remediation costs, and or credit monitoring services.
- ▶ **Availability and Reliability:** Ineffective security measures also contributes to the availability and reliability of web applications. We assess protections against distributed denial-of-service (DDoS) attacks to ensure that the web application remains accessible to users.
- ▶ **Protection Against Malware:** Our assessment also includes testing if the web application is vulnerable to malware attacks, which may compromise the security of users' devices. Specifically reviewing the supported browser versions.
- ▶ **Preventing Data Tampering:** We review the web application to ensure it prevents unauthorized parties from tampering with data.

Operating System Assessment

If access to the operating system is obtained or provided, we perform a detailed security review of the operating system configuration. These procedures are performed against all servers that comprise the web application infrastructure. Tools used include Rapid7, Tenable, Qualys, and other's based on the fingerprint of the operating system.

THEIR APPROACH

- ▶ Limited, if any, assessment of API, database, or operating system security.

THE SECURANCE WAY...

- ▶ Database-specific testing performed to identify risks.
- ▶ API-specific testing performed to identify data leakage and integrity.
- ▶ Operating system-specific testing performed against all servers that compromise the web application infrastructure.

...DELIVERS EXTRA VALUE TO YOU.

- ▶ No risk, threat, or vulnerability is missed.
- ▶ The Lottery will know exactly how to secure its application environment.



APPROACH AND METHODOLOGIES

Wireless Network Testing

Securance assesses the configuration and security of on-premise controller, cloud-based controller, and access point-based wireless networks. Our consultants will interview the wireless network administrator and review the following security controls:



Controller-Based Networks

For wireless networks with an on-premise controller or cloud based controller, Securance will:

- ▶ Assess controller configurations.
- ▶ Evaluate rogue access point detection and management.
- ▶ Uncover or identify hidden SSIDs.
- ▶ Assess encryption strength.
- ▶ Review network segmentation, including user authentication and access.
- ▶ Review administrative access controls and logging.
- ▶ Confirm access points can only receive configurations from the controller.
- ▶ Capture a handshake and attempt to crack the encryption.
- ▶ Install a rogue access point as a Pineapple device to attempt to divert user access.
- ▶ Assess device authentication.

For wireless networks with a cloud-based controller, Securance will evaluate the controls listed above to the extent the configurations are modifiable by the wireless administrator.

Access Point-Based Wireless Networks

Our access point-based assessment is similar to our controller-based assessment. However, because each access point has its own configuration, we will assess each access point's configuration individually.

Penetration Testing

Using assorted wireless radio devices, including Pineapple tools and various wireless adapters, we will intercept encrypted and unencrypted network packets. Depending on the rules of engagement, we will:

APPROACH AND METHODOLOGIES

Wireless Network Testing (cont.)



- ▶ Passively sniff and attempt to capture handshakes between the access point and client.
- ▶ Attempt to deauthenticate clients from the wireless network and capture the reestablished handshakes between the access point and client.
- ▶ Establish a rogue access point to lure client devices and capture their wireless authentication credentials.
- ▶ Attempt to crack the encrypted credentials and use them to breach the wireless network.

After gaining access to the wireless network, we will:

- ▶ Deploy executables and scripts to gain a presence on the network.
- ▶ Capture device and network information.
- ▶ Escalate privileges.
- ▶ Disable local firewalls and antivirus software.
- ▶ Create a new privileged user.
- ▶ Move laterally on the network to access and gain control of the domain controller(s).
- ▶ Exfiltrate data from host machines.
- ▶ Hide evidence of our breach.

Securance may use the following tools in this assessment:

- Vistumbler
- iStumbler
- Kismet
- Aircrack-ng suite
- Besside-ng
- Ncrack
- Hashcat
- John the Ripper
- Online rainbow tables
- Cain and Abel
- Mimikatz
- Advanced IP Scanner

THEIR APPROACH

- ▶ Perform interviews and configuration review of the wireless network.

THE SECURITY WAY...

- ▶ Assess not only the controller but also the access points.
- ▶ Install a pineapple to capture and decrypt handshake to penetrate the internal network.

....DELIVERS EXTRA VALUE TO YOU.

- ▶ Comprehensive analysis of how the wireless network can be used as a vector to attack the internal network with detailed recommendations to secure the wireless network.





APPROACH AND METHODOLOGIES

Internet of Things (IoT)

To threat actors, all connected devices are simply attack vectors. Internet of Things (IoT) devices create pathways into enterprise or private networks. A vulnerability in one of these IoT devices can lead to data breaches of sensitive information that affect an entire organization and lead to legal ramifications. Since most IoT devices are not centralized, it becomes difficult to properly secure devices that are constantly exposed to a physical attack surface. Without a secure location and continual surveillance, these devices allow potential attackers to gain information about their network's capabilities so they can initiate future remote attacks or gain control over the device. In addition, any time data is transmitted, received, or stored on these devices, the potential for a breach increases. As cyber threats evolve, the magnitude, automation, and customization of AI-powered attacks will make them increasingly more challenging to thwart. Securance will evaluate all types of IoT devices across every connection method to identify specific risks to the Lottery's security.

Securance's IoT testing includes, but is not limited to, assessing the following common IoT communication protocols:

- ▶ **Bluetooth:** Wireless technology that allows the exchange of data between different devices within a short distance using radio waves.
- ▶ **Wireless:** Information flows from a transmitter to a receiver. These devices can span distances from a few feet to thousands of miles.
- ▶ **Internet Protocol (IP) based:** Set of rules for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.
- ▶ **Low Power Wide Area Networks (LPWAN):** A type of wireless network that allows long-range communication between IoT devices, such as sensors, at a low bit rate and low power consumption.
- ▶ **Cellular:** Technology that enables devices to communicate wirelessly over cellular networks. These networks have evolved through different generations (3G, 4G, 5G).
- ▶ **Zigbee and other mesh protocols:** Zigbee is a wireless technology designed as an open global market connectivity standard for low-cost, low-power wireless IoT data networks that can support mesh networking. In a mesh network, nodes are interconnected with other nodes so that multiple pathways connect each node.

APPROACH AND METHODOLOGIES

Internet of Things (cont.)



OUR PROCESS

Security Practice and Protocol Evaluation

- ▶ Physical security—Securance will ensure that the physical components of the Lottery’s IoT systems, like devices, sensors, and gateways, are being properly protected from unauthorized access and damage. We will evaluate their location, access controls, monitoring systems, asset tracking systems, and disposal process.
- ▶ Network segmentation—Securance will ensure that the Lottery’s IoT devices are isolated from critical infrastructure and sensitive data.
- ▶ Device inventory and classification—Securance will ensure that the Lottery is regularly updating IoT device inventory, including device classification, capability, connectivity protocols, and security features.
- ▶ Data Security—Securance will evaluate the measures in place to protect IoT devices and the data they produce. Our assessment will include encryption methods if applicable, access controls, authentication methods, vulnerability scanning, and data governance policies.
- ▶ Compliance—Securance will ensure the Lottery’s IoT systems comply with data protection laws and industry standards.
- ▶ Gather information about relevant IoT devices, including hardware specifications, firmware versions, communication protocols, and known vulnerabilities by performing an IoT specific vulnerability scan.
- ▶ Analyze the configuration of IoT devices to identify outdated software components, default passwords, insecure communication channels, and weak encryption.
- ▶ Develop exploit techniques targeting the IoT devices in a controlled environment to assess their response to attacks.



APPROACH AND METHODOLOGIES

Internet of Things (cont.)

THEIR APPROACH

- Typically, does not address protocol risks and technical vulnerabilities with remediation unique to the Lottery's IoT network environment.

THE SECURANCE WAY...

- Recommendation on how to remediate security gaps with several targeted fix strategies including macro and micro-segmentation and port and service blocking.

...DELIVERS EXTRA VALUE TO YOU.

- The Lottery will receive every risk presented with actionable recommendations for IoT security improvement based on our risk-focused approach, customized assessments, and client-driven scope based on the Lottery's objectives and drivers.

Mitigation Recommendations

Based on our testing, Securance will prioritize the IoT device risks and create actionable remediation recommendations for the Lottery's improved security. Recommendations may include patches and updates, implementing security controls, improving access management, port security, and/or fortifying network segmentation.



APPROACH AND METHODOLOGIES

Next-Generation Firewall Assessment

Securance's approach to performing firewall configuration reviews covers misconfigurations, vulnerabilities, supporting IT processes, and other weaknesses that could leave an organization susceptible to attack. To ensure the Lottery's firewall configuration is secure, we will assess the current configuration against best practice guidelines. We will discern the optimal configuration for your firewall, according to your network environment and security goals. Our comprehensive assessment begins with gaining an understanding of the role the device plays in protecting and segmenting the Lottery's network infrastructure. Once we have gained an understanding of the firewall's role, our process includes:

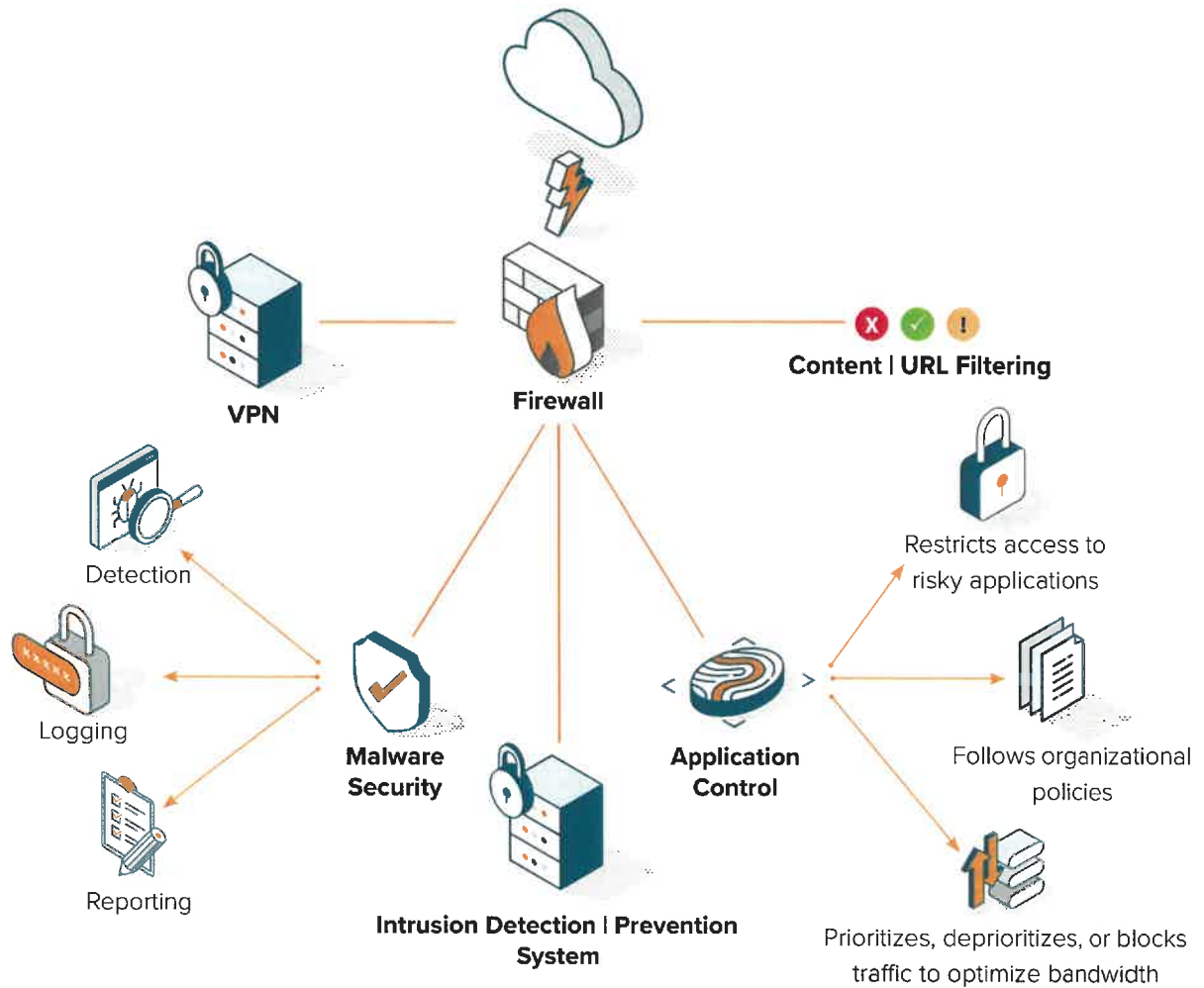


- ▶ Assessing the firewall environment and infrastructure. We will:
 - Interview Firewall Administrator(s).
 - Review Network and Firewall Diagrams.
 - Identify the Current Firmware Version.
 - Identify Internet Service Providers.
 - Identify Remote Connections.
 - Identify Additional Methods of Internet Access.
 - Obtain Default Vendor Configuration.
- ▶ Reviewing administrative and access controls.
 - Review Administrator Roles and Responsibilities.
 - Identify Primary and Backup Administrators.
 - Review Password Policy.
- ▶ Evaluating authentication methods.
- ▶ Review hardware and assets.
 - IP addresses | URLs.
- ▶ Assessing configuration against best practice standards (e.g. CIS, DISA).
 - Review Ruleset Line-by-Line.
 - Identify Problem Rules.
 - Identify Redundant Rules.
 - Identify Circular Rules.
 - Perform a Vulnerability Scan of the Device(s).
 - Review Logs Manually.
 - Analyze Traffic Patterns.
 - Identify Potential Virus and Hack Attempts.
 - Recommend Potential Rules to Improve Security.
 - Assess Use of Insecure Protocols.

APPROACH AND METHODOLOGIES

Next-Generation Firewall Assessment (cont.)

In addition, next-generation firewalls can provide several subscription-based services. The diagram below illustrates some of the available services.



Based on the services the Lottery subscribes to, we will evaluate how those services are configured. For example,

▶ **Intrusion detection | penetration system.**

- Ensure IPS is calibrated appropriately to solely stop intruders and not the Lottery's actual users.
- Ensure IDS and IPS are placed where they best function in the infrastructure.
 - Deploy IDS out of band so it can analyze all traffic and generate intrusion events from suspect or malicious traffic.
 - Deploy IPS in the path of traffic so that all traffic must pass through the appliance to continue to its destination, or it can disrupt the connection in the event of malicious intent.
- Configure to block an attack.

APPROACH AND METHODOLOGIES

Next-Generation Firewall Assessment (cont.)

▶ VPN.

- Establish another layer of protection to [Client's] network.
- Establish connections with network defenders.
- Encrypt your network.

▶ URL | Content filtering.

- Ensure filtering is enabled and up to date to safeguard users from online threats by offering precise control over user access and engagement with internet content by recognizing patterns indicative of undesirable content.

▶ Application Control.

- Restricts access to risky applications.
- Follows organizational policies.
- Prioritizes, deprioritizes, or blocks traffic to optimize bandwidth.

▶ Malware Security.

- Ensure Anti-malware definitions are updated in real time.
- Includes:
 - Logging.
 - Reporting.
 - Detection.
 - Honeypot files.
 - Cyclic redundancy check (CRC).
 - Machine learning behavior analysis.
 - Signature-based detection.
 - Static file analysis.
 - Dynamic malware analysis.
 - Application allowlisting.

THEIR APPROACH

- ▶ Typically a desktop and administrative review of ruleset.
- ▶ Shallow knowledge of next-generation firewalls as a pillar of ZTNA.

THE SECURANCE WAY...

- ▶ We take the time to understand the role of the firewall and how it is administered.
- ▶ We evaluate more than just firewall rules.
- ▶ We provide consultation on opportunities to optimize the firewall.

...DELIVERS EXTRA VALUE TO YOU.

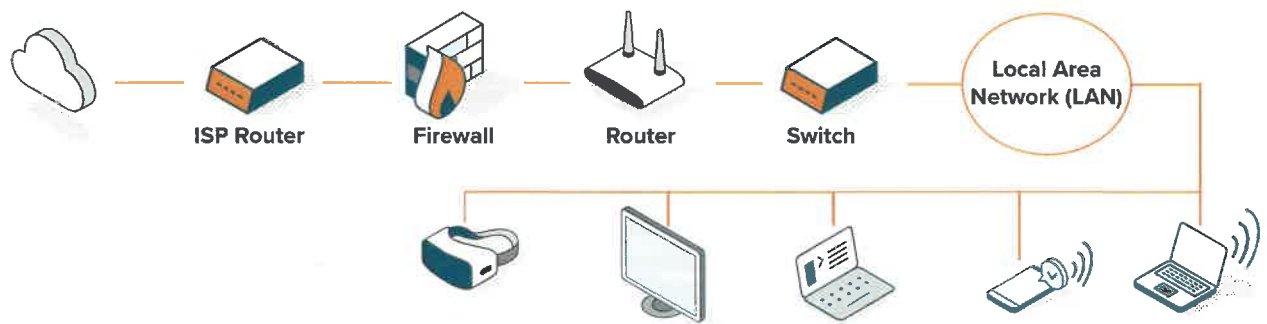
- ▶ First layer of defense configured to prevent unauthorized access or a network breach.



APPROACH AND METHODOLOGIES

Router-Switch Configuration Review

Network devices reviews, like routers and switches, are critical for maintaining secure network infrastructure. Securance has conducted router and switch reviews for clients across all major industries, over our 22 years of cybersecurity service. The Securance methodology for evaluating the security of these network devices focuses on ensuring components are correctly configured and firmware is updated to create and maintain a network devoid of infrastructural weaknesses.



Pre-Assessment

- ▶ Interview device administrator(s) to gain a preliminary understanding of the devices in the network and their current configurations.

Analysis

- ▶ Perform an automated and manual, line-by-line review of device configuration, ensuring:
 - The device is running the most up-to-date firmware version.
 - Default manufacturer passwords are not in use.
 - Insecure protocols are not in place:
 - Telnet configuration.
 - Unencrypted communications.
 - File transfer protocol (FTP).
 - Access control is strong—Securance will review Access Control Lists (ACLs) to control traffic flow, restrict unauthorized access, and enhance security.
 - Network Address Translation (NAT) is properly implemented to effectively manage translating private and public IP addresses.
 - Virtual Local Area Networks (VLANs) are configured to better segment network traffic.
 - Spanning Tree Protocol (STP) is configured to prevent network loops and ensure redundancy.



APPROACH AND METHODOLOGIES

Router-Switch Configuration Review (cont.)



- Port Security is configured to enhance protection against unauthorized devices.
- Quality of Service (QoS) settings are configured to prioritize certain aspects of the Lottery's network traffic.
- Changes to the device configuration comply with organizational change management procedures.

Vulnerability Scan

- ▶ Perform an unauthenticated and I or authenticated vulnerability scan of the device to identify vulnerabilities associated with the specific device. Based on the identified vulnerabilities, perform specific exploit testing with a goal of obtaining full control of the device.

Monitoring

- ▶ Review logs using manual and automated techniques to verify that:
 - Logging for security events is enabled.
 - Logs are housed in a central location.
 - Sensitive information, such as passwords, are not logged.
 - Logs are not altered.
 - Alerts are set up.
 - Logs are aggregated with other technology logs.
 - Logs are reviewed on a regular basis.

Gap Analysis

- ▶ Compare device configuration and policies to the Center for Internet Security (CIS) benchmarks to identify gaps and develop a plan for The Lottery to remediate them.

THEIR APPROACH

- ▶ Typically, a desktop and administrative review of the device's configuration.
- ▶ Results are based on superficial analysis providing incomplete recommendations.

THE SECURANCE WAY...

- ▶ Thorough examination of configuration, security, and best-practice adherence.
- ▶ Performs vulnerability scan to focus on critical areas and potential network risks.

...DELIVERS EXTRA VALUE TO YOU.

- ▶ The Lottery will receive a risk-focused and well documented report that provides clear solutions with actionable improvement steps.

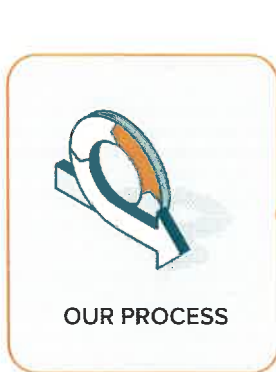
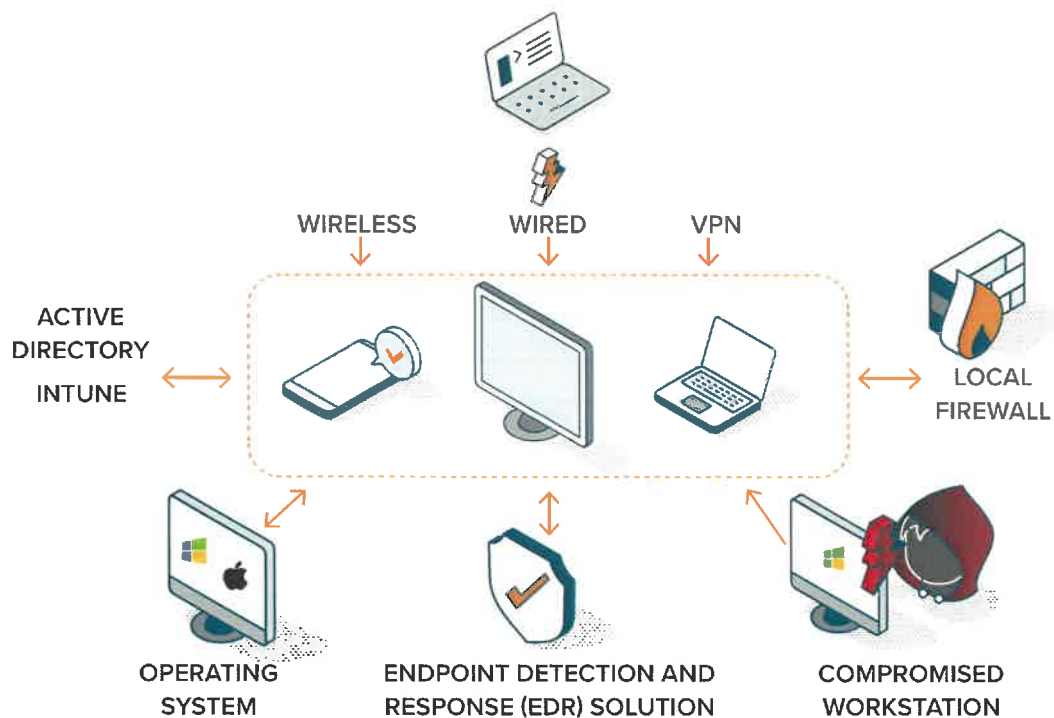
APPROACH AND METHODOLOGIES

Workstation Configuration Review

Securing end user devices, including workstations, is a critical component to ensuring an IT environment is secure. Securance has conducted workstation reviews for clients across all major industries over our 22 years of cybersecurity service.

Effective workstation hygiene reduces the likelihood of an attacker gaining access to enterprise data via an unsecured workstation and potentially compromising the Lottery's entire network.

Securance's workstation configuration assessment will examine the configuration of The Lottery's endpoint devices by taking a deeper dive into specific device settings and controls.



Our approach begins with assessing the device's configuration. This includes:

- ▶ Assessing the local security-related configuration options (e.g., BitLocker, enabled firewall).
- ▶ Assessing the security posture of the endpoint's underlying operating system and comparing it to industry standards and Center for Internet Security (CIS) benchmarks. To ensure the Lottery's system aligns with best practices, we will:
 - Assess the current operating system configurations.

APPROACH AND METHODOLOGIES

Workstation Configuration Review (cont.)



- Examples of traditionally overlooked registry changes include:
 - Confirming 'Remote Desktop Services (TermService)' is 'Disabled'.
 - Confirming 'Remote Registry (RemoteRegistry)' is 'Disabled'.
 - Ensuring 'Windows Remote Management (WS-Management) (WinRM)' is 'Disabled', if applicable for the environment.
 - Confirming 'Turn off Microsoft Peer-to-Peer Networking Services' is 'Enabled'.
 - Confirming 'Support device authentication using certificate' is 'Enabled'.
 - Confirming 'Disallow copying of user input methods to the system account for sign-in' is 'Enabled'.
 - Confirming 'Allow users to connect remotely by using Remote Desktop Services' is 'Disabled'.
 - Assessing the 'Set time limit for active but idle Remote Desktop Services sessions' is appropriately set to 15 minutes or less, but not 'Never (0)'.
 - Confirming that the 'Set time limit for disconnected sessions' is appropriately set.
 - Confirming that 'Allow remote server management through WinRM' is 'Disabled'.
 - Confirming that 'Allow Remote Shell Access' is 'Disabled'.
- Assess the process of creating and modifying workstation images.
- Assess the administration of deploy management tools.
- Monitor configuration management changes.
- Assessing the effectiveness of the implemented endpoint detection and response (EDR) solution by confirming:
 - It is configured to detect and respond to threats.
 - It is dynamic enough to incorporate new findings outside of core forensic evidence (e.g., file system metadata, account activity).
 - It is configured to collect event data from the endpoint.
 - It is configured for real-time alerts.
 - It is configured to remove an infected device from the network.

APPROACH AND METHODOLOGIES

Workstation Configuration Review (cont.)



- It provides forensic investigative capabilities alongside behavioral analysis (using AI or machine learning) that can paint a complete picture of how an attacker was able to compromise an endpoint.
- Its logs are ingested into a SIEM.

- ▶ Attempting to compromise the workstation by loading malware, visiting malware sites, and performing other simulated attacks like permissions escalation, to reach exponentially more sensitive data on the network.

THEIR APPROACH

- ▶ Process and desktop review of workstation security without deep knowledge of the Lottery's workstation environment or testing of security configurations.

THE SECURANCE WAY...

- ▶ Comprehensive assessment, including a review and testing of process controls, technical settings, and network security appliance configurations.

...DELIVERS EXTRA VALUE TO YOU.

- ▶ The Lottery will be provided with an actionable remediation report to improve its workstation security posture to a level supportive of a Zero Trust Network Architecture.

Once we have gained an understanding and tested the security of the device, we assess the configuration of network technologies deployed to protect the device and its data. This includes:

- ▶ Gaining an understanding and reviewing the configuration of network firewalls to protect the workstation environment.
- ▶ Gaining an understanding and reviewing the configuration of Intrusion Detection/Protection Systems (ID/PS) to protect the workstation environment.
- ▶ Gaining an understanding and reviewing the configuration of network web content filtering to protect the workstation environment.
- ▶ Gaining an understanding and reviewing the configuration of email filters to protect the workstation environment.
- ▶ Gaining an understanding and reviewing the configuration of Data Loss Prevention (DLP) systems to protect the workstation environment.
- ▶ Gaining an understanding of how the endpoint's authentication to the network is governed by assessing Active Directory's Password Policy Objects (PSOs) and Group Policy Objects (GPOs).
- ▶ Assessing the use of Multi-Factor-Authentication (MFA).

APPROACH AND METHODOLOGIES

Workstation Configuration Review (cont.)

- ▶ Reviewing the configuration of either the GPO or InTune by:
 - Assessing domain structure and policies.
 - Evaluating user and computer attributes.
 - Assessing the structure and use of InTune.
- ▶ Reviewing network access control (NAC) technologies and their configuration, including:
 - Configuration analysis.
 - Assessment of network segments and the systems defined for each segment.
 - Testing of access based on defined NAC rules.

Upon completing the assessment of the workstation environment, we will prepare a detailed narrative and technical report that includes actionable recommendations that have been confirmed with The Lottery's technicians and administrators.





APPROACH AND METHODOLOGIES

Server Operating System Assessment

The server's operating system is the environment in which an application runs. If not properly patched and updated, it will accrue vulnerabilities and leave application security susceptible to compromise. Our assessment is designed to ensure the organization's servers maintain a stable and secure environment and effective controls and policies to deter both physical and Internet-based malicious attacks.



We will evaluate each server operating system (OS) that hosts a presentation layer, application layer, and database layer for:

- ▶ OS-level vulnerabilities.
- ▶ Configuration aligned with The Lottery's standards and best practices.
- ▶ The following are included in our operating system analysis:
 - **Windows Server Review:**
 - 50+ security option settings.
 - Account policy (if applicable).
 - Account policy settings (if applicable).
 - Accounts with no password.
 - Change I patch management.
 - Comparisons against industry average and leading practice.
 - Connected servers and workstations.
 - Customer-selected registry key values.
 - Directory rights and privileges.
 - Disabled accounts.
 - Discretionary access controls.
 - Event logging (if applicable).
 - Group management.
 - Group policy objects (GPO) and links.
 - Network connections.
 - Network shares.
 - OS-specific vulnerability management (if applicable).
 - Overall structure.
 - RAS dial-in.
 - Security updates, patches, and hot fixes.
 - Services and drivers installed.
 - Trusted and trusting servers.
 - User administration.
 - User management.

APPROACH AND METHODOLOGIES

Server Operating System Assessment (cont.)



▶ The following are also included in our operating system analysis:

• **UNIX | Linux Server Review:**

- Accounts with expired dates.
- All password related setting.
- Change | patch management.
- Comparisons against industry average and leading practice.
- Current network connections.
- Disabled usernames.
- Discrepancies in password and shadow password files.
- Files with World writable permissions.
- FTP access.
- Group administrators.
- Groups and group members.
- Guest account management.
- Last logins.
- Login retries.
- Network services enabled.
- OS specific vulnerability management.
- Password shadowing.
- Passwords 30 days or older.
- Permissions on selected sensitive files | directories.
- Redundant groups and members.
- Rot account management and control.
- SUID and SGID permissions.
- System login script file.
- System search paths.
- System wide security setting.
- Trivial passwords.
- Trusted hosts.
- Use and control of “r” commands.
- Use of Telnet and high-risk protocols.
- User administration.
- Usernames, UIDs, and home directory.
- Users allowed to login remotely.
- Users with administrative status.

THEIR APPROACH

- ▶ Focuses on the server-specific controls only.

THE SECURANCE WAY...

- ▶ Assesses the entire server environment and any associated application stack(s).
- ▶ Includes supporting IT general controls.
- ▶ Incorporates technical testing where appropriate.

....DELIVERS EXTRA VALUE TO YOU.

- ▶ A comprehensive assessment report of every risk and technical vulnerability within the server environment.

In addition to performing a comprehensive review of the server OS, our approach also includes an assessment of the supporting IT general controls.

APPROACH AND METHODOLOGIES

Server Operating System Assessment (cont.)

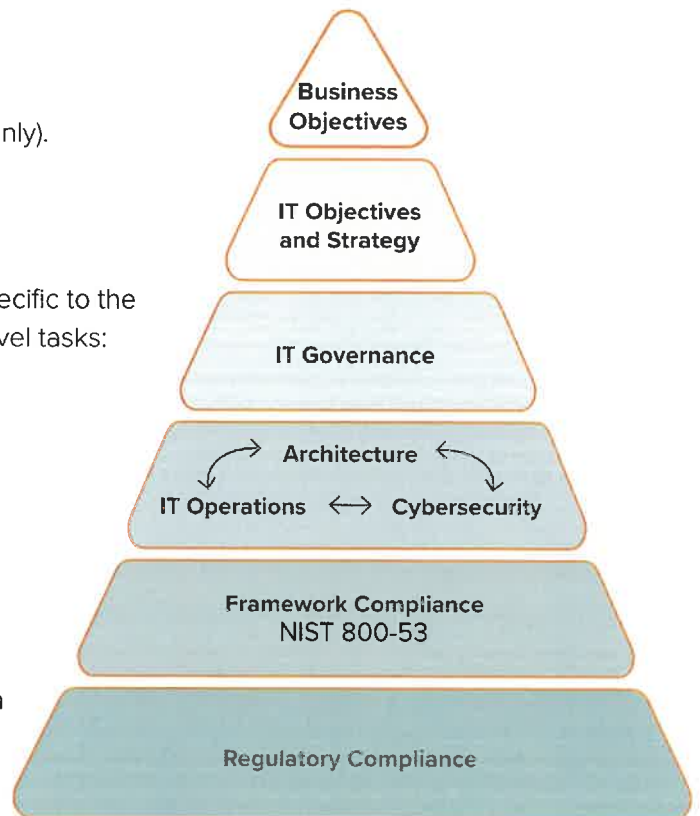
We will assess the IT general controls supporting the server environment and compare them to the Lottery's preferred framework or the National Institute of Standards and Technology (NIST) framework. The most common IT processes supporting an servers include:

- ▶ Password controls.
- ▶ Patch management.
- ▶ Physical security (on-premise applications only).
- ▶ System recovery.
- ▶ User provisioning.

Our assessment of these processes will be specific to the target server and include the following high-level tasks:

- ▶ Obtain and review supporting IT policies, procedures, standards, and guidelines.
- ▶ Interviews with technology administrators and or IT process owners.
- ▶ Identification of controls stipulated in policy documentation and comparison to The Lottery's desired control framework(s).
- ▶ Use of IT security and audit tools to perform specialized testing.
- ▶ Online and real-time review of technical configuration settings.
- ▶ Analysis of collected documents, technical reports, and other audit evidence.
- ▶ Completing our issue tracker for all potential findings.
- ▶ Immediate review with the Lottery's IT staff of any potential finding deemed Urgent or Critical.
- ▶ Discussion and confirmation of potential findings with the Lottery's IT staff and key stakeholders.

These tasks will complete our server assessment and inform our actionable findings and observations.



PROJECT MANAGEMENT

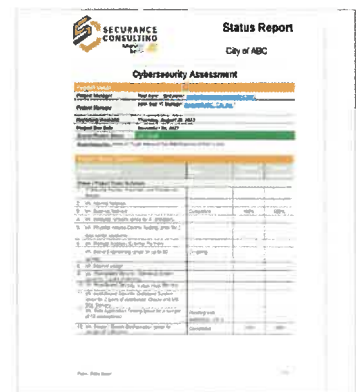
Securance is dedicated to performing this engagement as efficiently as possible. The assigned engagement manager (EM) will be responsible for ensuring project success by facilitating regular communication and providing status reports that will track progress, possible risks, and other information pertinent to the project. Their specific responsibilities are outlined below:



Engagement Manager Tasks

The EM will manage and oversee the entire project and be responsible for the following tasks:

- ▶ **Project Kick-Off:** Securance will hold a kick-off conference with the Lottery. During this meeting, we will introduce our project team and define the project scope, objectives, timeline, and deliverables. We will also review the Client Assistance Request, which is a memo listing all documentation and interviews required to complete the assessment. We will establish the frequency of meetings and project status updates, key stakeholders, and lines of communication for both the Lottery and Securance.
- ▶ **Work Plan:** Within one week of receiving the notice to proceed, Securance will submit a detailed work plan for the Lottery review and approval. Our work plan will include due dates for all deliverables, as well as intermediate milestones. We will update the work plan, as necessary, throughout the course of the project.
- ▶ **Status Reports:** Throughout the engagement, the Lottery PM will receive project status reports that will identify the past week's completed tasks, tasks planned for the upcoming week, pending requests for information, and any issues and I or risks that have been identified, with actions taken to mitigate them.



PROJECT MANAGEMENT



Shared Tasks

Securance's EM and key personnel will be responsible for the following tasks throughout the Lottery project:

- ▶ **Issue and Risk Management:** Securance prioritizes issues by taking the following into consideration:
 - Potential impact of the issue on the project.
 - Length of time the issue has been unresolved.
 - Criticality of the issue to the Lottery IT environment.

These factors will be looked at as a whole and discussed with the Lottery's PM to determine the ultimate priority of each issue. Additionally, as part of our status reports, we will document all project findings and related evidence in an "Issue Tracker" document that will also be shared with the Lottery's PM. Use of the tracker helps to avoid unwanted surprises and | or disputes over findings.

- ▶ **Continuous Improvement:** We will permit the Lottery employees to shadow our consultants as they execute technical engagements. Additionally, to ensure continuous improvement of the Lottery security objectives, our team will conduct a knowledge transfer session upon completion of the assessment.

THEIR APPROACH

- ▶ Communications are limited to project status.
- ▶ Findings are not communicated until the report has been drafted.

THE SECURANCE WAY...

- ▶ Constant and consistent project communication.
- ▶ **Immediate** communication of Urgent and Critical findings.
- ▶ Confirmation of findings prior to drafting.

...DELIVERS EXTRA VALUE TO YOU.

- ▶ Securance provides exceptional project management expertise, leveraging 22 years of experience and more than 2,500 cybersecurity assessments to deliver project success on time and on budget.

LOTTERY RESOURCES NEEDED TO COMPLETE THE PROJECT

When a contract or statement of work is executed, there are specific items Securance will need to perform the engagement. To ensure the Lottery obtains the most out of its partnership with Securance, we have provided an initial list of information, access requests, and documentation our experienced team will need to hit the ground running.



Access to the Lottery's Staff

- ▶ Adequate access to management and other key personnel for consultation and interviews. Very little of their time will be taken, but some contact will be necessary.
- ▶ Access to a project manager for scheduling interviews with appropriate Lottery staff.
- ▶ Access to technical staff (if needed) during the length of the technical testing (very little time needed).
- ▶ Access to staff who have been identified for interviews during the length of the project (approximately one hour each).
- ▶ Immediate access on a part-time basis to a cybersecurity staff member who can assist with questions (when needed).

Logical and Other Access Requests

- ▶ IP addresses for the external and internal network vulnerability assessments and penetration tests
- ▶ User IDs | passwords for web-applications | operating systems | workstations (if needed).
- ▶ Authority to access network components and operating systems (as needed).

Office Space for On-Site Work (As Needed)

- ▶ Identification badges, or equivalent should be available on arrival (if needed);
- ▶ Lockable cabinet for documentation.
- ▶ Workspace when on site.

Client Assistance Request Summary and Rules of Engagement Memo
(see examples of this documentation on the following pages).

LOTTERY RESOURCES NEEDED TO COMPLETE THE PROJECT

Sample Client Assistance Request Summary

Securance

2024 West Virginia Lottery Client Assistance Request

Location:

No.	Phase I	Request Description	Status/Notes/Comments
1	External Network	Please provide the contact information for the external network vulnerability assessment.	
2	External Network	Please provide a listing of all of the Internet-facing IP addresses to be assessed.	
3	External Network	Please provide any specific IP addresses that are out-of-scope that may be hosted by 3rd parties or too sensitive to be scanned.	
4	External Network	Please provide any information related to the period of daytime when scanning can be begin.	
5	Internal Network	Please provide the contact information for the internal network vulnerability assessment.	
6	Internal Network	Please provide the address from which we will authorized to work while performing the internal network vulnerability assessment.	
7	Internal Network	Please provide a listing of all of the internal IP addresses to be assessed.	
8	Internal Network	Please confirm if all initial scanning can be performed at one time.	
9	Internal Network	Please advise if there are any specific systems or IP addresses that should not be scanned.	
10	Internal Network	Please advise if there is a VOIP system. These systems typically failover during vulnerability testing.	
11	Internal Network	Please provide all available network diagrams. The more detailed the better.	

LOTTERY RESOURCES NEEDED TO COMPLETE THE PROJECT

Sample Rules of Engagement Memo



MEMORANDUM

DATE: _____ (version 1.0)
TO: [RFP Client's Project Management]
FROM: Securance LLC
RE: Security Assessment Rules of Engagement (RoE) - SAMPLE

This memo represents the mutually agreed upon RoE for the upcoming network security assessment.

ITEM	CLIENT RESPONSE
1. Scope of Effort	External network, internal network, and web application testing.
2. IT Environment Uniqueness	
3. VoIP Solution (Yes No)	
4. Scan VoIP Solution (Yes No)	
5. How to Handle Scope Creep	
6. Approved Date(s)	External: Web Apps: Internal:
7. Approved Time(s)	
8. Approved Tool(s)	Nmap, Rapid7, Qualys, Tenable, Cobalt Strike, Canvas, D2, NStalker, Others as necessary
9. Tool Configuration	
<ul style="list-style-type: none"> o Disable DDOS (Yes No) o Disable Brute Force (Yes No) o Disable Experimental Test (Yes No) o Privileged Testing (Yes No) o Disable Intrusive Test (Yes No) o Scan all TCP UDP Ports (Yes No) o Report by Hostname (Yes No) 	
10. If Privileged Testing (Admin Level: Yes No)	
11. Scan 3 rd Party-Hosted IP's (Yes No)	
12. Provide Client Lab's IP Address (Yes No)	



LOTTERY RESOURCES NEEDED TO COMPLETE THE PROJECT

Sample Rules of Engagement Memo (continued)



MEMORANDUM

ITEM	CLIENT RESPONSE
13. Interest in Whitelisting Lab's IP	
14. Communication Ground Rules	Communication will be via email. Provide daily status updates via: Email SMS Conference Call
15. Escalation Plan	Any signs of disruption, immediately contact consultant to discuss.
16. Communication Tools	Email, mobile and lab's direct phone (see consultant's info)
17. Client Specific Concern 1?	Disruption
18. Client Specific Concern 2?	
19. Securance PM Contact Information	
<ul style="list-style-type: none"> o Project Manager Name o Project Manager Email Address o Project Manager Mobile Phone o Project Manager Office/Lab Phone 	
20. Security Engineer Contact Information	
<ul style="list-style-type: none"> o Consultant Name o Consultant Email Address o Consultant Mobile Phone o Consultant Office/Lab Phone 	

By: _____ Title: _____
 Securance: Please Sign Please Type

Name: _____ Date: _____
 Please Type Please Type

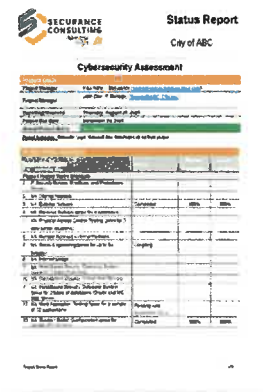
By: _____ Title: _____
 Client Project Manager: Please Sign Please Type

Name: _____ Date: _____
 Please Type Please Type

REPORTING

Status Reporting

Throughout the engagement, the Lottery's PM will receive project status reports that will identify the past week's completed tasks planned for the upcoming week, pending requests for information, and any issues and I or risks that have been identified, with actions taken to mitigate them.



Final Reports

The Lottery will receive two final reports at the end of each engagement, a management report and a technician's report. The Securance engagement manager will review the reports with the Lottery's team and other stakeholders to ensure that the findings and recommendations are understood, and to answer any questions that the Lottery may have. In addition, we will provide free technical support and advice throughout the remediation phase. In the Appendix, we provide a sample management report and technician's report for the Lottery to review.

Management Report

Within one week of completing our fieldwork for each assessment, Securance will provide the Lottery with a board-ready management report tailored to its environment and needs and developed with input from the Lottery's stakeholders and IT management. Our analysis of the risks identified within the Lottery's environment will take into account its threat profile and the likelihood and impact of exploitation of existing vulnerabilities. The report will document our analysis, prioritize risks based on their potential impact on the business, and provide realistic remediation recommendations aligned with the Lottery's risk appetite. Comprised of two sections, the report will include an executive summary and a detailed project report, each of which is described below.


During the engagement, if Securance identifies a vulnerability defined as urgent or critical by the Common Vulnerability Scoring System (CVSS) Version 3.1, or any other risk that we feel needs immediate attention, our team will promptly notify the Lottery. Once the Lottery's staff has addressed the risk or threat, Securance will reassess it to validate remediation success.

REPORTING

Management Report

Executive Summary

The executive summary will outline the engagement's scope, approach, findings, and recommendations in a manner suitable for management and will be presented to the Lottery stakeholders during the exit conference. It will include a heat map highlighting identified risks based on their likelihood and impact via a color-coded graph.



CLICK ON THUMBNAILS TO VIEW THE REPORTS

EXECUTIVE SUMMARY

BACKGROUND

ABC County (County) is home to more than 800,000 residents. The County strives to protect its assets, its residents, and the technology supporting government operations. In January 2022, the County's Internal Audit Department contracted Securix to perform an IT security assessment.

OBJECTIVES, SCOPE, AND SCOPE

The objective of the review was to identify weaknesses in the County's IT process controls and vulnerabilities in select technologies. The scope of our testing included the following components:

- IT processes:
 - Governance policies and procedures
 - Indicators of compromise (IoC)
- External (Internet-facing) network vulnerability assessment and penetration testing
- Internal network vulnerability assessment and penetration testing
- Wireless network
- Virtual private network (VPN)
- Network firewalls, routers, and switches
- Server operating systems
- Voice over Internet Protocol (VoIP) system

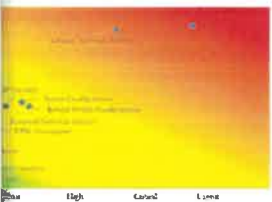
APPROACH AND METHODOLOGY

We designed an approach and applied our proven methodologies to ensure a comprehensive assessment. This approach included the following activities:

- Review of IT policies, procedures, and standards
- Interviews with IT management and personnel
- Review of collected evidence and testing of relevant IT operations and processes
- Automated and manual security testing

The review was limited to the technologies and processes listed on the preceding page and was not intended to cover the County's entire information systems function.


INTERNAL AUDIT HEAT MAP



IMPACT

Detailed Management Report

The detailed project report will provide specifics regarding the project scope, approach, and methodology, as well as findings and actionable recommendations co-developed by Securix and the Lottery.



CLICK ON THUMBNAILS TO VIEW THE REPORTS

SUMMARY OF FINDINGS

The following section provides a summary of our findings from the IT security assessment.

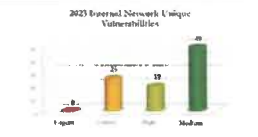
FINDING TITLE	Severity	Impact	CVSS	Score	Category
1 Patch Management	5	High	4	3	1
2 Internal Network Vulnerability Assessments and Penetration Test	4	High	3	2	1
3 External Network Vulnerability Assessment	3	High	2	1	1
4 VPN Assessment	2	High	1	1	1
5 Router/Switch Configuration Analysis	1	High	1	1	1
6 Server Configuration Analysis	1	High	1	1	1
7 VoIP Security	1	High	1	1	1
8 Policies and Procedures	1	High	1	1	1
9 System IoC	1	High	1	1	1
10 Wireless Network Assessment	1	High	1	1	1
11 External Network Public Information	1	High	1	1	1
12 Firewall Configuration Analysis	1	High	1	1	1
13 Firewall Optimization	1	High	1	1	1

No. 2: Internal Network Vulnerability Assessment and Penetration Test

We scanned the County's internal network and identified 25 critical, 19 high, and 49 medium-priority unique vulnerabilities. The scan results revealed vulnerabilities that increase the likelihood of an internal network breach.

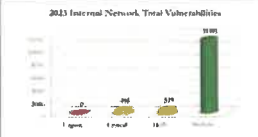
The chart below shows the vulnerabilities we identified, prioritized by level of severity, as defined by the Common Vulnerability Scoring System, Version 3.0 (CVSS v3.0). The technician's report summarizes the unique vulnerabilities, affected systems, and recommended solutions. In many cases, the recommended solution requires a system security patch. Vulnerability details are provided in a separate technician's report. Low-risk vulnerabilities and informational disclosures are only provided in the technician's report. A finding and technical vulnerability report is provided in an appendix.

2022 Internal Network Unique Vulnerabilities



Severity	Count
High	19
Medium	49
Low	1

2023 Internal Network Total Vulnerabilities



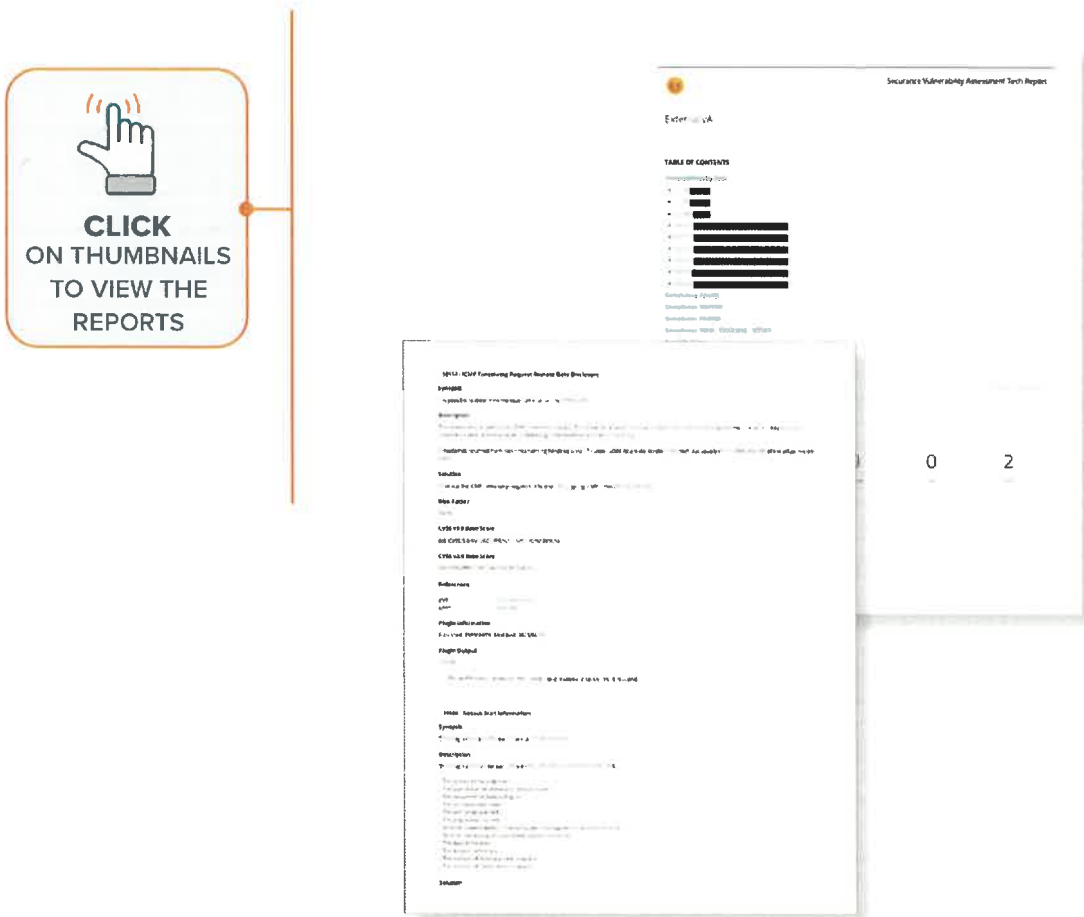
Severity	Count
High	19
Medium	49
Low	0

REPORTING


Technician's Report

Technician's Report

Intended to guide engineers and administrators through the remediation process, the technician's report will contain raw data extracted from our security tools. While the management report will focus on urgent, critical, high, and medium risks and vulnerabilities that require management's attention, the technician's report will cover all vulnerabilities, even low-risk vulnerabilities and advisory comments.



REQUIRED FORMS

	Department of Administration Purchasing Division 2019 Washington Street East Post Office Box 50130 Charleston, WV 25305-0130	State of West Virginia Centralized Request for Quote Service - Prof
---	--	---

Proc Folder: 1369290	Reason for Modification:
Doc Description: Network Penetration Testing and Cybersecurity Assessments	
Proc Type: Central Master Agreement	

Date Issued	Solicitation Closes	Solicitation No	Version
2024-03-08	2024-03-28 13:30	CRFQ 0705 LOT2400000009	1

BID RECEIVING LOCATION

BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Customer Code:
Vendor Name : Securance LLC

Address :
Street : 13916 Monroes Business Park, Suite 102
City : Tampa
State : Florida **Country :** United States **Zip :** 33635

Principal Contact : Pat Swere, Proposal Manager
Vendor Contact Phone: 877.578.0215 **Extension:** ext. 118

FOR INFORMATION CONTACT THE BUYER
 Brandon L Barr
 304-558-2652
 brandon.l.barr@wv.gov

Vendor  Signature X **FEIN#** 03-0392503 **DATE** 3.21.24

All offers subject to all terms and conditions contained in this solicitation

REQUIRED FORMS

Vendor Form (cont.)

ADDITIONAL INFORMATION
The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Lottery to establish a contract for Network Penetration Testing and Cybersecurity Assessments per the terms and conditions, Exhibit A Pricing Page and Exhibit B NDA, and specifications as attached.

INVOICE TO		SHIP TO	
LOTTERY PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	External Network Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
See Attached Specifications and Exhibit - A Pricing Page

INVOICE TO		SHIP TO	
LOTTERY PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Website Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
See Attached Specifications and Exhibit - A Pricing Page



REQUIRED FORMS

Vendor Form (cont.)

INVOICE TO		SHIP TO	
LOTTERY PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Internal/Client-Side Network Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
See Attached Specifications and Exhibit - A Pricing Page

INVOICE TO		SHIP TO	
LOTTERY PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Wireless Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
See Attached Specifications and Exhibit - A Pricing Page

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Questions due by 10:00am ET	2024-03-21

REQUIRED FORMS

Designated Contact Form

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Patrick Swere, Proposal Manager
13916 Monroes Business Park, Suite 102
(Address) Tampa, FL 33635
(Phone Number) / (Fax Number) 877.578.0215 ext. 118
(email address) pswere@securanceconsulting.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Securance LLC

(Company) [Signature]
(Signature of Authorized Representative)
Paul Ashe, President
(Printed Name and Title of Authorized Representative) (Date)
877.578.0215
(Phone Number) (Fax Number)
contactus@securanceconsulting.com
>Email Address)

Revised 8/24/2023



REQUIRED FORMS

Contract Manager Form

REQUEST FOR QUOTATION
West Virginia Lottery
Network Penetration Testing and Cybersecurity Assessments

10.2. The following remedies shall be available to Agency upon default.

10.2.1. Immediate cancellation of the Contract.

10.2.2. Immediate cancellation of one or more release orders issued under this Contract.

10.2.3. Any other remedies available in law or equity.

11. MISCELLANEOUS:

11.1. Contract Manager: During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager: Patrick Swere
Telephone Number: 877.578.0215 ext. 118
Fax Number: None.
Email Address: pswere@securanceconsulting.com

REQUIRED FORMS

Exhibit B

EXHIBIT B NON-DISCLOSURE AGREEMENT (NDA)

MUTUAL NON-DISCLOSURE AGREEMENT

This Mutual Non-Disclosure Agreement (“Agreement”) is entered into by and between the West Virginia Lottery, with its principal offices located at 900 Pennsylvania Avenue Charleston, WV 25302 (“Lottery”), and Securance LLC, with its principal offices located at 13916 Monroes Business Park, Suite 102, Tampa, FL 33635 (“Party of the second part”), with an Effective Date of 3.21.24. Lottery and Party of the second party also are referred to herein individually as a “party”, or collectively as the “parties”.

WHEREAS, the parties to this Agreement may wish to exchange certain information related to the provision of certain information or communication technology services by one party of interest to the other party; and

WHEREAS, the parties agree that improper disclosure of either party’s Confidential Information, as defined below, by the other party could cause material harm to the party whose Confidential Information was improperly disclosed;

NOW THEREFORE, in order to protect certain Confidential Information that may be disclosed between the parties, Lottery and Alpha agree to maintain the confidentiality of the Confidential Information as follows:

I. Definition of Confidential Information. The “Confidential Information” disclosed under this Agreement is defined as follows:

Any data or information that is proprietary to the disclosing party and not generally known to the public, whether in tangible or intangible form, whenever and however disclosed, including, but not limited to: (i) any marketing strategies, plans, financial information, or projections, operations, sales estimates, business plans and performance results relating to the past, present or future business activities of such party, its affiliates, subsidiaries and affiliated companies; (ii) plans for products or services, and customer or supplier lists; (iii) any scientific or technical information, invention, design, process, procedure, formula, improvement, technology or method; (iv) any concepts, reports, data, know-how, works-in-progress, designs, development tools, specifications, computer software, source code, object code, flow charts, databases, inventions, intellectual property, and trade secrets; (v) solicitation for proposals, responses to proposals, bids, or information disclosed in connection with such solicitation, response, or bid; (vi) any other information that should reasonably be recognized as confidential information of the disclosing party.

II. Disclosure Period and Term. This Agreement protects against the disclosure of Confidential Information which is disclosed between the parties during each party’s performance of its obligations associated with that certain CRFQ Agreement executed between the parties on _____ (the “Effective Date”) and 3 year(s) after the termination of such Agreement (“Disclosure Period”). Therefore, the duty of a recipient of Confidential Information to protect such Confidential Information disclosed under this Agreement begins on the Effective Date and expires 3 year(s) after the end of Disclosure



REQUIRED FORMS

Exhibit B (cont.)

EXHIBIT B NON-DISCLOSURE AGREEMENT (NDA)

Period. Upon termination of this Agreement or upon the disclosing party's request, the recipient shall cease use of Confidential Information and return or destroy it.

- III. Use of Confidential Information.** A party hereunder receiving Confidential Information shall use such Confidential Information solely for the purposes of, as applicable to the recipient, understanding current business activities of a party, soliciting a proposal for certain information technology services, responding to such proposal solicitation, reviewing solicitation responses, tendering a bid, or discussions or negotiations related to such solicitation, proposal, or bid.
- IV. Protection of Confidential Information.** Each party shall not disclose the Confidential Information of the other party to any third party. The recipient shall protect the Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination or publication of the Confidential Information as the recipient uses to protect its own confidential information of a like nature. A recipient shall restrict disclosure of Confidential Information to its employees, provided that such employees (i) have a need to know, and (ii) are bound by obligations of confidentiality equally as restrictive as the terms of this Agreement.
- V. Exclusions.** This Agreement imposes no obligation upon the recipient with respect to Confidential Information which: (a) was in the recipient's possession before receipt from the disclosing party; (b) is or becomes a matter of public knowledge through no fault of the recipient; (c) is rightfully received by the recipient from a third party without a duty of confidentiality; (d) is disclosed by the disclosing party to a third party without a duty of confidentiality on the third party; (e) is independently developed by the recipient; (f) is disclosed under operation of law; or (g) is disclosed by the recipient with the disclosing party's prior written approval.
- VI. Miscellaneous.** Neither party to this Agreement shall acquire any intellectual property rights nor any other rights under this Agreement except the limited right to use as set forth in this Agreement. This Agreement does not prevent either Party from competing with one another for work or clients unless the parties specifically agree otherwise, in writing, as to a specific client. Each disclosing party warrants and represents that the Confidential Information and other information provided which is necessary to the purposes described hereunder, are true and correct to the best of the disclosing party's knowledge and belief. Nothing in this Agreement shall be construed to preclude either party from developing, using, marketing, licensing, and/or selling any software or other material that is developed without reference to the Confidential Information.
- VII. Export Administration.** Each party to this Agreement agrees to comply fully with all relevant export laws and regulations of the United States and other countries to assure that no Confidential Information or any portion thereof is exported, directly or indirectly, in violation of such laws.
- VIII. No Obligation to Purchase or Offer Products or Services.** Neither party has an obligation under this Agreement to purchase or otherwise acquire any service or item from

REQUIRED FORMS

Exhibit B (cont.)

**EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)**

the other party. Neither party has an obligation under this Agreement to commercially offer any products using or incorporating the Confidential Information. The disclosing party may, at its sole discretion, offer such products commercially and may modify them or discontinue such offerings at any time.

IX. General. The parties do not intend that any agency or partnership relationship be created between them by this Agreement. This Agreement sets forth the entire agreement with respect to the Confidential Information disclosed herein and supersedes all prior or contemporaneous agreements concerning such Confidential Information, whether written or oral. All additions or modifications to this Agreement must be made in writing and must be signed by both parties. This Agreement and all matters arising out of or relating to this Agreement shall be governed by the laws of the State of West Virginia. The parties agree that the information provided as allowed by this Agreement will not contain any proprietary technical or confidential contractual information, or any financial information related to the relationship between Alpha and its partners. As a result, damages will not be included as a remedy.

The undersigned authorized representatives of each party have agreed to be legally bound by the terms of this Agreement as of the Effective Date shown above.

WEST VIRGINIA LOTTERY

By: _____

Name: _____

Title: _____

Securance LLC _____ **(VENDOR)**

By:  _____

Name: Paul Ashe _____

Title: President _____



REQUIRED FORMS

Addendum Acknowledgment Form

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: LOT240000009

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Securance LLC

 Company

Authorized Signature

3.22.24

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

REQUIRED FORMS

Background Check Agreement

Securance agrees to provide names, addresses, and fingerprint information for a law enforcement background check for any staff working on the The Lottery project team.



APPENDIX: SAMPLE REPORT



ABC TREASURY

Date: June 26, 2023

Cybersecurity Assessment



www.securanceconsulting.com

VERSION MANAGEMENT

VERSION	DATE APPROVED	APPROVED BY	BRIEF DESCRIPTION
1.0.0	June 7, 2023	Securance	Initial Draft
FINAL	June 26, 2023	Securance	Final Report

This report is intended solely for the management of ABC Treasury for its internal use and is not intended to, nor may, be relied upon by any other party ("Third Party"). Neither this deliverable nor its contents may be distributed to, discussed with, or otherwise disclosed to any Third Party without the prior written permission of Securance Consulting. Securance Consulting accepts no liability or responsibility to any Third Party that gains access to this report. © 2023 Securance LLC.

TABLE OF CONTENTS

SECTION I: EXECUTIVE SUMMARY

Background, Objectives, and Scope.....	4
Findings and Technical Vulnerability Legend.....	5
Summary of Findings	6
Conclusion	9

SECTION II: CYBERSECURITY ASSESSMENT REPORT

Background.....	10
Specific Objectives and Detailed Scope.....	10
Approach and Methodology.....	11
Findings and Recommendations	14

SECTION III: SECURANCE VALUE

Securance Value	24
-----------------------	----

APPENDIX A

Technician's Report(s).....	25
-----------------------------	----

EXECUTIVE SUMMARY

BACKGROUND

Client background has been redacted. The technologies and applications that support ABC Treasury (ABC) are critical and must be properly secured. In June 2023, Securance Consulting conducted a cybersecurity assessment for ABC.

SPECIFIC OBJECTIVES AND SCOPE

The objective of the review was to identify risks and vulnerabilities in ABC's technologies. The scope of our testing included the following components:

1. External network vulnerability assessment and penetration testing
2. Internal network vulnerability assessment and penetration testing
3. Assessments of the following web applications:

- <https://www.webapp-1.net>
- <https://www.webapp-2.net>
- <https://www.webapp-3.net>
- <https://www.webapp-4.net>
- <https://www.webapp-5.net>
- <https://www.webapp-6.net>
- <https://www.webapp-7.net>
- <https://www.webapp-8.net>
- <https://www.webapp-9.net>

4. Social engineering, including:
 - Email phishing
 - Vishing
 - Physical security testing at the following locations:
 - 123 Any Street, Any City, ZZ 12345
 - 456 Same Avenue, Same City, ZZ 54321

APPROACH AND METHODOLOGY

We based our approach on our proven methodologies to ensure a comprehensive assessment. This approach included the following activities:

- Review of IT policies, procedures, and standards.
- Interviews with IT management and personnel.

Provided for: ABC Treasury

Securance Consulting

- Review of collected evidence and testing of relevant IT operations and processes.
- Use of commercial security tools and manual testing techniques.

The review was limited to the areas we considered necessary to complete the assessment and was not intended to cover ABC's entire information systems function.

Remainder of page left blank intentionally.

FINDING LEGEND:



Urgent-Risk (Level 5) – Immediate remediation required.

Note: If finding is a technical vulnerability, it provides remote intruders with remote root or remote administrator capabilities.



Critical-Risk (Level 4) – Immediate action recommended, with remediation ASAP.

Note: If finding is a technical vulnerability, it provides intruders with remote user, but not remote administrator or root user, capabilities.



High-Risk (Level 3) – Immediate action recommended, with remediation in 90 days.

Note: If finding is a technical vulnerability, it provides hackers with access to specific information, including security settings, stored on the ABC. This level of vulnerabilities could result in potential misuse of the ABC by intruders.



Medium-Risk (Level 2) – Action recommended, with remediation in 180 days.

Note: If finding is a technical vulnerability, it may expose sensitive information, such as precise versions of services, from the ABC. With this information, hackers could research potential attacks to try against ABC.



Low-Risk/Informational (Level 1) – Effective control. No immediate changes recommended. Opportunity for slight improvement.



Advisory Comment – Action suggested at the discretion of management.

Note: Remediation timeframes are based on best practices and Securance's experience.

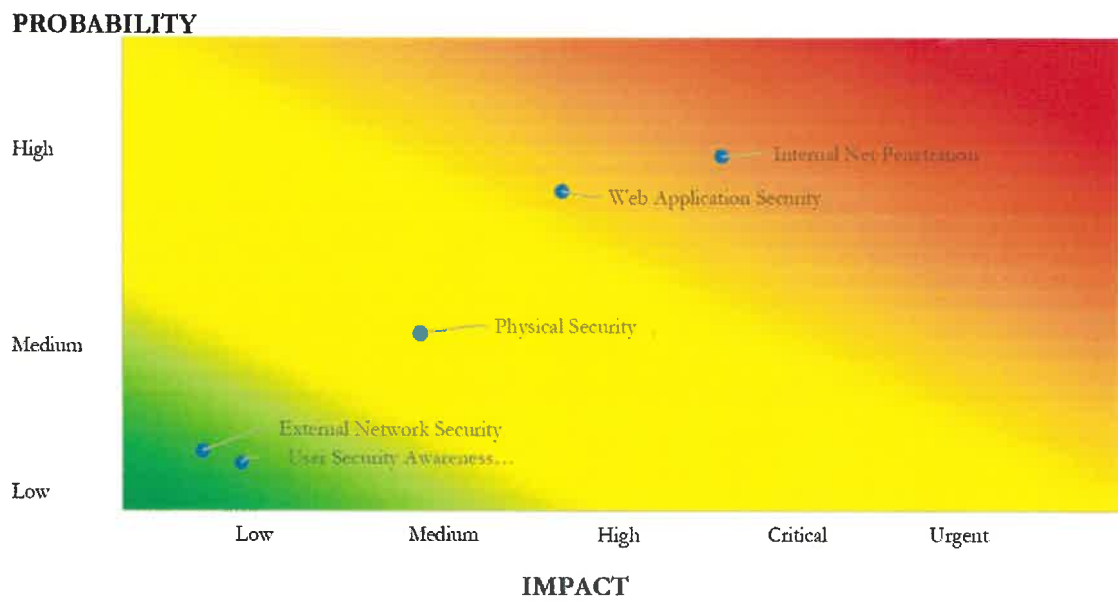
SUMMARY OF FINDINGS

The following section summarizes our findings from the cybersecurity assessment.

NO.	FINDING TITLE	5 URGENT	4 CRITICAL	3 HIGH	2 MEDIUM	1 LOW	A ADVISORY
1	Internal Network Vulnerability Assessment and Penetration Test		✓				
2	Web Application Vulnerability Assessment			✓			
3	Physical Security of Geographic Perimeter and Facilities				✓		
4	External Network Vulnerability Assessment					✓	
5	End-User Security Awareness Training					✓	
6	External Network Public Information						✓
Total Findings:		0	1	1	0	2	1

Remainder of page left blank intentionally.

ABC's CYBERSECURITY ASSESSMENT HEAT MAP





No. 1: Internal Network Vulnerability Assessment and Penetration Test – we scanned ABC’s internal network and identified three critical-, three high-, and 10 medium-priority unique vulnerabilities, excluding vulnerabilities in the Secure Socket Layer (SSL) protocol family. The scan results revealed vulnerabilities that increase the likelihood of an internal network breach. We also performed exploit testing and successfully breached two hosts.



No. 2: Web Application Vulnerability Assessment – we performed a detailed security assessment of several Internet-facing web applications. Based on our testing, all the tested web applications are at a low risk of being compromised, except for abcbank.gov, which we believe is at a high risk of being compromised because of its current configuration.



No. 3: Physical Security of Geographic Perimeter and Facilities – we assessed physical security at the following locations and identified a few opportunities for improvement:

- 123 Any Street, Any City, ZZ 12345
- 456 Same Avenue, Same City, ZZ 54321

CONCLUSION

Based on the procedures we performed, our knowledge of ABC’s computing environment, and our IT security experience, it is our opinion that there are opportunities to improve ABC’s IT security and internal controls. However, we also recognize that ABC’s CISO and IT management understands the importance of, and strives for, security and control across the computing environment.

We recommend that ABC review and implement our recommendations to improve security and process controls. The remainder of this report provides a detailed analysis of our approach and methodology, the risks and vulnerabilities we identified, and detailed mitigation recommendations.

Remainder of page left blank intentionally.

CYBERSECURITY ASSESSMENT REPORT

BACKGROUND

Client background has been redacted. The technologies and applications that support ABC are critical and must be properly secured. In June 2023, Securance Consulting conducted a cybersecurity assessment for ABC.

SPECIFIC OBJECTIVES AND SCOPE

The objective of the review was to identify risks and vulnerabilities in ABC's technologies. The scope of the review included the following:

1. External network subnets XXX.XX.XXX.XXX/XX, XX.XX.XXX.XXX/XX, and XXX.XXX.XX.XX/XX.
2. Internal network subnets, including:
 - XX.X.X.X/XX
 - XX.X.XX.X/XX
 - XX.X.XX.X/XX
 - XX.X.XX.X/XX
 - XX.X.XX.X/XX
 - XX.X.XX.X/XX
 - XX.X.XX.X/XX
 - XX.X.XX.X/XX
 - XX.X.XX.X/XX
 - XX.X.XX.X/XX
 - XX.X.XXX.X/XX
 - XX.X.XXX.X/XX
 - XX.X.XXX.X/XX
 - XX.X.XXX.X/XX
 - XX.X.XXX.X/XX
 - XX.X.XXX.X/XX
 - XX.X.XXX.X/XX
 - XX.X.XXX.X/XX
 - XX.X.XXX.X/XX
 - XXX.XXX.XXX.X/XX
 - XXX.XXX.XXX.X/XX
 - XXX.XXX.XXX.X/XX
 - XXX.XXX.XXX.X/XX
 - XXX.XXX.XXX.X/XX
 - XXX.XXX.XXX.X/XX
 - XXX.XXX.XXX.X/XX
3. Testing of the following web applications:
 - <https://www.webapp-1.net>
 - <https://www.webapp-2.net>
 - <https://www.webapp-3.net>
 - <https://www.webapp-4.net>
 - <https://www.webapp-5.net> – per IT staff, no longer used
 - <https://www.webapp-6.net>
 - <https://www.webapp-7.net>
 - <https://www.webapp-8.net>
 - <https://www.webapp-9.net>

- 4. Social engineering, including:
 - Email phishing – 139 users tested
 - Vishing – 139 users tested
 - Physical security testing at the following locations:
 - 123 Any Street, Any City, ZZ 12345
 - 456 Same Avenue, Same City, ZZ 54321

APPROACH AND METHODOLOGY

To achieve the ABC’s objectives, we relied on our proven assessment methodologies, summarized below:

EXTERNAL AND INTERNAL NETWORK TESTING

We used discovery, vulnerability assessment, and penetration testing procedures, listed below, to identify weaknesses in IP network services:

- Internet Discovery – using public tools, manual tasks, publicly available information, and information from ABC’s IT management, we created a profile of computer addresses and other information about ABC’s external and internal networks.
- External and Internal Network IP Scans – using Nmap and Nessus Professional vulnerability scanner, we scanned the approved ranges of external and internal IP addresses. We configured scanning policies that minimized disruption to ABC’s external and internal network systems and devices. This included disabling denial of service and brute force attack attempts.
- False Positive Identification – we analyzed the results and, based on our knowledge and information from the scans, attempted to identify and remove all false-positive vulnerabilities.
- Penetration Testing – we attempted to exploit select vulnerabilities on the internal network and gain access to system resources.

WEB APPLICATION TESTING

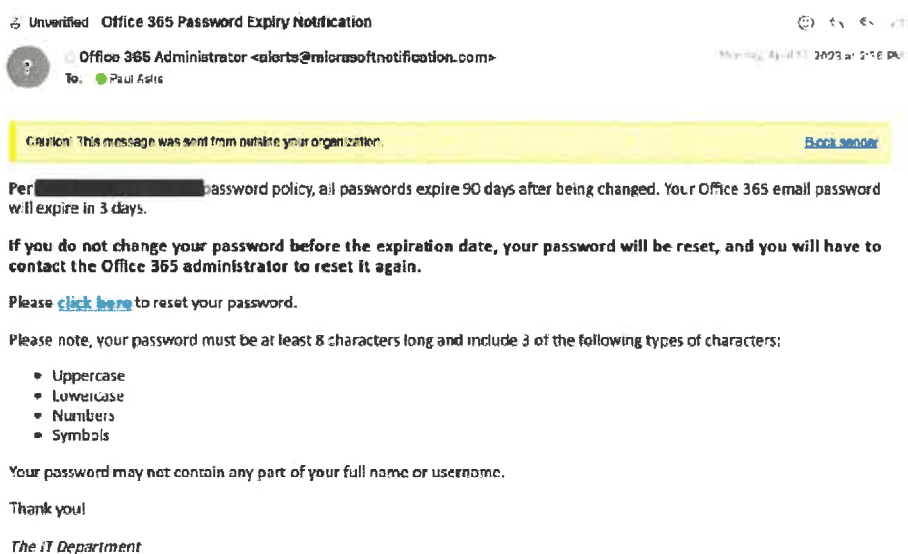
Using Nmap, a commercial port scanner, and nStalker, a commercial web-application security testing tool, we tested the web applications for vulnerabilities in the following attack categories:

- | | | | |
|----------------------------|-------------------------------|------------------------|------------------------------|
| • Cross-site Scripting | • PHP File Include | • Buffer Overflow | • Microsoft CGI Attacks |
| • SQL Injection | • Parameter Deletion | • Format String | • CGI Attacks |
| • Remote Execution | • Special Parameter Addition | • Integer Overflow | • Microsoft IIS Attacks |
| • Directory/File Traversal | • Boolean Parameter Tampering | • Information Exposure | • Common HTTP Device Attacks |
| • CRLF Injection | • Blind SQL Injection | • Generic HTTP Attacks | |

SOCIAL ENGINEERING

Securance designed phishing campaigns to test the effectiveness of internal user security awareness training.

- Email phishing is a technique in which the perpetrator sends out legitimate-looking emails to solicit the recipient to respond with confidential, and often sensitive, data, such as a username, password, or social security number.



- Vishing is the practice of making phone calls or leaving voice messages, purporting to be from reputable companies, to induce individuals to reveal personal information, such as bank details and credit card numbers. We used the following message in our automated vishing calls to ABC employees:

This is an automated call from your organization to inform you that we are crediting a small amount required to set up a desk for work at home to your account. To register, Press 1.

1: Please enter your salary bank account number, followed by #.

2: Please enter your registered phone number with the organization, followed by #.

To receive complete details by email, Press 2.

To listen to the options again, Press 3.

End: Thank you for the confirmation.

- Physical security assessments are used to determine whether an unauthorized person can enter an organization's facilities to access sensitive information and internal systems.

The review was limited to the areas we considered necessary to complete the assessment and was not intended to cover ABC's entire information systems function.

Remainder of page left blank intentionally.

FINDINGS AND RECOMMENDATIONS

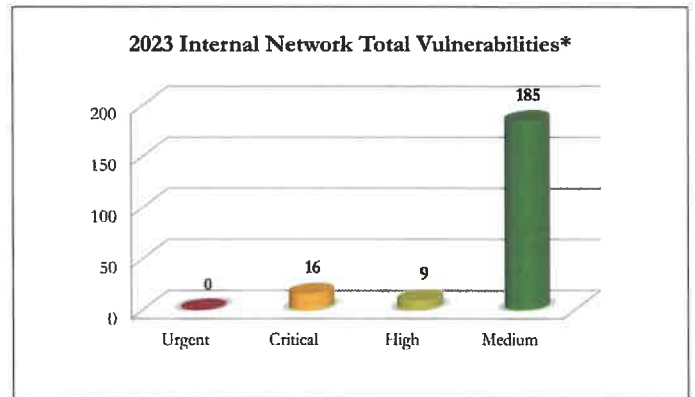
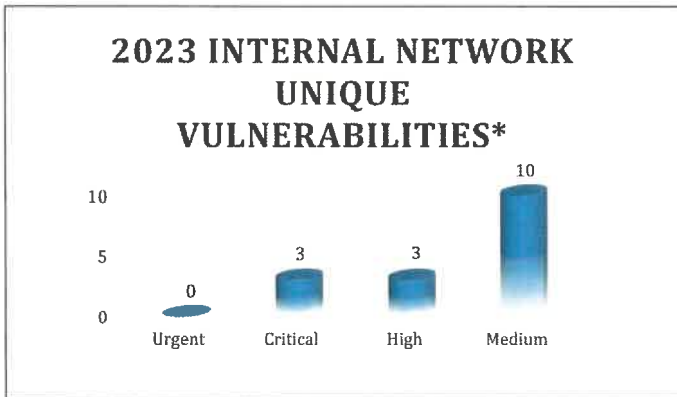
The following recommendations, based on our cybersecurity assessment and technical testing, are intended to improve the security and control of ABC's IT environment.



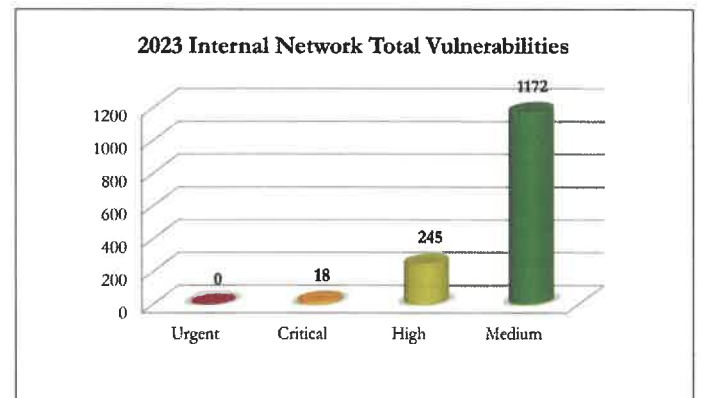
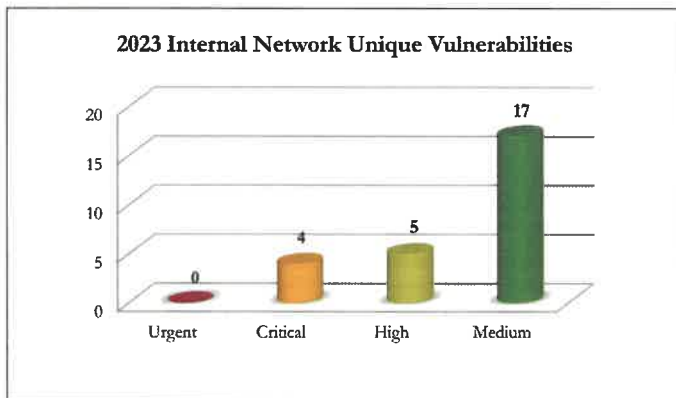
No. 1: Internal Network Vulnerability Assessment and Penetration Test

We scanned ABC's internal network and identified three critical-, three high-, and 10 medium-priority unique vulnerabilities, excluding vulnerabilities in the Secure Socket Layer (SSL) protocol family. The scan results revealed vulnerabilities that increase the likelihood of an internal network breach.

The charts below show the vulnerabilities we identified, prioritized by level of severity, as defined by the Common Vulnerability Scoring System, Version 3.0 (CVSS v3.0). The technician's report summarizes the unique vulnerabilities, affected systems, and recommended solutions. In many cases, the recommended solution requires a system security patch.



*Excluding SSL and transport layer security (TLS) vulnerabilities.



Securance analyzed the results of the internal vulnerability assessment to determine an effective penetration testing plan. We identified hosts and systems to target during the penetration test. We presented the results to ABC’s CISO, who approved penetration testing of the following systems.

HOSTNAME IP	VULNERABILITY SUMMARY	EXPLOIT RESULTS
<ul style="list-style-type: none"> XXX.XX.XX.XXX 	Axis Network Camera .srv to Parhand RCE	Success: Root access gained. Files written to system.
<ul style="list-style-type: none"> abcxx.treasury.local (XX.X.XX.XX) abcxxxx.treasury.local (XX.X.X.XX) 	SMB Signing Not Required	Exploit attempts were unsuccessful.

No. 1: Internal Network Penetration Test continued

HOSTNAME IP	VULNERABILITY SUMMARY	EXPLOIT RESULTS
<ul style="list-style-type: none">abcxxautomate.treasury.local (XX.X.XX.XX)	Tomcat Vulnerability	Success: Webserver information retrieved. Variable payloads could lead to retrieval of additional information.

While our exploits targeting the four hosts listed above were not fully successful, it is worth noting the following:

- We identified 16 hosts with three unique critical vulnerabilities and nine hosts with three unique high vulnerabilities.
- A bad actor would not request approval to attempt exploits, would have unlimited time to deploy advanced persistent threat techniques, and might experience success. The details of our penetration testing efforts are in the technician’s report.

Potential Risk:

As a result of our testing, we believe that ABC’s internal network is at a moderate to high risk of being compromised by an attacker. If a breach were to occur, depending on the type of breach, systems could be rendered unresponsive, and data could be compromised.

Recommendation:

We recommend that ABC’s IT staff review the vulnerabilities identified and address the critical-, high-, and medium-priority vulnerabilities associated with systems that meet the following criteria:

- The system is maintained by ABC’s IT staff.
- Applying the recommended patch will not disrupt the other technologies that the system supports.
- The system is neither a target for replacement nor a part of the legacy server plan.

Vulnerability details are provided in a separate technician’s report. Low-risk vulnerabilities and informational disclosures are only provided in the technician’s report. A finding and technical vulnerability legend is provided on page 5.



No. 2: Web Application Vulnerability Assessment

We performed a detailed security assessment of the following Internet-facing web applications:

- <https://www.webapp-1.net>
- <https://www.webapp-2.net>
- <https://www.webapp-3.net>
- <https://www.webapp-4.net>
- <https://www.webapp-5.net> – per IT staff, no longer used
- <https://www.webapp-6.net>
- <https://www.webapp-7.net>
- <https://www.webapp-8.net>
- <https://www.webapp-9.net>

All of the web applications we tested are at a low risk of being compromised, except for abctreasury.gov, which we believe is at a high risk of being compromised because of its current configuration. Refer to Appendix A for a summary of the technical vulnerabilities.

Potential Risk:

In the event of a successful attack, depending on the type of attack, one or more web applications could be rendered unresponsive, or data could be compromised.

Recommendation:

Notwithstanding the layered defenses protecting ABC's Internet-facing applications, we recommend that IT management address the high- and medium-risk vulnerabilities identified in Appendix A.



No. 3: Physical Security of Geographic Perimeter and Facilities

We assessed physical security at the following locations:

- 123 Any Street, Any City, ZZ 12345
- 456 Same Avenue, Same City, ZZ 54321

The results of our assessment are below:

123 Any Street, Any City, ZZ 12345

- There is no security guard, but drive-bys are performed nightly and recorded.
- All entrances and exits to the building are locked.
- A Lenel key card access system is installed and managed.
- Physical keys are limited to appropriate personnel.
- Security cameras are installed both inside and outside of the building. However, there is no video surveillance policy to govern administration and management of the security camera system.
- A receptionist is stationed at the front desk during business hours. Visitors are logged and must be escorted. However, physical tailgating is possible, as the receptionist is not always at the desk.
- There are open and enabled network ports throughout the building. However, Cisco Identity Services Engine (ISE) is being implemented.

456 Same Avenue, Same City, ZZ 54321

- There is no security guard, and drive-bys are not performed.
- All entrances and exits to the building are locked.
- A Lenel key card access system is installed and managed.
- Physical keys are limited to appropriate personnel. Security cameras are installed both inside and outside of the building. However, there is no video surveillance policy to govern administration and management of the security camera system.
- A receptionist is stationed at the front desk during business hours. Visitors are logged and must be escorted. However, physical tailgating is possible, as the receptionist is not always at the desk.

No. 3: Physical Security of Geographic Perimeter and Facilities continued

- There are open and enabled network ports throughout the building. However, Cisco ISE is being implemented.

Potential Risk:

Perimeter security measures can deter, delay, and detect unwanted intrusions. Absent effective perimeter security, an organization must rely on other security measures that, if reliant on humans, are not failproof. If all perimeter security defenses fail, an intruder could access a controlled area.

Recommendation:

We recommend that ABC facilities and IT management consider implementing the following to improve physical security:

- Implement a security surveillance policy.
- Enable port security so that accessible ports are not automatically enabled.
- Continue with the implementation of Cisco ISE.
- Periodically review visitor logs and document the review.
- Implement a process to back up the receptionist, so that the front desk is never left without a staff member to monitor who enters and exits the facility.

Remainder of page left blank intentionally.



No. 4: External Network Vulnerability Assessment

We scanned ABC's external network and identified one medium-priority unique vulnerability. The scan results did not reveal vulnerabilities that increase the likelihood of an external network breach. We did not attempt to exploit the vulnerability.

The charts on the following page show the vulnerabilities we identified, prioritized by level of severity, as defined by CVSS v3.0. Refer to the technician's report for the details of the unique vulnerabilities, affected systems, and recommended solutions. In several cases, the recommended solution requires a system security patch.

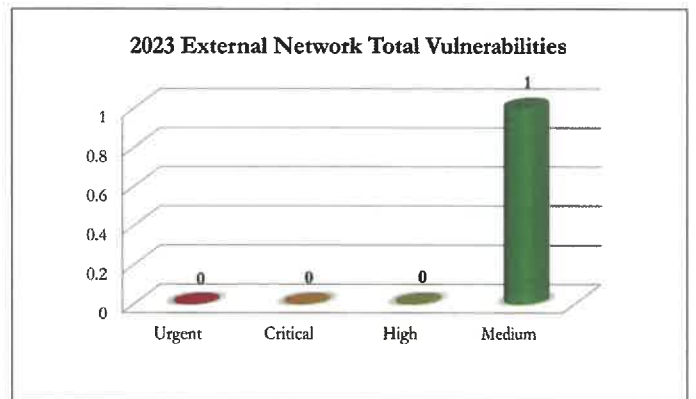
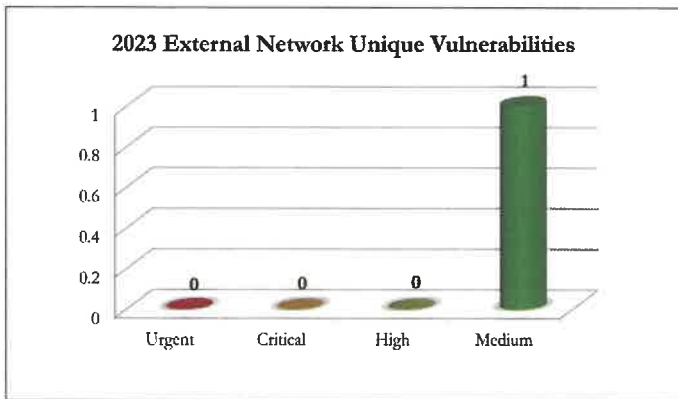
Potential Risk:

As a result of our testing, we believe that ABC's external network is at a low risk of being compromised by an attacker. If a breach were to occur, depending on the type of breach, systems could be rendered unresponsive, data could be compromised, or segments of the network could be used to breach internal systems.

Recommendation:

We commend ABC's IT staff for effectively managing the technical vulnerabilities associated with ABC's Internet-facing technologies, excluding web-applications. We recommend that the current process of managing technical vulnerabilities continue, as the threat landscape continually changes.

Vulnerability details are provided in a separate technician's report. A finding and technical vulnerability legend is provided on page 5.



Remainder of page left blank intentionally.



No. 5: End-User Security Awareness Training

We performed social engineering to assess ABC employees’ level of security awareness. Our procedures, designed to persuade employees to provide access credentials, are summarized below. The results indicate that ABC’s end users are aware of their responsibility to protect the organization’s technology assets.

2023 SOCIAL ENGINEERING RESULTS	PHISHING	VISHING
Summary Results:		
• Number of Users Targeted	139	139
• Emails Opened Calls Answered	13	139
• Link Clicked	2	N/A
• User Registrations Credentials Entered	1	0

Potential Risk:

End-user security awareness training is a critical component of enterprise information system security. If users are not taught the importance of information system security, they may provide an attacker system credentials (i.e., usernames and passwords) that could be used to breach the network. Depending on the type of breach and the attacker’s objectives, the network or an application could be compromised. In addition, if the attacker uses valid credentials, it may appear that an authorized employee caused the attack.

Recommendation:

We commend ABC for training its employees about their role in protecting the organization’s technology assets. We recommend continued end-user training.



No. 6: External Network Public Information

We searched for publicly available information about ABC's Internet-facing (external) network and found that the American Registry for Internet Numbers (ARIN) identifies subnet XX.XX.XXX.XXX as registered to EPIC. Subnets XX.XX.XXX.XX/XX and XXX.XXX.XX.XX/XX are registered to ABC. The registry information for all subnets is appropriately sanitized to minimize unnecessary sharing of information, such as names and email addresses.

We also searched the "surface web," social media sites (Glassdoor, Facebook, Instagram, YouTube, Twitter, and LinkedIn), and the "dark web" (i.e., .onion), using the TOR browser and multiple sites (ahmia.fi, The Hidden Wiki, TORCH, and Candle), but did not find additional information about ABC's Internet-facing network.

Potential Risk:

Public information about an organization's Internet-facing network is both unnecessary and an entry point for attackers.

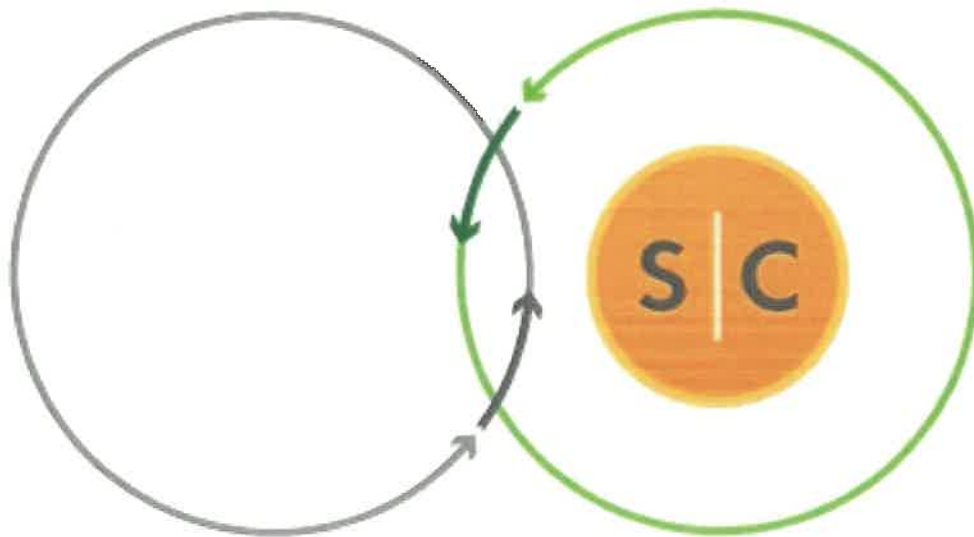
Recommendation:

We commend ABC's cybersecurity office for ensuring the organization's IP registrations are sanitized. We recommend that ABC periodically review IP address registrations, the surface web, and the dark web to ensure all available information remains properly sanitized.

SECURANCE VALUE

Securance Consulting would like to **THANK YOU** for your business. Aside from benefiting from the highest level of service possible, you also received unique advantages that only Securance Consulting delivers. Our hands-on approach is tailored to fit the needs of the IT department and your technology environment. Our technical expertise, outstanding reputation, and personalized attention ensure you receive a level of service surpassed by no other technology risk management firm in the market.

As a Securance customer, you can be confident in your sound decision to manage your technology risk through a co-sourced relationship with Securance!



APPENDIX A: TECHNICAL VULNERABILITY SUMMARIES

NO. 18: WEB APPLICATION VULNERABILITY ASSESSMENT AND PENETRATION TESTING

THREAT LEVEL	WEB APP	VULNERABILITY FAMILY	FIX RECOMMENDATION
High	<ul style="list-style-type: none"> brsftp.abc.state* ftp.abc.treas* abcbanking.state* 	Found Support for Weak Ciphers in SSL/TLS Communication	Disable weak ciphers.
High	<ul style="list-style-type: none"> abcbanking.state* 	Webserver Vulnerable to MiTM Attack (BEAST)	Implement strong ciphers in the webserver's cipher list.
High	<ul style="list-style-type: none"> abcbanking.state* 	Vulnerable to SSLv3 POODLE Attack	Disable SSLv3.
High	<ul style="list-style-type: none"> brsftp.abc.state* ftp.abc.state* 	Possible Blind SQL Injection Fault Found	Possible False Positive: Sanitize all user input.
Medium	<ul style="list-style-type: none"> brsftp.abc.state* fs.abc.state ftp.abc.state* bondtracker** portal.abc.state** 	Application Appears Susceptible to Clickjacking Attacks	Add the following HTTP header to your server's response: X-FRAME-OPTIONS: DENY or X-FRAME-OPTIONS: SAMEORIGIN (if you want to allow it only under the same domain context).
Medium	<ul style="list-style-type: none"> bondtracker brsftp.abc.state* ftp.abc.state* abcdportal portal.abc.state* 	Found an Insecure Cookie for Scripting (no HttpOnly Enabled)	Enable HttpOnly according to your web platform instructions.
Medium	<ul style="list-style-type: none"> abcbanking.state* 	Found Support for RC4 in SSL/TLS Cipher Suites	Reconfigure your webserver and consider using TLSv1.2.
Medium	<ul style="list-style-type: none"> brsftp.abc.state* ftp.abc.state* abcbanking.state* 	Webserver is Vulnerable to Attacks on 64-bit Block Ciphers in TLS and OpenVPN (Sweet32 Attack)	Weak ciphers, such as RC4, DES, 3DES, etc., should be disabled in SSL configuration.

THREAT LEVEL	WEB APP	VULNERABILITY FAMILY	FIX RECOMMENDATION
Medium	<ul style="list-style-type: none"> • bondtracker* • abcpfapp.state* • abcpfd.state* 	Found an Invalid SSL Certificate	Obtain a valid certificate.
Medium	<ul style="list-style-type: none"> • brsftp.abc.state • ftp.abc.state 	Possible Backup File Found	Remove all backup files from the webserver.
Medium	<ul style="list-style-type: none"> • brsftp.abc.state* • fs.abc.state • ftp.abc.state* • abcbanking.state* 	Multiple Cross-Site Request Forgery Vulnerability Found	MABC prevention techniques work by embedding additional authentication data into requests that allows the web application to detect requests from unauthorized locations.
Medium	<ul style="list-style-type: none"> • ftp.abc.state 	Possible HTTP Parameter Pollution Vulnerability Has Been Found	Sanitize user's input.
Medium	<ul style="list-style-type: none"> • abcbanking.state* 	Web Form Allows Password Caching (Autocomplete = on)	Disable autocomplete.

*Privileged and Unprivileged | **Privileged Only



External VA

TABLE OF CONTENTS

Vulnerabilities by Host

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

- Suggested Remediations

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)



0

CRITICAL

0

HIGH

0

MEDIUM

0

LOW

2

INFO

Scan Information

Start time: Mon Dec 4 14:05:12 2023

End time: Mon Dec 4 14:17:53 2023

Host Information

IP:



Vulnerabilities

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS v2.0 Base Score

0.0 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

icmp/0

The difference between the local and remote clocks is 1 second.

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

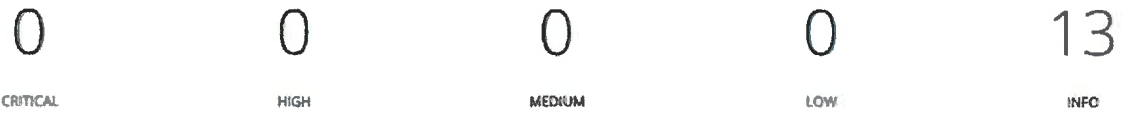
Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

tcp/0

Information about this scan :

Nessus version : 10.0.2
Nessus build : 20291
Plugin feed version : 202311281630
Scanner edition used : Nessus
Scanner OS : DARWIN
Scanner distribution : macosx
Scan type : Normal
Scan name : ██████████
Scan policy used : BASIC Network Scan
Scanner IP : ██████████
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : ██████████
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/12/4 14:05 CST
Scan duration : 752 sec
Scan for malware : no



Scan Information

Start time: Mon Dec 4 14:05:13 2023
End time: Mon Dec 4 14:27:19 2023

Host Information

IP: ██████████
OS: Linux Kernel 2.6

Vulnerabilities

105160 - AXIS Web Interface Detection

Synopsis

The web interface for an AXIS device was detected on the remote host.

Description

Nessus was able to detect the web interface for an AXIS device on the remote host.

See Also

<https://www.axis.com/en-us>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/12/12, Modified: 2023/11/20

Plugin Output

tcp/80/www

```
URL : ██████████
Version : 6.53.4
confidence : 100
model : M5054
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>
<https://nvd.nist.gov/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2023/10/16

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel -> Linux Kernel

Following hardware CPE matched on the remote system :

x-cpe:/h:axis:network_camera:6.53.4

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 65
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.0 200 OK
```

```
Protocol version : HTTP/1.0
```

```
SSL : no
```

```
Keep-Alive : no
```

```
Options allowed : (Not implemented)
```

Headers :

Content-Length: 1127
Cache-Control: no-cache no-store
Content-Type: text/html

Response Body :

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta http-equiv="Expires" content="Tue, 12 May 1962 1:00:00 GMT" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Cache-Control" content="no-cache" />
<meta http-equiv="Content-type" content="text/html; charset=iso-8859-1" />
<meta http-equiv="Content-language" content="en" />

<script>
var refreshUrl = "/view/view.shtml?id=224731";
var questMark = refreshUrl.indexOf('?') < 0 ? "?" : "&";
var imagePath = "/mjpg/video.mjpg";

var completePath = "imagepath=" + encodeURIComponent(imagepath) + "&size=1";

if (refreshUrl.indexOf("view.shtml") >= 0) {
window.location.href = refreshUrl + questMark + completePath;
}
else {
window.location.href = refreshUrl;
}
</script>
<title>Index page</title>
<noscript>
Your browser has JavaScript turned off.<br>For the user interface to work, you must enable JavaScript in your browser
and reload/refresh this page.
</noscript>
</head>
<body>
</body>
</html>
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/80/www

Port 80/tcp was found to be open

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/554

Port 554/tcp was found to be open

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

tcp/0

Information about this scan :

Nessus version : 10.0.2
Nessus build : 20291

Plugin feed version : 202311281630
Scanner edition used : Nessus
Scanner OS : DARWIN
Scanner distribution : macosx
Scan type : Normal
Scan name : ██████████
Scan policy used : Basic Network Scan
Scanner IP : ██████████
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : ██████████
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/12/4 14:05 CST
Scan duration : 1302 sec
Scan for malware : no

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

Plugin Output

tcp/0

Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP

The remote host is running Linux Kernel 2.6

10762 - RTSP Server Type / Version Detection

Synopsis

An RTSP (Real Time Streaming Protocol) server is listening on the remote port.

Description

The remote server is an RTSP server. RTSP is a client-server multimedia presentation protocol, which is used to stream videos and audio files over an IP network.

It is usually possible to obtain the list of capabilities and the server name of the remote RTSP server by sending an OPTIONS request.

See Also

<https://en.wikipedia.org/wiki/Rtsp>

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 2001/09/14, Modified: 2019/11/22

Plugin Output

tcp/554

```
Server Type : GStreamer RTSP server
```

```
The remote RSTP server responds to an 'OPTIONS *' request as follows :
```

```
----- snip -----  
CSeq: 1  
Public: OPTIONS, DESCRIBE, GET_PARAMETER, PAUSE, PLAY, SETUP, SET_PARAMETER, TEARDOWN  
Server: GStreamer RTSP server  
Date: Mon, 04 Dec 2023 19:53:07 GMT
```

```
----- snip -----
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

25220 - TCP/IP Timestamps Supported

Synopsis

An error was detected along the way.
An error was detected along the way.
An error was detected along the way.
An error was detected along the way.
An error was detected along the way.
An error was detected along the way.
An error was detected along the way.
An error was detected along the way.
An error was detected along the way.
An error was detected along the way.
An error was detected along the way.
An error was detected along the way.
An error was detected along the way.
An error was detected along the way.
An error was detected along the way.



Hop Count: 9

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

<http://www.robotstxt.org/orig.html>

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/80/www

Contents of robots.txt :

User-agent: *

Disallow: /



Scan Information

Start time: Mon Dec 4 14:05:14 2023
End time: Mon Dec 4 14:17:06 2023

Host Information

IP:

Vulnerabilities

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS v2.0 Base Score

0.0 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:N)

References

CVE [CVE-1999-0524](#)
XREF [CWE:200](#)

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

icmp/0

The remote clock is synchronized with the local clock.

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.0.2
Nessus build : 20291
Plugin feed version : 202311281630
Scanner edition used : Nessus
Scanner OS : DARWIN
Scanner distribution : macosx
Scan type : Normal
Scan name : ██████████
Scan policy used : Basic Network Scan
Scanner IP : ██████████
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : ██████████
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/12/4 14:05 CST
Scan duration : 703 sec
Scan for malware : no
```



0

CRITICAL

0

HIGH

0

MEDIUM

0

LOW

3

INFO

Scan Information

Start time: Mon Dec 4 14:05:18 2023

End time: Mon Dec 4 15:11:43 2023

Host Information

DNS Name:



IP:



Vulnerabilities

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

 resolves as .

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.0.2
Nessus build : 20291
Plugin feed version : 202311281630
Scanner edition used : Nessus
Scanner OS : DARWIN
Scanner distribution : macosx
Scan type : Normal
Scan name : ██████████
Scan policy used : Basic Network Scan
Scanner IP : ██████████
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : ██████████
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialled checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/12/4 14:05 CST
Scan duration : 3980 sec
Scan for malware : no
```

185519 - SNMP Server Detection

Synopsis

An SNMP server is listening on the remote host.

Description

The remote service is an SNMP agent which provides management data about the device.

See Also

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2023/11/14, Modified: 2023/11/14

Plugin Output

udp/161

Nessus detected the following SNMP versions:
- SNMPv3



Scan Information

Start time: Mon Dec 4 14:05:18 2023
End time: Mon Dec 4 15:10:42 2023

Host Information

DNS Name: [Redacted]
IP: [Redacted]

Vulnerabilities

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

[Redacted] resolves as [Redacted].

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.0.2
Nessus build : 20291
Plugin feed version : 202311281630
Scanner edition used : Nessus
Scanner OS : DARWIN
Scanner distribution : macosx
Scan type : Normal
Scan name : ██████████
Scan policy used : Basic Network Scan
Scanner IP : ██████████
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : ██████████
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/12/4 14:05 CST
Scan duration : 3919 sec
Scan for malware : no
```

185519 - SNMP Server Detection

Synopsis

An SNMP server is listening on the remote host.

Description

The remote service is an SNMP agent which provides management data about the device.

See Also

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2023/11/14, Modified: 2023/11/14

Plugin Output

udp/161

Nessus detected the following SNMP versions:
- SNMPv3



Scan Information

Start time: Mon Dec 4 14:05:19 2023
End time: Mon Dec 4 14:16:33 2023

Host Information

DNS Name: [Redacted]
IP: [Redacted]

Vulnerabilities

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

[REDACTED] resolves as [REDACTED].

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.0.2
Nessus build : 20291
Plugin feed version : 202311281630
Scanner edition used : Nessus
Scanner OS : DARWIN
Scanner distribution : macosx
Scan type : Normal
Scan name : [REDACTED]
Scan policy used : Basic Network Scan
Scanner IP : [REDACTED]
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : [REDACTED]
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
```

Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialled checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/12/4 14:05 CST
Scan duration : 669 sec
Scan for malware : no

185519 - SNMP Server Detection

Synopsis

An SNMP server is listening on the remote host.

Description

The remote service is an SNMP agent which provides management data about the device.

See Also

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2023/11/14, Modified: 2023/11/14

Plugin Output

udp/161

Nessus detected the following SNMP versions:
- SNMPv3



0

CRITICAL

0

HIGH

2

MEDIUM

0

LOW

23

INFO

Scan Information

Start time: Mon Dec 4 14:05:20 2023
End time: Mon Dec 4 14:18:22 2023

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/443/www

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject :



45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>
<https://nvd.nist.gov/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information

THE GROWING CHALLENGE IN CYBERSECURITY

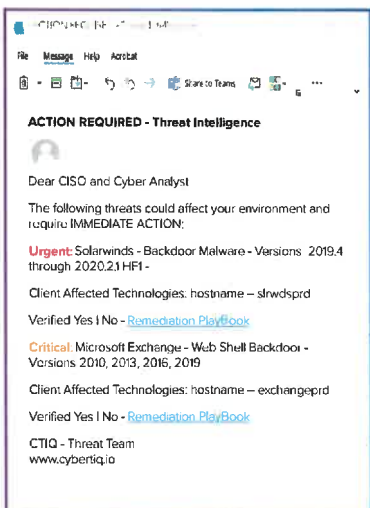
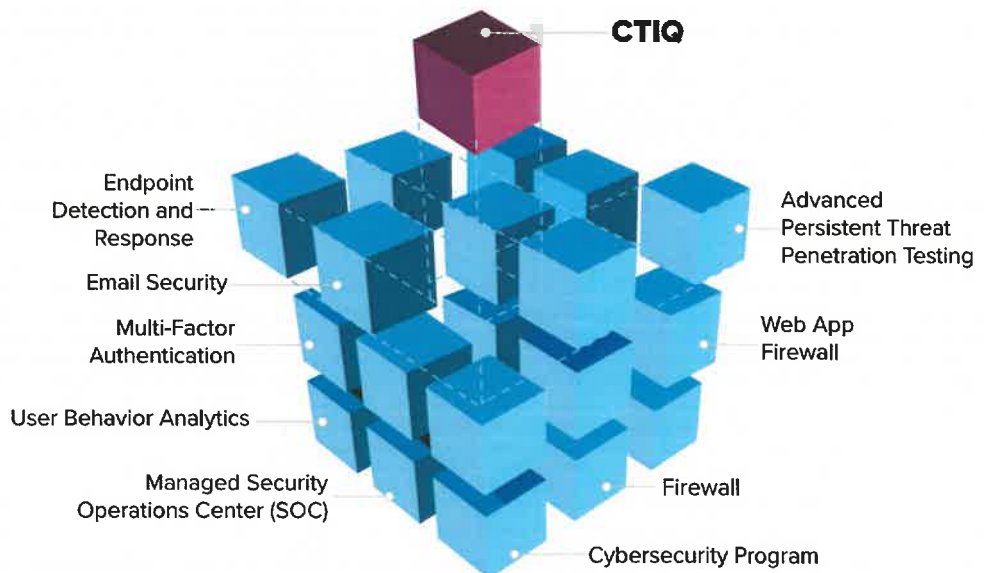


REDUCE ALERT FATIGUE

RECEIVE ONLY RELEVANT INFORMATION

PRIORITIZE THREATS

REVOLUTIONIZE YOUR CYBER DEFENSE WITH AI-POWERED INTELLIGENCE



CTIQ utilizes advanced AI technology to gather real-time data from various intelligence sources and centralizes it into one platform. You will receive emails that provide clarity, context, and actionable remediation recommendations specific only to the technology in your environment.

BECOME A BETA CLIENT

<https://cybertiq.io/> | info@cybertiq.io



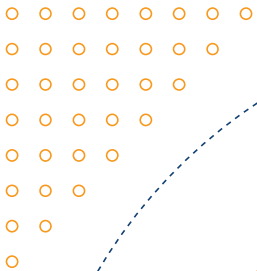
13916 Monroes Business Park, Suite 102 • Tampa, FL 33635
www.securanceconsulting.com



MARCH 28, 2024

COST PROPOSAL

RFQ #CRFQ 0705 LOT2400000009 NETWORK PENETRATION TESTING AND CYBERSECURITY ASSESSMENTS



Contact for RFP Response:

Patrick Swere

Proposal Manager

pswere@securanceconsulting.com

P: 877.578.0215 ext. 118

www.securanceconsulting.com

EXHIBIT A: PRICING PAGE

EXHIBIT A - Pricing Page


Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	\$15,840 -	\$ 121,176 -
2	4.2	Website Penetration Testing	8	\$3,960 -	\$ 30,294 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	\$17,160 -	\$ 131,274 -
4	4.4	Wireless Penetration Testing	8	\$6,600 -	\$ 50,490 -
TOTAL BID AMOUNT					\$ 333,234 -

Please note the following information is being captured for auditing purposes and is an estimate for evaluation only

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

Any product or service not on the Agency provided Pricing Page will not be allowable.

The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.

Vendor Name:	Securance LLC
Vendor Address:	13916 Monroes Business Park, Suite 102, Tampa, FL 33635
Email Address:	pswere@securanceconsulting.com
Phone Number:	877.578.0215 ext. 118
Fax Number:	None.
Signature and Date:	 3.21.24

PROPOSED FEES

Pricing

Securance has provided itemized pricing for the major aspects of this project in the tables below.

External Network Penetration Testing Project Scope Item	Line Item Fee
External Network Vulnerability Assessment and Penetration Test (2 external IP address blocks and approximately 15 external IP addresses) — Value Add	\$2,640
Firewall Configuration Review (10 firewall appliances: 1 of each pair running in HA mode)	\$7,920
VPN Review (price for a sample of 2)	\$4,752
Social Engineering — Phishing (200 active The Lottery staff)	\$1,584
External Network Vulnerability Assessment and Penetration Test Report	\$1,584
External Network Findings Presentation — Value Add	\$1,056
Unit Cost per Assessment and Reports Total	\$15,840
Unit Cost per Assessment and Reports with 5% Discount for Repeat Assessments*	\$15,048

Website Penetration Testing Project Scope Item	Line Item Fee
Website Penetration Testing (1 externally accessible website)	\$2,640
Website Penetration Testing Report	\$1,320
Website Penetration Testing Findings Presentation — Value Add	\$1,056
Unit Cost per Assessment and Reports	3,960
Unit Cost per Assessment and Reports with 5% Discount for Repeat Assessments*	\$3,762

Internal Client-side Network Penetration Testing Project Scope Item	Line Item Fee
Internal Network Vulnerability Assessment and Penetration Test (27 internal IP address blocks and 500 IP addresses)	\$7,920
Windows Workstations Configuration Review (250 windows OS endpoints of various versions)	\$1,848
Windows Servers Reviews (price for reviewing up to 3 unique Windows servers versions)	\$1,848
Router Switch Configuration Review (sampling approach)	\$4,224

PROPOSED FEES

Pricing

Internal Client-side Network Penetration Testing Project Scope Item	Line Item Fee
Internal Network Vulnerability Assessment and Penetration Test Report	\$1,320
Internal Network Findings Presentation — Value Add	\$1,056
Unit Cost per Assessment and Reports	\$17,160
Unit Cost per Assessment and Reports with 5% Discount for Repeat Assessments*	\$16,302
Wireless Penetration Testing Project Scope Item	Line Item Fee
Wireless Penetration Testing (includes IoT based attacks)	\$5,280
Wireless Penetration Testing Report	\$1,320
Wireless Penetration Testing Findings Presentation — Value Add	\$1,056
Unit Cost per Assessment and Reports	\$6,600
Unit Cost per Assessment and Reports with 5% Discount for Repeat Assessments*	\$6,270
Value Adds Across Projects	Line Item Fee
Project Management (across projects) — Value Add	\$2,112
Status Reporting (across projects) — Value Add	\$3,168
Knowledge Transfer — Value Add	\$1,056
Independent Project Review**	Included

The professional fees listed above are inclusive of all out-of-pocket expenses. The Lottery will **NOT** be billed for expenses such as travel, meals, and incidentals.

**The total reflects pricing for one instance of each assessment in the first year of contract. Securance will offer a 5% discount for repeat instances of each assessment and reporting deliverable. For example, if a second external network vulnerability assessment | penetration test is requested, Securance will offer the Lottery a 5% discount off the price of the first assessment.*

PROPOSED FEES

Pricing

***Each assessment completed by Securance is reviewed by a consultant independent of the project, in order to ensure that the engagement thoroughly addresses all scope items, all observations are factual and appropriately documented, recommendations are feasible and customized to the client, and all assessment components adhere to the firm's quality control standards.*

To provide the Lottery with cost certainty, we are offering a “not to exceed” (NTE) proposal, which means that the total cost of the project or service will not exceed the amount specified on the previous pages. However, we guarantee we will complete all items identified in the scope of services and listed in the contract or statement of work. Often, the actual project fee is less than the NTE fee listed. Our reasons for this pricing model include:

- ▶ The Lottery's project manager may ask our team to suspend additional testing based on the risks, threats, and vulnerabilities we discover and report. In this situation, our effort will be reduced, and we will pass those savings on to the Lottery or allocate those hours to other areas, as deemed necessary.
- ▶ The Lottery's project manager may wish to change the scope based on additional information obtained prior to project execution. In that case, the Lottery will not have to renegotiate the contract fees. Our pricing model is flexible to changes in scope.

Assumptions

Securance's proposed fees are based on the information that has been made available to us and on our understanding of the engagement. If the basis of our pricing is inaccurate, then the total cost to complete this engagement may differ from the firm, fixed price in this proposal. If events or circumstances, such as changes in scope, loss or unavailability of the Lottery personnel, or unavailability of documentation occur, Securance will determine their effect on the engagement scope, timing, and fees and promptly notify the Lottery of any such changes. Securance will not proceed with any changes or additions to the scope of work without the Lottery's explicit written approval.

Hourly Rate

Securance's cost proposal is based on an hourly rate of \$132, inclusive of labor, system licenses, and other reimbursable expenses. The hourly rate applies to all tasks and personnel resources required to complete this project. Any follow-up assessments or consulting engagements will be billed at the same hourly rate.

Payment Terms

Securance will submit an invoice after delivering a draft management report. All fees are due within 30 days following receipt of invoice. Securance will deliver the final management report following receipt of payment.

PROPOSED FEES

Building a Successful Partnership

For Securance, this is not just another project. It is an opportunity to help your team solve problems, exceed your goals, and pursue our mutual passion for improving the Lottery's security posture. After reviewing your needs and taking the time to understand your business, we are the best fit for this opportunity and **we want to partner with you!** We are offering the following free value adds as one way to demonstrate our passion, our desire to work with you, and the lasting value brought by the Securance advantage.

Deliverable	Value
External Network Vulnerability Assessment and Penetration Test	Securance will provide the requested external network vulnerability assessment and penetration test at no cost to the Lottery. Please see our Technical Proposal for more information regarding our approach and methodology to perform the external network assessment.
Project Management	Securance will provide project management across projects at no cost to the Lottery.
Status Reporting	To enhance the effectiveness of this engagement and to demonstrate our commitment to The Lottery, Securance will provide status reports across all projects at no cost to the Lottery.
External Network Findings Presentation	Securance will provide the requested external network findings presentation at no cost to the Lottery.
Website Findings Presentation	Securance will provide the requested website findings presentation at no cost to the Lottery.
Internal Network Findings Presentation	Securance will provide the requested internal network findings presentation at no cost to the Lottery.
Wireless Network Findings Presentation	Securance will provide the requested wireless network findings presentation at no cost to the Lottery.
Knowledge Transfer	To ensure our assessment provides high value, is fully understandable, and the information obtained is sustained, we will conduct a knowledge transfer session with appropriate Lottery staff. This session will provide answers as to why and how Securance performed specific tasks, so the Lottery's staff are able to repeat the task at will.

If you have questions or would like additional information, do not hesitate to contact us. We want to make sure you have everything you need to make your decision.

We want to partner with you and will be your best partner!



13916 Monroes Business Park, Suite 102 • Tampa, FL 33635
www.securanceconsulting.com