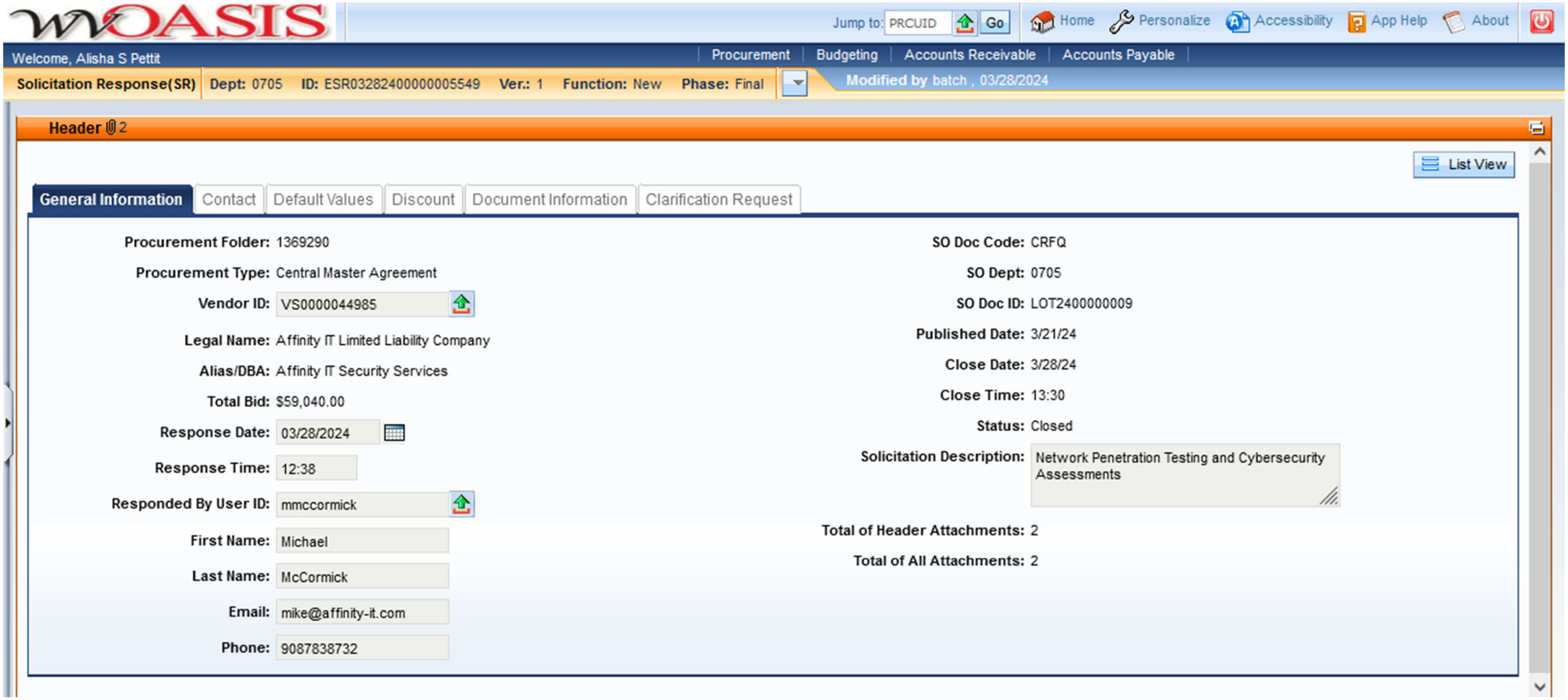
West Virginia
Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

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.



Welcome, Alisha S Pettit

Solicitation Response(SR) **Dept:** 0705 **ID:** ESR032824000000005549 **Ver.:** 1 **Function:** New **Phase:** Final

Modified by batch , 03/28/2024

Header 2

Procurement Folder:	1369290
Procurement Type:	Central Master Agreement
Vendor ID:	VS0000044985
Legal Name:	Affinity IT Limited Liability Company
Alias/DBA:	Affinity IT Security Services
Total Bid:	$59,040.00
Response Date:	03/28/2024
Response Time:	12:38
Responded By User ID:	mmccormick
First Name:	Michael
Last Name:	McCormick
Email:	mike@affinity-it.com
Phone:	9087838732

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 ESR03282400000005549	1

VENDOR

VS0000044985
Affinity IT Limited Liability Company

Solicitation Number: CRFQ 0705 LOT2400000009

Total Bid: 59040 **Response Date:** 2024-03-28 **Response Time:** 12:38:32

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				19160.00

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				7960.00

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				15960.00

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				15960.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

CRFQ LOT2400000009

Network Penetration Testing and Cybersecurity Assessments

Due Date March 28, 2024

Prepared
Exclusively For:

West Virginia Lottery Commission
219 Washington Street
Charleston, WV 25305

Submitted by:
Affinity IT Security Services
1243 Sussex Turnpike, Suite #1
Randolph, NJ 07869
(800) 840-2335
info@affinity-it.com

AFFINITY
SECURITY SERVICES

Table of Contents

Cover Letter

Brandon Barr, Buyer
West Virginia Purchasing Division
2019 Washington Street
East Charleston, WV 25305

March 29, 2024

Dear Brandon,

We are pleased to have the opportunity to participate in your CRFQ process. We have been performing similar work for many clients over the past 17 years and have the necessary experience to plan, coordinate, and execute strategic and cost-effective cybersecurity assessment and remediation programs. We have extraordinary technical expertise that is agile and responsive to our client's needs. Our goal is to assist you in strengthening your cybersecurity and protecting your assets and operations.

It is not just the number of assessments performed, we ensure our customers understand our reports and findings and are prepared to remediate. Our proprietary reports rank findings by severity and occurrence, empowering clients to reduce their risk and vulnerability count quickly.

We are pleased to share that for the last two years, we have provided Network Penetration Testing and Cybersecurity Assessments for the City of Charleston, West Virginia. The summary of the work we provided is detailed in the *References* section of this response.

We have extensive Project Management experience running Cybersecurity Consulting projects. It is literally what we do. We have deep PM expertise, having taught PM for IT for several years. We value and excel at communication throughout each project lifecycle. Clients are consistently apprised of plans, status, and progress. We achieve exceptional knowledge transfer by ensuring reports are clear, with findings that are presented in live readouts. Clients feel comfortable reaching out to us with questions, and those questions are always welcomed and answered.

Our response provides all the requested information, but if you need any additional details as you consider your options, please let me know. I would also be happy to furnish additional references, or to simply discuss our qualifications and experience.

We are completely committed to delivering on all services and information as detailed in both the CRFQ and the Q&A documents as well as within our response.

We appreciate your consideration, and we look forward to the opportunity to work as your partner to keep the West Virginia Lottery Commission secure.

Joseph W. Fisher

Joseph W. Fisher, President
Affinity IT LLC.
(800) 840-2335
joe@affinity-it.com

Company Profile and Relevant Experience

Affinity IT Security Services is the registered DBA (doing business as) name of Affinity IT, LLC. Affinity IT, LLC is a Limited Liability Company certified small business registered in New Jersey. **Affinity IT Security Services is SOC 2 certified, is on the GSA Schedule, is an IBM Business Partner, Tenable Assure Partner, and Value-Added-Reseller (VAR) with NinjaOne and Cynet.**

The official name and address are:

Affinity IT, LLC.
1243 Sussex Turnpike, Suite #1
Randolph, NJ 07869
(800) 840-2335
info@affinity-it.com
www.affinity-it.com

The primary contact for this project is:

Joseph W. Fisher, President
joe@affinity-it.com

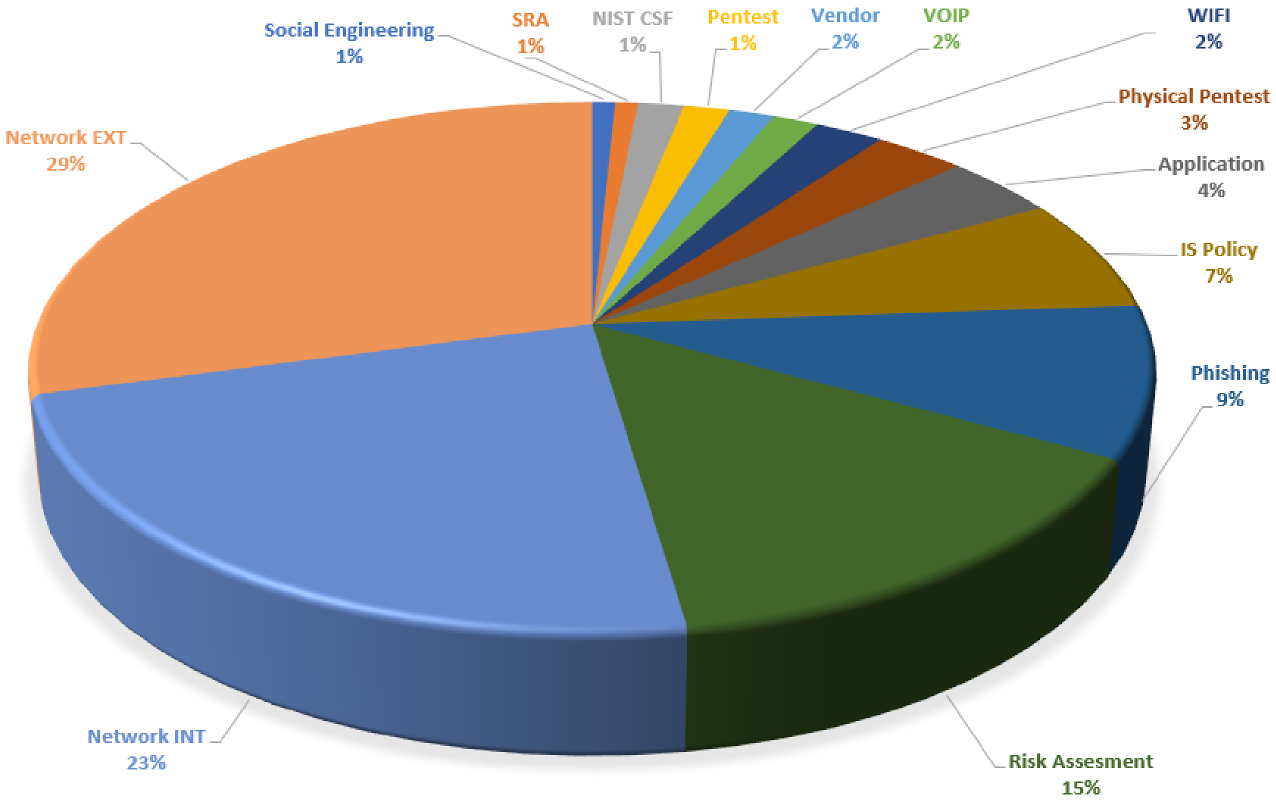
Affinity IT was incorporated in 2007 and has 8 individuals on staff:

- Joseph W. Fisher: President and founder, Senior Security Analyst
- Konrad Gawronski: Security Analyst
- Michael McCormick: Security Analyst
- Daven Ryerson: Security Analyst
- Frank Alemar: Security Analyst
- James M. Strain: Senior Security Analyst and Security Software Developer**
- James Moralez: Industrial Control System Security Analyst**
- Ching Loo: Office Administrator and Operations Manager

** Contractor engaged for special needs.

We are US based and employ only US Citizens. We are 100% network security focused. We are dynamic and agile by necessity. We maintain flexible operations that allow us to perform security assessments both at the customer site as well as remotely. We are disciplined in our approach, yielding systematic execution for all aspects of network security testing. Our decades of experience produce a competitive advantage, as we can identify and quickly respond to Indicators of Compromise (IOCs) that others may overlook. Our methods cultivate reliability and efficiency, producing continuous feedback and weekly report readouts from our team with not just technical expertise but also decades of competent project management experience. Whatever the network security concern, we have the experience to continuously deliver solutions and recommendations that protect and defend against present and future threats to network security.

We are not just auditors, we are Network Engineers, Computer Scientists, and Certified Ethical Hackers (CEH) with decades of hands-on technical experience. We find vulnerabilities that others do not. During the past five years, Affinity IT has completed 116 security assessments, with 44 of those being performed over the last 12 months.



With over 17 years of cybersecurity consulting experience, Affinity IT Security has the precise skills and expertise demanded by this project. We bring a deep understanding of networking, software, and security to the task, specifically:

1. Strong networking analysis and design expertise
2. Extensive network, application, and operational security assessment experience
3. The forward-looking technical vision necessary to create a technology roadmap to facilitate the smooth evolution of technology.
4. Extensive security awareness training programs
5. Extraordinary social engineering expertise
6. Extraordinary expertise in municipal organization operations and needs
7. Strong project management skills
8. Strong communication skills.

We are cybersecurity consultants, not salespeople. We always seek to recommend practical and cost-effective solutions that truly improve your cybersecurity across the enterprise. Since 2009 we have worked with companies large and small to protect and secure their IT assets.

Our expertise includes the following:

- Information Security Assessments

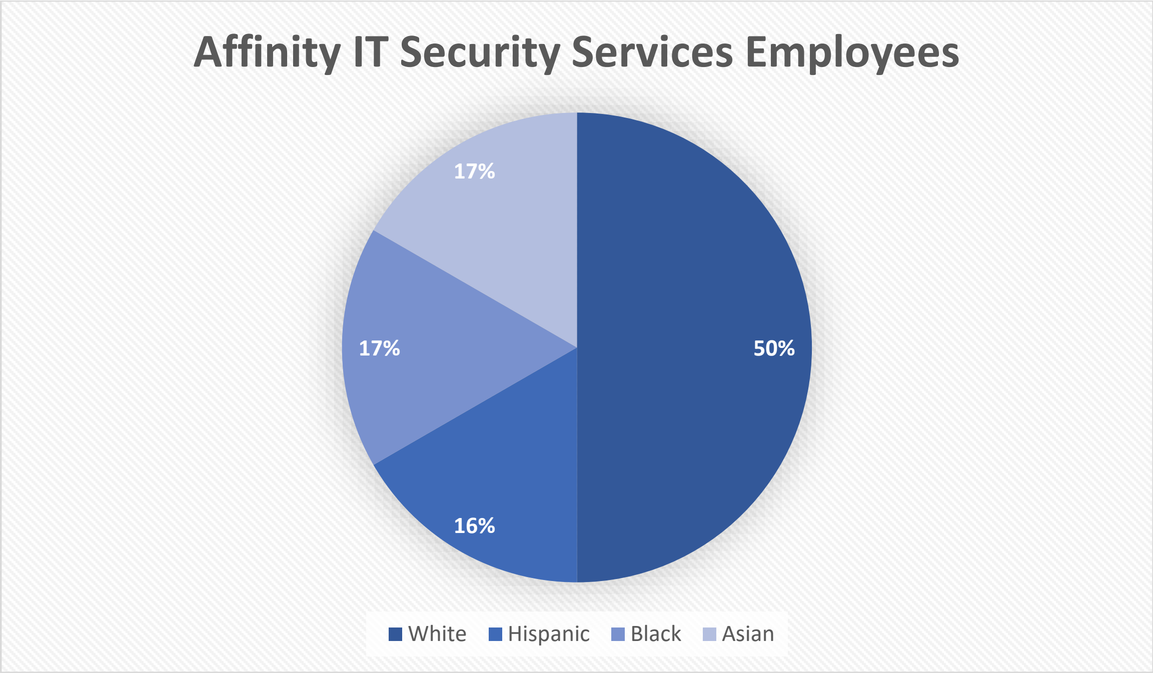
  - Evaluating all aspects of your information security, both operational and IT, and reporting on deficiencies and priorities

- Network Security Vulnerability Assessments and Penetration Testing
  - Identifying and reporting vulnerabilities in both internal and publicly exposed servers, conducting live readout(s) with your IT staff, and making specific suggestions regarding remediation
- Website Security Assessment
  - Identifying and reporting web application vulnerabilities, conducting live readout(s) with your development staff, and making specific suggestions regarding remediation
- Web Application Security Assessment
  - Test existing applications to discover inherent security vulnerabilities
  - Penetration Test applications to assess their resistance to attack
- Cybersecurity Compliance
  - Incorporating your regulatory and/or compliance requirements into a comprehensive and practical cost-effective cybersecurity plan. Expertise includes CJIS and HIPAA Compliance, CIS Controls / NIST CSF, NIST 800-53
- Secure Application Development
  - Training development staff in secure design and train testers how to test security
  - Creating a secure Software Development Lifecycle (SDLC)
- Information Security Policies and Procedures
  - Developing practical and effective Policies specific to your needs
- Cybersecurity Training
  - In addition to EC Council Certificate training, Affinity IT Security offers in-depth technical training in several Information Security topics.

We have a deep understanding of the NIST 800-53 control set, as we routinely advise our clients on regulatory compliance.

Commitment to Diversity

Affinity IT Security is committed to hiring the best and brightest individuals. Our employees come from different backgrounds and bring unique experiences that enhance our ability to meet the needs of our customers. The chart below provides a glimpse of our diversity breakdown. In addition, please note that we employ 1 female and 2 active Air and National Guard members**.**



Equal Employment Opportunity and Affirmative Action Policy

Affinity IT, LLC. provides equal employment opportunities to all employees and applicants for employment and prohibits discrimination and harassment of any type without regard to race, color, religion, age, sex, national origin, disability status, genetics, protected veteran status, sexual orientation, gender identity or expression, or any other characteristic protected by federal, state, or local laws.

This policy applies to all terms and conditions of employment, including recruiting, hiring, placement, promotion, termination, layoff, recall, transfer, leaves of absence, compensation, and training.

Joseph W. Fisher

Mr. Fisher is the founder and principal and performs and/or supervises all security work performed by the firm. Mr. Fisher has over 30 years of IT experience including systems development, training, and cybersecurity consulting. He brings the following credentials to the table:

- BS, Computer Science
- MS, Computer Science
- Master of Business Administration (MBA)
- ISACA Certified Information Systems Auditor (CISA)
- EC-Council Certified Ethical Hacker (CEH)
- SANS/GIAC Certified Web-Application Penetration Tester (GWAPT)

Mr. Fisher will act as Project Manager on this project and will be on-site for each visit and participate in all aspects of the work. He will ensure the planning is strategic and detailed, the execution carefully orchestrated, and vulnerabilities clearly documented and communicated. Mr. Fisher will also be responsible for documentation gathering and review, interviews, reports, and the presentation of findings.

Konrad P. Gawronski

Mr. Gawronski joined Affinity IT Security from the NJ National Guard Cyber Warfare Operations Center and brings a strong networking background and a passion for cybersecurity. Mr. Gawronski designed and implemented the current Affinity IT Security Phishing Platform, and personally manages all campaigns. Mr. Gawronski will work with Mr. Fisher, Mr. McCormick and Mr. Ryerson and be responsible for information gathering, network scanning, security analysis and reviews, and documentation of findings.

Michael J. McCormick

Mr. McCormick brings over 35+ years of IT and cybersecurity experience to the project. His expertise includes Critical Infrastructure Protection (CIP), and risk assessment. Mr. McCormick will work with Mr. Fisher, Mr. Gawronski and Mr. Ryerson and be responsible for information gathering, network scanning, security analysis and reviews, and documentation of findings.

Frank Alemar

Mr. Alemar is an accomplished professional with 13 years of military experience, all within the National Guard, including as a Cyber Warfare Technician with the US Army Cyber Center of Excellence. Mr. Alemar will work with Mr. Fisher, Mr. Gawronski, Mr. McCormick, and Mr. Ryerson and be responsible for information gathering, network scanning, security analysis and reviews, and documentation of findings.

Daven Ryerson

Mr. Ryerson recently joined our Affinity security team and brings additional IT and cybersecurity expertise to the project. Mr. Ryerson will work with Mr. Fisher, Mr. Gawronski and Mr. McCormick and be responsible for information gathering, network scanning, security analysis and reviews, and documentation of findings.

Resume

President and Founder, Senior Security Analyst Director

joe@affinity-it.com

973.895.5777

EDUCATION

MBA, Fairleigh Dickinson University

MSCS, Rensselaer Polytechnic Institute, Troy, NY

BSCS, Merrimack College, North Andover, MA

CERTIFICATIONS

Certified Information Systems Auditor (CISA) - ISACA

Certified Web Application Penetration Tester – GIAC (SANS)

Certified Ethical Hacker (CEHv10) – EC Council

PROFESSIONAL AFFILIATIONS

Trustee, Past President: Executive Council of the Society of Information Management (SIM), NJ

Underwriters Laboratories (UL) Standards Technical Panel Member (Cybersecurity of IoT)

Joseph W. Fisher | 35 Years' Experience

Summary

Experienced cybersecurity practitioner with extensive experience in software development, project management, and IT Security. A fast learner with keen insight into the strengths and limitations of technologies and their use within organizations, (hands-on) proficient in numerous technologies and disciplines and comfortable discussing the practical application of many more. Performs effectively individually as well as in team environments, and brings enthusiasm, humor, and strong analytical and organizational skills to all endeavors. Equally at ease with entry level IT staff as well as senior managers, can communicate effectively with both business and technical personnel. Capable of contributing to and securing all aspects of the software development lifecycle.

Relevant Experience

Provide consulting in IT Security Vulnerability Assessment and remediation of IT infrastructure and web applications. Employ Nessus and Nmap for network vulnerability scanning, Kali Linux for Penetration Testing.

Projects and roles include:

- Application Security Consultant: Major US Financial Exchange.
- Web Application Security Consultant: Large Health Insurer, New York.
- Application Security Engineer: Fortune Global 100 Fortune Bank and Financial Services firm.
- Web Application Security Assessor: Fortune 50 Bank and Financial Services firm.
- IT Security vulnerability assessment of a financial organization that included the examination and analysis of physical security, and policies and procedures governing all operations. Reported and presented numerous (including critical) findings and prioritized remediation recommendations.
- Consulted with a $38M cloud SAAS provider to train QA and Developers in secure development techniques. Engagement resulting in the detection and remediation of numerous security vulnerabilities.
- Conducted external vulnerability scans of global infrastructure for privately held financial services software company. Engagement resulting in the detection and remediation of numerous security vulnerabilities.

Resume

Security Analyst

konrad@affinity-it.com

973.895.5777

EDUCATION

US Air Force – AETC, Cyber Warfare Operations, Network Warfare, Cyber Transport Systems

CERTIFICATIONS

SANS GIAC Intrusion Analyst (GCIA)

SANS GIAC Security Essentials (GSEC)

Certified Ethical Hacker (CEHv11) – EC Council

CompTIA Security+

CompTIA CySA+

CCNA Cyber Ops

PROFESSIONAL AFFILIATIONS

New Jersey Air National Guard 140th Cyberspace Operations Squadron – Cyber Warfare Operations

Konrad P. Gawronski | 8 Years' Experience

Summary

Experienced Cybersecurity Professional proficient in conducting comprehensive network security assessments and ethical hacking. Skilled in vulnerability analysis, phishing campaign management, and network infrastructure planning. Strong expertise in forensic analysis, endpoint security, and SOC alert triage.

Relevant Experience

Conduct comprehensive internal and external network security assessments, encompassing both physical and software penetration testing. Execute the entire ethical hacking lifecycle, from reconnaissance and fingerprinting to vulnerability discovery and exploitation. Document findings meticulously and engage directly with clients to articulate identified vulnerabilities and propose effective remediation strategies through detailed reports and live presentations. Additionally, oversee customer phishing engagements, tailoring campaigns to meet specific business requirements, and ensuring seamless phish delivery while implementing proper whitelisting measures.

Highlighted projects and skills encompass:

- Executing network/host-based forensic analysis.
- Coordinating endpoint/network vulnerability scans.
- Crafting comprehensive remediation recommendations.
- Spearheading the deployment of Nessus and Cynet agent software.
- Conducting in-depth Wi-Fi security assessments and generating signal analysis reports.
- Managing and orchestrating phishing and smishing campaigns.
- Leading physical penetration engagements to assess physical security measures.
- Conducting Tier 1 SOC alert triage to swiftly identify and address security incidents.
- Planning and implementing network security infrastructure to fortify defenses.
- Conducting penetration testing and proficient packet manipulation for vulnerability identification.
- Delivering cybersecurity training to enhance organizational security awareness.

Resume

Security Analyst

mike@affinity-it.com

973.895.5777

EDUCATION

BS in Mathematics and Computer Science, Montclair State University

CERTIFICATIONS

Certified Ethical Hacker (CEHv11) – EC Council – In Process

Michael J. McCormick | 35 Years' Experience

Summary

Senior Network Security Analyst dedicated to the development and testing of computer networking and telecommunications solutions. Member of the historic AT&T Bell Laboratories team that built the first IEEE 802.3 implementation of Ethernet over twisted pair and has spent over 20 years dedicated to delivering secure solutions to the marketplace, including Critical Infrastructure. A passionate advocate for passive monitoring of Operational Technology (OT) environments to protect our nation's critical infrastructure.

Relevant Experience

Perform internal and external network security assessments and penetration testing. Enact the entire ethical hacking lifecycle including reconnaissance, fingerprinting, vulnerability discovery, and exploitation. Document and directly interface with clients to communicate vulnerabilities and suggest remediations in written reports and live presentations. Tools utilized include Nessus Pro, Kali Linux, Burp Suite, and Nmap. Optimize internal network configuration and operations.

Past Projects and rolls include:

- Working with utility commissioners and their staff from around the country to act as a liaison between the Public Utilities Commission (PUC) and the utilities they regulate (electric, gas, water) to perform Cybersecurity Preparedness Assessments as it relates to Critical Infrastructure Protection (CIP). Assessment details focus on identifying existing vulnerabilities, proposing protection strategies that detect cybersecurity events, utilizing the latest continuous passive monitoring techniques. Assessment also included recommendations to assist with incident response and recover.
- Rolling out cybersecurity solutions integrating Network Anomaly Detection used as intrusion detection and intrusion prevention utilizing passive monitoring techniques driven by an embedded Linux-based sensor managing critical substation infrastructure.
- Implementing Behavioral Learning and Network Flow Whitelisting.

Resume

Security Analyst

frank@affinity-it.com

973.895.5777

EDUCATION

US Army Cyber Center of Excellence, Cyber Warfare Technician

AS in Electronic Technology - Community College of the Air Force

Extensive DoD Cyber Security Training

CERTIFICATIONS

CompTIA Security +

CompTIA Network +

Frank Alemar | 7 Years' Experience

Summary

Frank specialized in Information Protection for various weapons systems and achieved full qualification as a Cyber Warfare Technician. This involved an intensive 750-hour academic course covering both Offensive and Defensive Cyber Operations. He developed expertise in safeguarding military assets against cyber threats, demonstrating a strong commitment to the highest standards of security.

Known for his adaptability, leadership, and strong work ethic, Frank brings a unique blend of military precision and private-sector acumen to any professional setting. He contributes his extensive skills to drive success with information protection, cybersecurity, and strategic planning.

Relevant Experience

Perform internal and external network security assessments and penetration testing. Enact the entire ethical hacking lifecycle including reconnaissance, fingerprinting, vulnerability discovery, and exploitation. Document and directly interface with clients to communicate vulnerabilities and suggest remediations in written reports and live presentations. Tools utilized include Nessus Pro, Kali Linux, Burp Suite, and Nmap. Optimize internal network configuration and operations.

Past Projects and rolls include:

- Information Systems Security Officer at Joint Force Headquarters for the Connecticut National Guard. In this role, he played a pivotal part in ensuring the security and integrity of information systems critical to national defense. His ability to adapt to diverse environments and apply military discipline to private-sector challenges was evident.
- Information Systems Security Officer at Joint Force Headquarters for the Connecticut National Guard. In this role, he played a pivotal part in ensuring the security and integrity of information systems critical to national defense.
- As an Engineer for a Digital Risk Protection company, he leveraged his military background to provide unique insights into cybersecurity solutions. He utilized advanced software to protect digital assets of private companies, employing threat intelligence and monitoring to effectively mitigate risks

Resume

Security Analyst

daven@affinity-it.com

973.895.5777

EDUCATION

NGT Academy

Cybersecurity Specialist

CERTIFICATIONS

Certified Ethical Hacker (CEHv11) – EC Council

CompTIA Security+

NGT Cyber Security Professional (NCSP)

Certified Ethical Hacker Master (CEH Master)

100w Cyber Security Practices for Industrial Control Systems

210W-01 Differences in Deployments of Industrial Control Systems (FY22)

210W-03 Common ICS Components

210W-2 Influence on IT Components on Industrial Control Systems

Daven Ryerson | 4 Years Experience

Summary

Highly motivated professional with hands-on project experience in Analyzing Threats, Networking, and Network Security. Currently holds CEH (Certified Ethical Hacker), CEH Master (Certified Ethical Hacker Masters), and CompTIA Security+ certifications. Awarded NGT Cyber Security Professional (NCSP) status by NGT Academy.

Actively receiving certifications from U.S Department of Homeland Security CyberSecurity and Infrastructure Security Agency (CISA) and pursuing the ICS/SCADA certification offered by the EC-Council. Instrumental in achieving SOC 2 compliance for the firm, demonstrating a commitment to robust security practices and regulatory standards. Passionate about advancing knowledge and skills in cybersecurity for critical infrastructure protection.

Relevant Experience

Proficient in conducting comprehensive internal and external network security assessments and penetration testing, following the entire ethical hacking lifecycle from reconnaissance to exploitation. Skillfully document findings and interface directly with clients to communicate vulnerabilities, offering remediation suggestions through written reports and live presentations. Proficient in utilizing advanced tools such as Nessus Pro, Kali Linux, Burp Suite, and Nmap. Demonstrated expertise in optimizing internal network configurations and operations.

Projects and skills include:

- Played a pivotal role in creating and implementing security protocols for remote access.
- Implemented effective measures to identify vulnerabilities in critical network infrastructure.
- Coordinated network vulnerability scans and provided thorough remediation recommendations.
- Responsible for security trend reporting to ensure scalable network protection.
- Proficient in network security infrastructure planning and implementation, with expertise in Cisco routers and switches.
- Skilled in executing virus deconstruction techniques and adept at managing legacy and enterprise network platforms.
- Experienced in enacting security measures to enhance the security posture of growing networks.
- Competent in network security management, penetration testing, and packet manipulation techniques.

Relevant Industry Certifications

We recognize that professional certifications are important within the industry. In addition to the vast experience of our staff, listed below are various security credentials and certifications earned by Affinity IT Security Services personnel.

- Bachelor of Science (Computer Science)
- Master of Science (Computer Science)
- Master of Business Administration (MBA)
- ISACA Certified Information Systems Auditor (CISA)
- EC-Council Certified Ethical Hacker (CEH)
- EC-Council Certified Ethical Hacker Master (CEH Master)
- SANS/GIAC Certified Web-Application Penetration Tester (GWAPT)
- US Air Force – AETC, Cyber Warfare Operations, Network Warfare, Cyber Transport Systems
- US Army Cyber Center of Excellence, Certified Cyber Operations Technician
- NY Army National Guard, Cyber Protection, Warrant Officer, Cyber Warfare Technician
- SANS GIAC Intrusion Analyst (GCIA)
- SANS GIAC Security Essentials (GSEC)
- CompTIA Security+
- CompTIA Network+
- CompTIA CySA+
- NGT Cyber Security Professional (NCSP)
- EC-Council Accredited Training Center

Methodology / Response to Requirements

Affinity IT Security is submitting this response to the West Virginia Lottery Commission and providing details for the work identified in the CRFQ and Q&A documents. This response outlines our abilities to deliver the Network Penetration Testing and Cybersecurity Assessment Services requested. Our areas of expertise are thoroughly aligned with the services you are requesting:

- External Network Penetration Testing
- Internal Network Vulnerability Assessments
- Website and Web Application Security Penetration Testing
- Wireless (Wi-Fi) Network Assessment and Penetration Testing
- CIS / NIST CSF Cybersecurity Maturity Assessment
- Network Architecture Evaluation
- Firewall Configuration Assessment (VPN, DMZ, VLAN)
- Server Evaluation Assessment (Physical and Virtual)
- Data Store Review and Security Assessment
- Microsoft AD, Azure AD and O365 Configuration Assessment
- Mobile Device Management Assessment
- Social Engineering / Phishing
- Strategic Remediation Roadmap and Implementation Plan

Sequence of Activities

Assessments typically begin with a kick-off meeting to introduce the participating personnel and set expectations between the client and vendor. Kick-off topics include the high-level schedule, documentation requests, permission form(s), technical requirements, and coordinating on-site visitation.

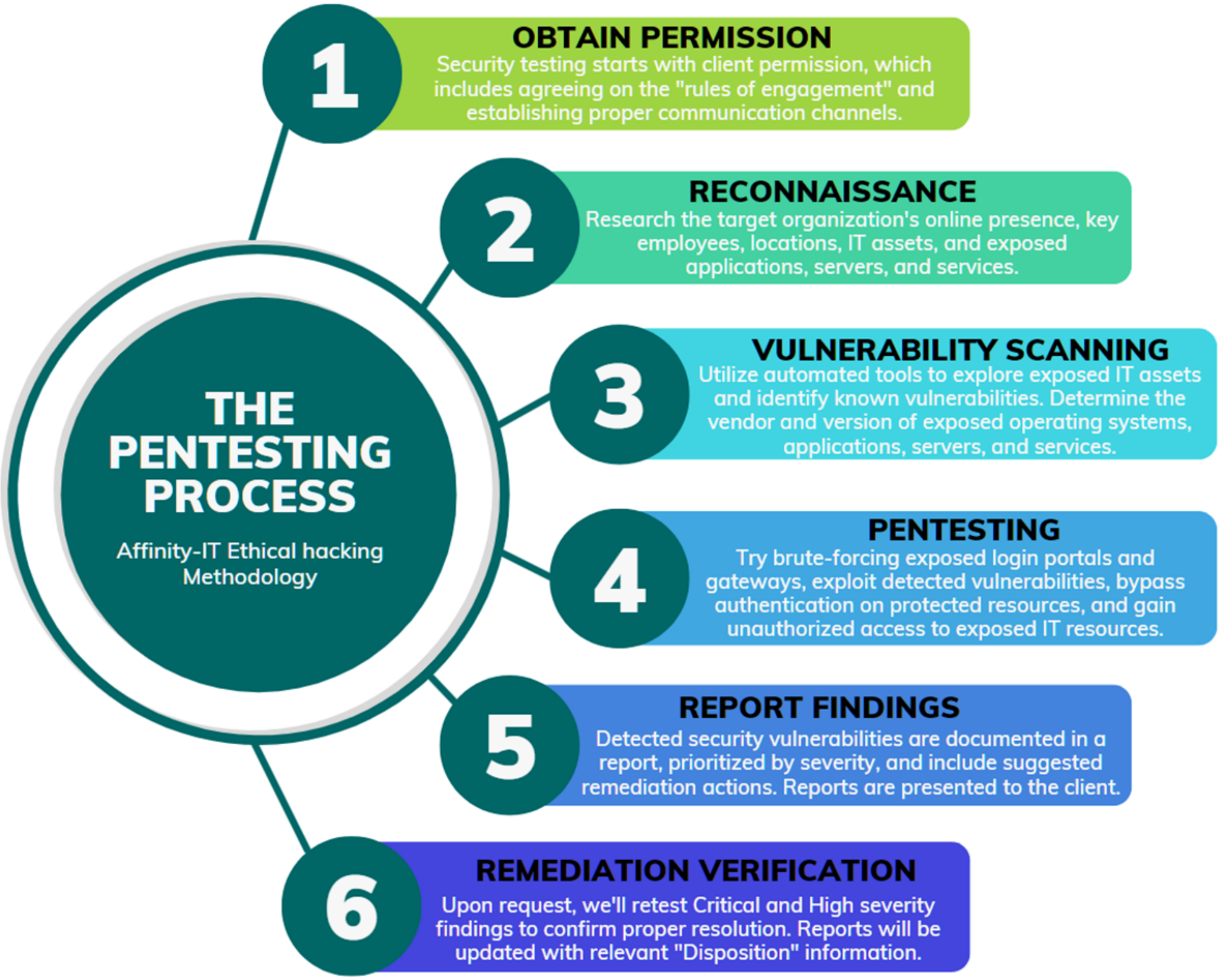
External scanning is usually the first activity to be completed, as it has the fewest dependencies. Penetration Testing occurs immediately following scanning. This produces a report and readout.[1]

This will be followed by the on-site visitation in which internal network security assessment and vulnerability scanning, and physical security penetration testing activities occur.

In all activities, **the focus is on planning and communication to ensure consistent expectations** on both sides. We also insist on explicit written permission to perform each testing step and IT chaperones to supervise any "hands on" configuration work within the environment. In short, **you will enjoy complete confidence that our work does not negatively impact your environment or operations**.

[1] All reports are delivered in encrypted form and reviewed in a live remote presentation, called a "readout".

Network Vulnerability and Penetration Testing



THE PENTESTING PROCESS

Affinity-IT Ethical hacking Methodology

1 OBTAIN PERMISSION
Security testing starts with client permission, which includes agreeing on the "rules of engagement" and establishing proper communication channels.

2 RECONNAISSANCE
Research the target organization's online presence, key employees, locations, IT assets, and exposed applications, servers, and services.

3 VULNERABILITY SCANNING
Utilize automated tools to explore exposed IT assets and identify known vulnerabilities. Determine the vendor and version of exposed operating systems, applications, servers, and services.

4 PENTESTING
Try brute-forcing exposed login portals and gateways, exploit detected vulnerabilities, bypass authentication on protected resources, and gain unauthorized access to exposed IT resources.

5 REPORT FINDINGS
Detected security vulnerabilities are documented in a report, prioritized by severity, and include suggested remediation actions. Reports are presented to the client.

6 REMEDIATION VERIFICATION
Upon request, we'll retest Critical and High severity findings to confirm proper resolution. Reports will be updated with relevant "Disposition" information.

Affinity IT follows a structured approach to test networks, based on the Certified Ethical Hacking methodology. Experienced analysts add their intuition to this process, ensuring thoroughness and efficiency. We use tools like Nmap, the Kali Linux suite, and Nessus Professional for testing. Additionally, we gather information from archived web pages and social media platforms like LinkedIn, Twitter, and Facebook. This helps us understand a client's network better. We scan for vulnerabilities and manually test them for exploits. If we breach a client's system, we inform them immediately. Detected vulnerabilities are documented using industry standards like the National Vulnerability Database and the Common Vulnerability Scoring System, which helps us prioritize and suggest fixes.

Website and Web Application Security Penetration Testing

For application security testing, our approach is based on the GIAC Web Application Penetration Tester (GWAPT) program. The process includes mapping the target application, understanding key design aspects such as authentication, session management, and permissions, and then executing targeted tests to detect vulnerabilities in the design. Common vulnerabilities such as the OWASP Top 10 are tested, along with significant additional ad-hoc testing by the security analyst. Accounts corresponding to each role supported by the application are used to test permissions and privileges. Once again, we rely on our security analysts' intuition as to how to violate designer's expectations and utilize malformed input and unexpected interactions to discover application vulnerabilities. Typical tools used for application testing include Burp Suite and Postman. Vulnerabilities are categorized and identified using the industry standard Common Weakness Enumeration (CWE). Given that it is not known how many applications are in scope for this testing at the time of this response, we included the cost for 3 applications in the "Costs" section.

All testing begins with a "Permission to Test" form that must be completed by the client that includes the type(s) of testing to be performed, along with the specific IPs and domain names that are in-scope. A Communication Plan identifying critical contacts on both sides, and notification requirements is developed.

In terms of "Rules of Engagement", in the event of a successful breach, the client is notified immediately, and additional infiltration discussed. The deliverable is a report of findings detailing detected vulnerabilities, organized by IP, cross-referenced by vulnerability, each accompanied by one or more suggested remediations.

The deliverable from all security tests are reports detailing the scope, approach, findings, and suggested remediations. Each report is always presented in a live readout session. Original scan reports (i.e., raw reports produced by the scanner) are available on request.

Follow up verification of fixes is performed (remotely) on request as part of the original test.

Application Security testing also requires written permission to test, along with "Rules of Engagement" regarding testing times, and protection of production environments. Under typical conditions, we will instrument the application and utilize it as each "role" would, looking for potential ways to exploit the design and violate developer assumptions. Vulnerabilities are identified, documented, and potential fixes specified. A readout is performed in which findings are presented and discussed with developers. Validation (remote) of critical findings is part of the service.

Protection of Institutional Sensitive Information

Client reports and scans are stored in encrypted form.

Client reports are transmitted via email in encrypted form and the password is communicated via a secondary channel (such as SMS[2]).

Regarding sensitive client information, the best solution is not to have it. Thus, in addition to the fact that Affinity IT and the client will have a mutual NDA that prohibits the sharing of any client information that is not public, Affinity IT does not and will not collect or store client data during testing beyond the scans and reports used to identify infrastructure and potential vulnerabilities.

Wireless Penetration Testing

[2] i.e., text message.

Our wireless network assessment testing focuses on a scan of the 2.4 and 5ghz range. We begin with a building heat map of the exterior of the facility to discern the degree to which Wi-Fi signal bleeds into public areas. This helps to determine how far from the building a malicious user can listen from to capture the Wi-Fi signals.

Interior walkthroughs are also performed to identify potential man-in-the-middle/rogue access points that could pose as an official access point. The collected SSIDs are then compared to the client provided approved list to help determine any outliers.[3]

We also take a hard look at each individual access point and perform an in-depth examination of the security configuration. Based on our observations, we provide detailed configuration recommendations.

Lastly, we may simulate a malicious user, create a rouge access point, and collect user connections, by standing up fake phishing login portals. We then force user connections to drop from the network where they are connected and subsequently capture their "handshakes" as they reconnect so to perform offline password cracking.

The findings from the wireless network assessment testing are then documented in a separate report readout.

Controls and Procedures

Although we generally endeavor to schedule scans and penetration tests during non-business hours to minimize potential operational impacts, active testing always entails some risk of operational impact.

We rely on the communication plan to keep both sides informed of events and conditions during testing. The purpose of the communication plan is to ensure both sides know who to contact and under what conditions.

Offending activities are immediately halted if/when impacts are reported. Conversely, we occasionally need to notify the client that we have been blacklisted and request access be restored.

Process for Re-testing of Remediated Items

We will immediately retest any critical findings that have been remediated to verify remediation upon client request. We expect the client to batch up fixes and notify us when to re-test. An amended report containing a "Disposition of Findings" section will be delivered upon client request.

Comprehensive Solution

Our solution is a one price, turnkey solution and does not require any software licensing, maintenance, and/or third-party agreements. We provide all labor, equipment, materials, supplies, tools, transportation, and services to complete the project. **We do not utilize subcontractors.**

[3] Note this requires the client to provide a list of "official" Wi-Fi access points.

CIS / NIST CSF Cybersecurity Maturity Assessment

Affinity IT bases its cybersecurity assessment approach on the NIST Cybersecurity Framework (CSF) and has a deep understanding of the NIST 800-53 control set. Using the criteria defined in the framework, we can discern a level of maturity based on information gathered through documentation, interviews, and observations.

The assessment seeks to understand and calibrate the current state of activities within the organization based on the risk management steps identified by the NIST CSF (Identify, Protect, Detect, Respond and Recover). Ultimately, we are seeking to discern:

1. What are the assets connected to the network?
2. How are they currently being protected from unwanted intrusion?
3. How well does the current network detect, respond, and recover from unwanted intrusion?
4. Are there safeguards in place to ensure that the organization's most critical data is protected?
5. What is the organization's target profile and how closely does it map to the current profile?
6. What are the steps that need to be taken to reach the target profile?
7. How complete, robust, and appropriate are existing IS Policies and Plans?
8. How well are they currently being implemented within the organization?
9. How well do they align with the organization's objectives?
10. How well do they comply with all required security standards (**HIPAA, CJIS, PII, ePHI**, etc.)?

To do so we will employ interviews, observations, testing, and documentation reviews to measure the organization's current alignment with the NIST CSF. This will yield an action plan as well as a "maturity level" for the organization's cybersecurity program. Based on the score achieved, appropriate roadmaps and recommendations can then be made to further secure the organization.

When analyzing potential remediations, we carefully consider the potential effectiveness, cost, benefit, and impact on the organization of each before making our recommendations.

It is critical to identify in advance which NIST CSF activities are "in scope" and which are "out of scope" to properly demonstrate due diligence. The table on the page below displays the complete list of functions and categories that define the NIST CSF Framework. Each category in the table has subcategories, breaking down the examination effort further into its individual piece parts. From there, each subcategory examination is presented according to its "Current Tier" and "Target Tier", scoring each according to an "Implementation Tier" score defined as 1-Partial, 2-Risk Informed, 3-Repeatable, and 4-Adaptive.

Appendix A shows screen shots of a sample NIST CSF evaluation worksheet that captures the cybersecurity maturity of an organization. Notice how the examination result of each subcategory has a "Current Tier" of "Partial" and a "Target Tier" of "Repeatable". Even though the highest and best tier is "Adaptive", at present the target or goal of the organization in the example is simply to reach "Repeatable". That would be a two-tier improvement to their current state.

Understanding that targeting only a subset of the 108 controls contained within the framework is typically desired, nonetheless, Affinity IT Security is fully equipped to execute on the entire set of framework controls.

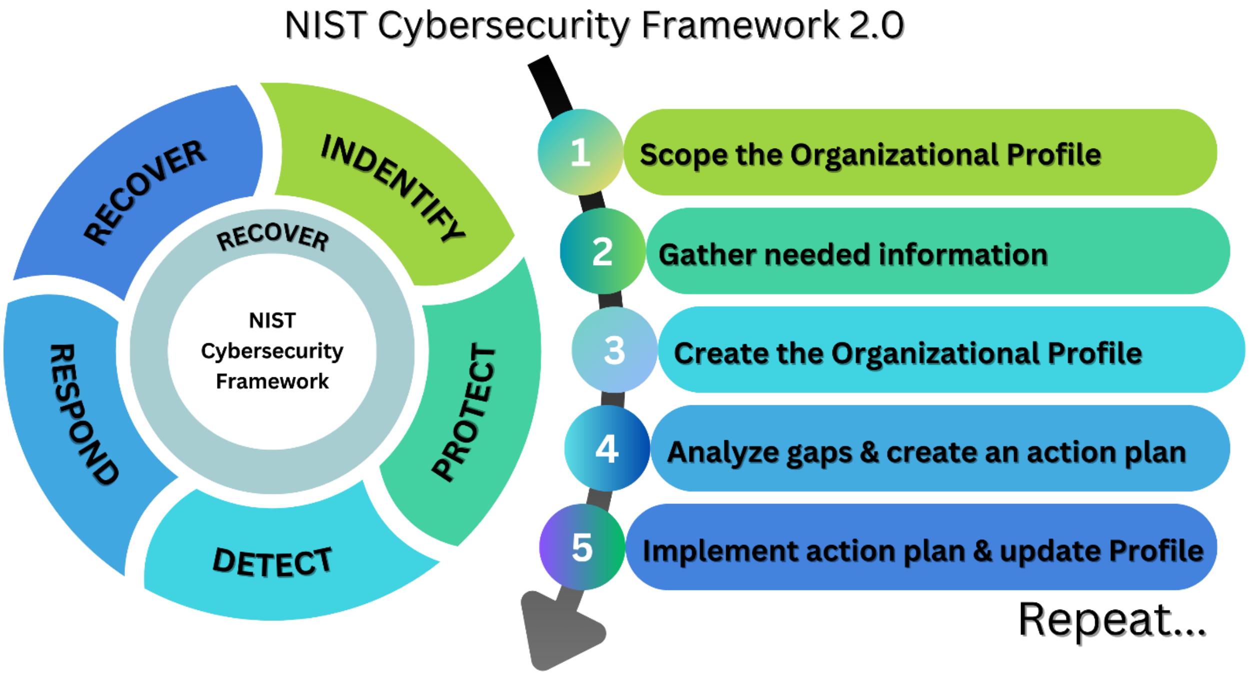

NIST Cybersecurity Framework 2.0
RECOVER
INDENTIFY
RECOVER
NIST Cybersecurity Framework
PROTECT
RESPOND
DETECT
1 Scope the Organizational Profile
2 Gather needed information
3 Create the Organizational Profile
4 Analyze gaps & create an action plan
5 Implement action plan & update Profile
Repeat...

Fig: NIST Steps for creating and using a CSF Organizational Profile

In summary, the NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes.

Social Engineering / Phishing

Our solution is highly tailored and goes considerably beyond traditional/out-of-box phishing campaign solutions such as KnowB4. We use two main tools: GoPhish and Mail-In-A-Box. This lets both Affinity-IT and clients create and run phishing campaigns. We can also send text message phishing campaigns, which many providers do not offer.

Most clients prefer us to handle everything. With our system, clients can also manage their campaigns online whenever they want. In a typical 1-year subscription plan we include up to 4 campaigns as part of our service.

Every phishing engagement begins with written permission from the client, authorizing us to proceed. Clients must also approve the content of each phishing email, ensuring they stay informed and retain control.

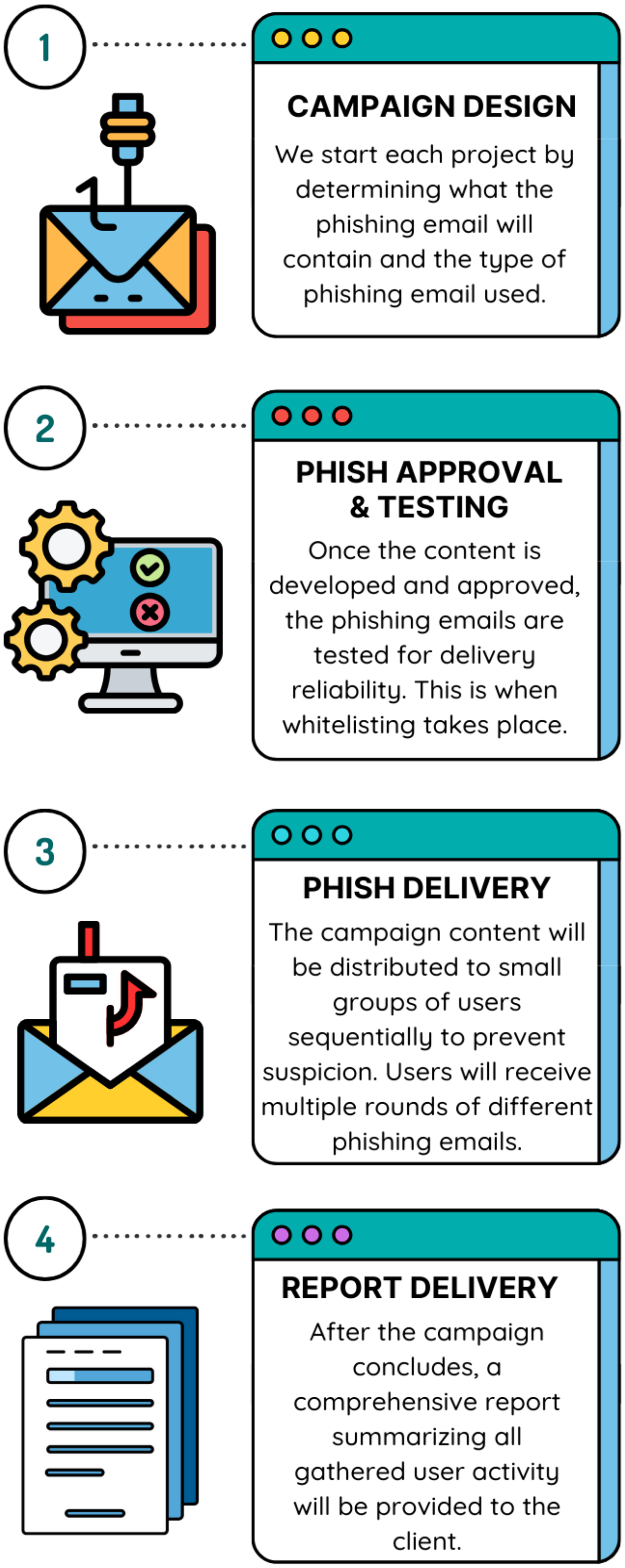
To make our phishing emails more convincing, we use special techniques. Our emails are built in a certain way to get past spam filters. On average, our fake phishing emails score well when tested against anti-spam systems.

We test everything carefully to make sure our phishing emails reach the right people, **our simulated Phish score 8.4/10 with Mail-Tester.com**, but with recent security enhancements to Email services and the implementation of zero-trust principle against unknown senders, so it's best to whitelist our emails.

Once we're sure everything is set up depending on requirements, we start sending out the phishing emails. We usually send 4 rounds of emails to each person over a period of time. Each round is a bit different, but they include trying to trick people into giving away their login details.

After each round, we collect data on how people reacted. This illuminates phishing risk and effectiveness of complementary awareness training.

We can also help with other types of security tests, like calling people on the phone or sending them text messages. We work closely with clients to make sure we get all the information we need to do a good job.



1

CAMPAIGN DESIGN

We start each project by determining what the phishing email will contain and the type of phishing email used.

2

PHISH APPROVAL & TESTING

Once the content is developed and approved, the phishing emails are tested for delivery reliability. This is when whitelisting takes place.

3

PHISH DELIVERY

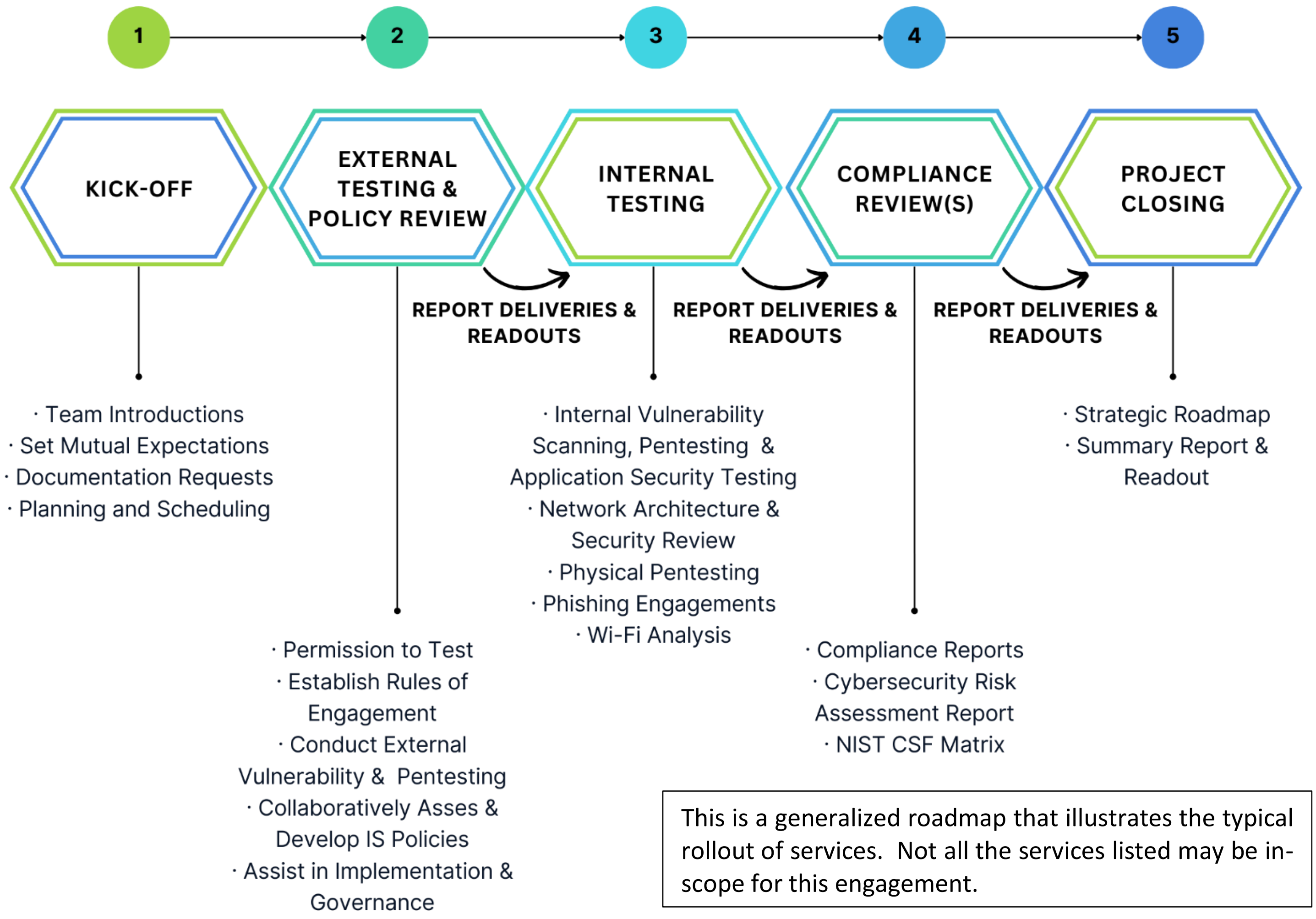
The campaign content will be distributed to small groups of users sequentially to prevent suspicion. Users will receive multiple rounds of different phishing emails.

4

REPORT DELIVERY

After the campaign concludes, a comprehensive report summarizing all gathered user activity will be provided to the client.

Project Management



1 KICK-OFF

- Team Introductions
- Set Mutual Expectations
- Documentation Requests
- Planning and Scheduling

2 EXTERNAL TESTING & POLICY REVIEW

- Permission to Test
- Establish Rules of Engagement
- Conduct External Vulnerability & Pentesting
- Collaboratively Asses & Develop IS Policies
- Assist in Implementation & Governance

REPORT DELIVERIES & READOUTS

3 INTERNAL TESTING

- Internal Vulnerability Scanning, Pentesting & Application Security Testing
- Network Architecture & Security Review
- Physical Pentesting
- Phishing Engagements
- Wi-Fi Analysis

REPORT DELIVERIES & READOUTS

4 COMPLIANCE REVIEW(S)

- Compliance Reports
- Cybersecurity Risk Assessment Report
- NIST CSF Matrix

REPORT DELIVERIES & READOUTS

5 PROJECT CLOSING

- Strategic Roadmap
- Summary Report & Readout

This is a generalized roadmap that illustrates the typical rollout of services. Not all the services listed may be in-scope for this engagement.

Affinity IT Security Services prides itself on having project management expertise that is often lacking from our competitors. **We train project managers in how to manage IT projects**. We understand how to balance **scope, time, and resources,** and how to maintain that balance throughout the lifecycle of the project, namely through meticulous initiation, planning, execution, and all the way to a successful project closure.

Our unique leadership and technical knowledge skillsets enable us to effectively **organize, plan, and communicate** collaboratively with our clients and coordinate each step of the process with their staff. As an example, this is how we can operate tasks in parallel for projects we are awarded.

Proposed Interaction

We encourage the client to create a hybrid team of responsible staff to support each test, including network and system administrators, asset owners, and developers as needs dictate. This collaborative team is kept aware of testing plans and execution, facilitates set-up and access, manages questions and answers, participates in readouts, and requests post-testing verification of fixes.

Affinity IT will present a live (web) read-out of findings for client staff that includes a detailed explanation of each finding, the associated risk, and recommended remediation. It is at the client's discretion as to who should attend this meeting. Occasionally, clients will request separate presentations for management and technical staff, and we are happy to accommodate.

Additional Assurances

Affinity IT has a deep understanding of the NIST 800-53 control set, as we advise our clients on regulatory compliance. Internally, we have implemented the following controls as appropriate for a firm of our size:

• Role-based access control	• IT Asset Management
• Patch Management	• Password Policy
• Account Management	• Business Continuity
• Mobile Device Policy	• Cybersecurity Awareness
• Physical Security	• Endpoint Security

Our **SOC2 certification** is complete. We can provide evidence of the status of this certification from an auditor if necessary. Affinity IT Security is also participating in Project Spectrum, the DoD initiative promoting cybersecurity for small businesses.

Deliverables

Our analysis of this RFP will lead to a work plan where the following deliverables are produced:

Network Penetration Test Report	Describes the vulnerabilities in devices detected through external & internal penetration testing with priorities based on severity and suggested remediations. The report also details the ethical hacking activities that were carried out (if any).
Cybersecurity Risk Assessment Report (a.k.a. Cybersecurity Risk Management Plan)	This report describes the relative risk of several cybersecurity concerns. Each is characterized and documented, yielding a prioritized strategy for improving security posture. This is the basis for the Strategic Roadmap.
Website and Web Application Security Vulnerability Report	This report describes significant un-remediated vulnerabilities that could be used to compromise the confidentiality, availability, or integrity of an application.
NIST CSF Maturity Assessment	A matrix of the NIST CSF categories and hierarchy along with a collaborate judgement regarding current maturity and practical target maturity.[4]
Social Engineering Report	This report describes remote and local attempted Social Engineering exploits and results.
Phishing Campaign Report	Summarizes Phishing campaign findings, indicating the phishing emails that have been sent to a target list provided by the client. This report details the response to those emails.
Strategic Remediation Roadmap and Implementatio Plan	Collaborative document that provides a tentative mapping of suggested Cybersecurity initiatives drawn from the Cybersecurity Risk Assessment.
Executive Summary Report	Succinct comprehensive project summary suitable for senior management.
Technical Report	All of the above reports, with the exception of the Executive Summary Report, are technical reports. Our Cybersecurity Risk Assessment Report contains relevant details from all other reports and will address this deliverable.
Comprehensive Summary Report	Detailed comprehensive project report on work performed, findings, and suggested remediations.

All reports are also presented in a live format for relevant personnel. **Each report can be amended after remediation with a "Disposition of Findings" section that details whether verification of fixes has occurred.**

Strategic Remediation Roadmap and Implementation Plan

Based on the results of the overall Network Security Assessment, we will provide a collaborative, strategic roadmap that will detail and prioritize the cybersecurity initiatives, always with an eye toward existing resources, effectiveness, cost, benefit, and impact on the organization.

[4] It is as important to recognize which NIST CSF activities should be "out of scope" to demonstrate due diligence as it is to identify those that should be "in scope".

Cybersecurity is about reducing risk to IT resources, and the traditional approaches to risk management are applicable. As with other domains of risk-reduction, there are diminishing returns as one continues to attempt to reduce risk. The cost of reducing risk rises as additional, increasingly less effective, and more burdensome tactics are implemented to further reduce risk. Some will have you believe that the right combination of products will eliminate the risk of breach or loss, but history dictates otherwise.

The correct strategy is to identify your risks, analyze them for probability and impact, and prioritize them accordingly. Then, working in priority order, devise one or more strategies for addressing each risk. Finally, choose which strategies to implement and when, based on a cost/benefit analysis of your options. The result should be a multi-year practical and cost-effective risk-reduction plan.

While there can never be a guarantee of invulnerability, we will work side-by-side with you to accomplish an effective strategy towards Cyber Resilience.

The results of the Cybersecurity Assessment will dictate a strategy that will look to ensure:

1. Regular Data Backups stored offsite in a safe, secure location.
2. Properly configured firewalls are deployed to protect each network segment.
3. Anti-Virus Software and/or Endpoint Security solutions are deployed and consistently updated.
4. A Strong Password Policy is adopted and maintained.
5. Sensitive Information is protected in Storage and in Transit.
6. Employees routinely complete Cybersecurity Awareness Training.
7. Network Security Testing is conducted regularly:
a. External Penetration Testing
b. Network Vulnerability Assessments
c. Server Vulnerability Assessments
d. Endpoint Assessments
e. Website Assessments
f. Operational Security Assessment
8. Hardware and Software Assets are inventoried.
9. All IT assets are routinely Patched.
10. Practical and Effective IS Policies, Procedures, Governance and Training are implemented and maintained.

The services we provide as cybersecurity consultants allow us to significantly reduce cybersecurity risk and create cyber resilience for our clients across the board. For this we take pride and derive great satisfaction. However, our expertise often extends beyond the scope of our contracts, allowing us to identify risks that are left as “not fully addressed” since they are often not fully in scope.

As an example, there is often a lack of focus on all aspects of Social Engineering, which is still the most effective attack vector for gaining access to client networks. According to the FBI, social engineering techniques were responsible for 20% of all data breaches in 2022 and have increased more than tenfold in the last 3 years, leading to reported losses exceeding $6.9 billion.

Organizations frequently mandate canned online tutorials for their employees, passing them off as proper Cybersecurity Awareness Training. Employees gain little from this exercise, often leaving them disillusioned by the same old worn-out content. Our online training seminars deliver live, customized updated content that achieves an interactive and effective knowledge transfer rather than self-paced training modules.

For these reasons, we encourage our clients to take a closer look at each cyber category to consider the risks that can accompany the failure to properly address all areas of potential compromise. This kind of comprehensive expertise is why we often maintain long-term relationships with our clients.

References

REFERENCE 1

Client Business Name:	**City of Charleston, West Virginia**
Primary Industry:	**Municipality**
Dates of contract:	April 2022 to Present
Point of Contact (POC) Information	
Name:	**Adam Cottrell**
Title:	Interim IS Director/GIS Manager
Email Address:	adam.cottrell@cityofcharleston.org
Phone Number:	**(304) 308-8048 x145**
Office Address:	**612 Washington St E** **Charleston, WV 25301**

REFERENCE 2

Client Business Name:	**Summit County, Colorado**
Primary Industry:	**Municipality**
Dates of contract:	January 2024 to Present (Ongoing)
Point of Contact (POC) Information	
Name:	**Neal Stolz**
Title:	Information Systems Director
Email Address:	Neal.Stolz@summitcountyco.gov
Phone Number:	**(970) 453-3423**
Office Address:	**501 N Park Avenue** **Breckenridge, CO 80424**

REFERENCE 3

Client Business Name:	**City of Glendale, California**
Primary Industry:	**Municipality**
Dates of contract:	November 2022 to Present
Point of Contact (POC) Information	
Name:	**Jason Miller**
Title:	Assistant CIO
Email Address:	jmiller@glendaleca.gov
Phone Number:	**(818) 550-4520**
Office Address:	**141 N. Glendale Avenue** **Glendale, CA 91206**

Past Involvement with Similar Projects

Affinity IT Security services a broad spectrum of industries and are pleased to cite an impressive array of clients, many of whom have a global presence. Our client portfolio includes many **government municipalities and household names in the healthcare, financial, and insurance industries.** We do not list them all publicly due to NDA restrictions but are happy to discuss them. You will benefit from similar discretion.

Our experience has taught us that cybersecurity assessments are similar across industries, and that finding and documenting vulnerabilities is the critical skill set. The key skills required include strong communication, familiarity with **CIS Controls / NIST CSF, NIST 800-53**, **compliance with security standards, and project management**. Any judgment calls that must be made with respect to alternative remediations will be made collaboratively with the West Virginia Lottery Commission.

- **City of Charleston, WV (April 2022 to Present):**
  Affinity IT Security was selected from a broad field of cybersecurity consulting firms for its breadth of experience and depth of technical expertise. Our services for this client include **NIST CSF Cybersecurity Maturity Assessment, internal and external network vulnerability scanning, network penetration testing, information security policies and procedures review and gap analysis, network architecture review, CJIS Compliance and strategic roadmap and planning.**

- **Summit County, CO (January 2024 to Present) (Ongoing):**
  Summit County, CO, has approximately 31,000 residents, is one of the top outdoor destinations in the United States. Our services for this client include **internal and external network vulnerability scanning, internal and external network penetration testing, physical security penetration testing, network architecture and firewall evaluation, information security policies and procedures review and gap analysis, VOIP configuration review, wireless network testing, social engineering / phishing, and NIST CSF cybersecurity maturity assessment.**

- **City of Glendale, CA (November 2022 to Present):**
  Glendale, CA has a population of over 200,000 and is the fourth largest city in Los Angeles County. Our services for this client include **internal and external network vulnerability scanning, network penetration testing, web-application security testing, firewall assessment, wireless network testing, CJIS Compliance and physical security testing.**

- **City of Camden, NJ (February 2023 to Present):**
  With more than 73,000 residents, Camden is the 13th most populated city in the State of New Jersey, out of a total of 565 municipalities. Our services for this client include **internal and external network vulnerability scanning, network penetration testing, web-application security testing, social engineering / phishing, policies and procedures review, network architecture review, and strategic roadmap and planning.**

- **Consolidated Tribal Health Project, (CTHP) (March 2023 to Present):**
  CTHP services Mendocino County, CA, which has approximately 88,000 residents, most of whom live in unincorporated areas throughout the county. Our services for this client include **internal and external network vulnerability scanning, internal and external network penetration testing, network architecture and firewall evaluation, information security policies and procedures review and gap analysis, VOIP configuration review, wireless network testing, social engineering / phishing, and NIST CSF cybersecurity maturity assessment.**

- **PhilaPort, The Port of Philadelphia, (CTHP) (October 2023 to Present):**
  PhilaPort is responsible for the management, maintenance, marketing, and promotion of port facilities along the Delaware River in Pennsylvania. Our services for this client include **internal and external network vulnerability scanning, internal and external network penetration testing, network architecture evaluation, information security policies and procedures review and gap analysis, wireless network testing, social engineering / phishing, and NIST CSF cybersecurity maturity assessment.**

NDAs for these projects do not allow us to disclose certain proprietary details including exact final costs as well as any challenges encountered during this work. But we can share that all 6 efforts were very successful. The contact information details for the first 3 referenced projects shown here are listed in the references section above.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: LOT2400000009

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)

[X] Addendum No. 1

[ ] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] 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.

Affinity IT, LLC
Company

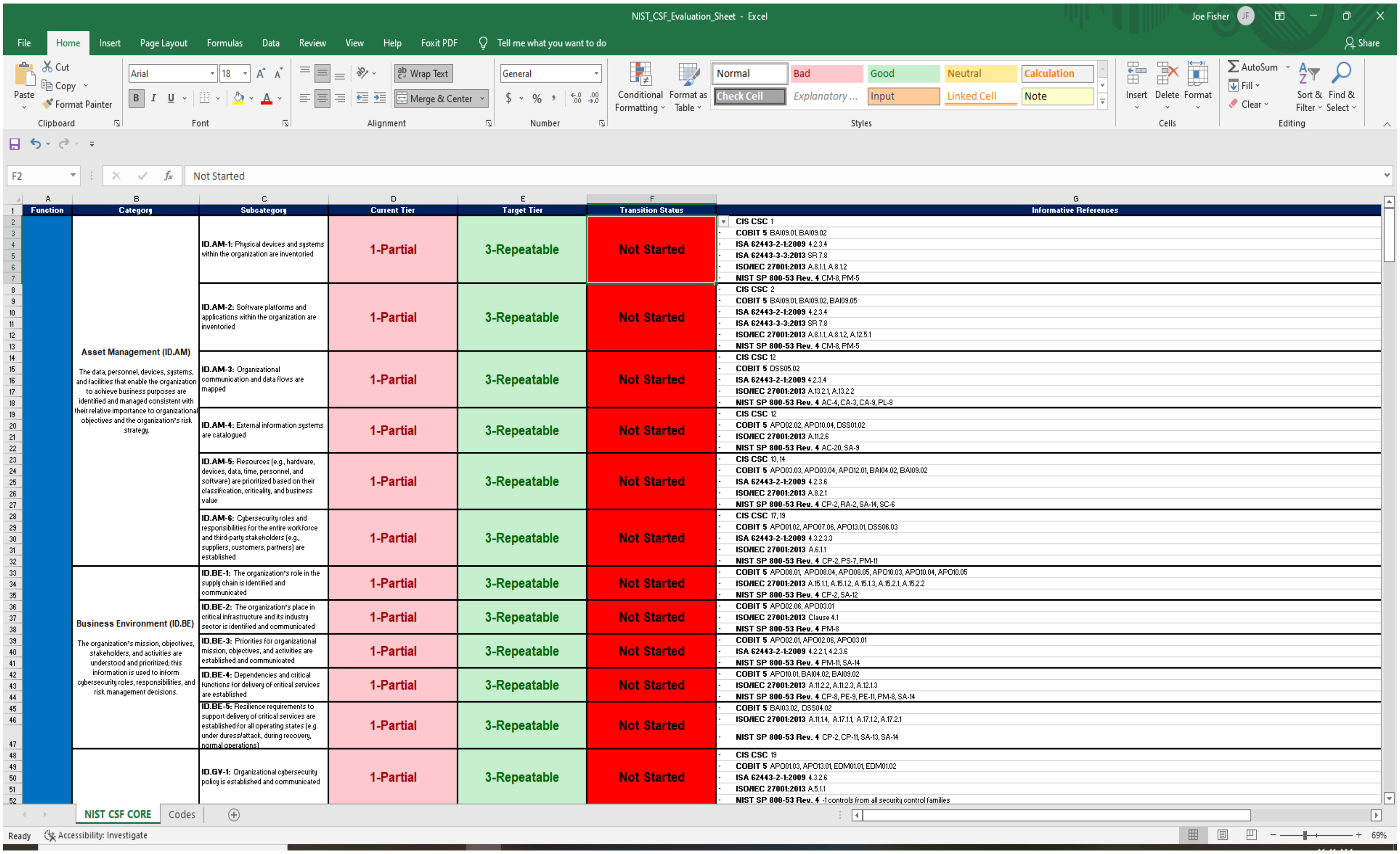
Joseph W Fisher
Authorized Signature

3/28/2024
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Appendix A: NIST CSF Evaluation Worksheet

The following are screenshots of the Excel worksheet we use to capture the current cybersecurity maturity of an organization as well as targeted future states. The spreadsheet can serve as a dashboard to demonstrate progress towards documented targeted CSF Profiles. Only a small sample of the CSF is shown.



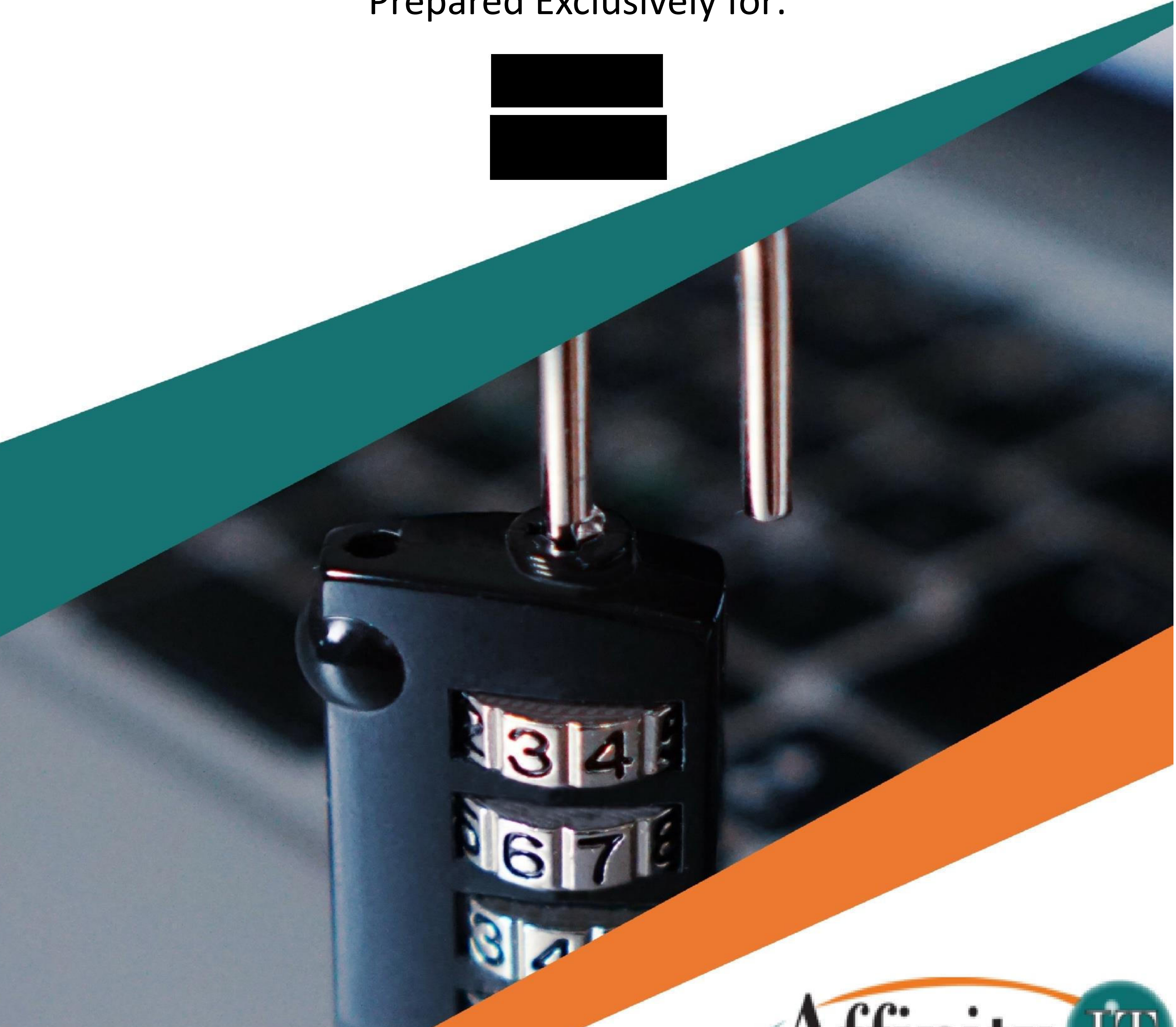
Function	Category	Subcategory	Current Tier	Target Tier	Transition Status	Informative References
	Asset Management (ID.AM) The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	1-Partial	3-Repeatable	Not Started	**CIS CSC** 1 - **COBIT 5** BAI09.01, BAI09.02 - **ISA 62443-2-1:2009** 4.2.3.4 - **ISA 62443-3-3:2013** SR 7.8 - **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 - **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	1-Partial	3-Repeatable	Not Started	- **CIS CSC** 2 - **COBIT 5** BAI09.01, BAI09.02, BAI09.05 - **ISA 62443-2-1:2009** 4.2.3.4 - **ISA 62443-3-3:2013** SR 7.8 - **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 - **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	1-Partial	3-Repeatable	Not Started	- **CIS CSC** 12 - **COBIT 5** DSS05.02 - **ISA 62443-2-1:2009** 4.2.3.4 - **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 - **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	1-Partial	3-Repeatable	Not Started	- **CIS CSC** 12 - **COBIT 5** APO02.02, APO10.04, DSS01.02 - **ISO/IEC 27001:2013** A.11.2.6 - **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	1-Partial	3-Repeatable	Not Started	- **CIS CSC** 13, 14 - **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 - **ISA 62443-2-1:2009** 4.2.3.6 - **ISO/IEC 27001:2013** A.8.2.1 - **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	1-Partial	3-Repeatable	Not Started	- **CIS CSC** 17, 19 - **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 - **ISA 62443-2-1:2009** 4.3.2.3.3 - **ISO/IEC 27001:2013** A.6.1.1 - **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE) The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	1-Partial	3-Repeatable	Not Started	- **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 - **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 - **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	1-Partial	3-Repeatable	Not Started	- **COBIT 5** APO02.06, APO03.01 - **ISO/IEC 27001:2013** Clause 4.1 - **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	1-Partial	3-Repeatable	Not Started	- **COBIT 5** APO02.01, APO02.06, APO03.01 - **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 - **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	1-Partial	3-Repeatable	Not Started	- **COBIT 5** APO10.01, BAI04.02, BAI09.02 - **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 - **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	1-Partial	3-Repeatable	Not Started	- **COBIT 5** BAI03.02, DSS04.02 - **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 - **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
		ID.GV-1: Organizational cybersecurity policy is established and communicated	1-Partial	3-Repeatable	Not Started	- **CIS CSC** 19 - **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 - **ISA 62443-2-1:2009** 4.3.2.6 - **ISO/IEC 27001:2013** A.5.1.1 - **NIST SP 800-53 Rev. 4** -1 controls from all security control families

Appendix B: Sample Executive Summary Report

Cybersecurity Risk Assessment Report – June 2023

Prepared Exclusively for:

[redacted]



AFFINITY-IT-SECURITY.COM
(800) 840-2335
1243 SUSSEX TURNPIKE, RANDOLPH, NJ 07869

This confidential document has been produced by Affinity IT Security Services exclusively for [redacted] Inc.

This report details the results of network security testing performed in accordance with the corresponding Consulting Services Agreement (CSA). The findings and recommendations provided in this report reflect the state of the client network at the time of testing. Although every effort is made to maximize vulnerability detection, results must never be considered fully comprehensive of all security issues due to the volatile nature of networks and potential vulnerabilities.

Questions may be directed to:

Affinity IT Security Services
1243 Sussex Turnpike, Suite #1
Randolph, NJ 07869
(800) 840-2335
info@affinity-it.com

Date: June 30, 2023

Contents

Introduction

Affinity IT Security has been engaged by [redacted] Inc. ([redacted] to analyze and document their current security posture, to propose improvements, and to consult on remediation. [redacted] operates a dual use (manufacturing and office) facility located in [redacted] [redacted]. The company employs 175 employees. The [redacted] is part of the [redacted] Group of companies but was not part of this assessment.

Operational Overview

The manufacturing and office facility produces a variety of [redacted] products. In addition to dedicated office space for business functions, offices directly supporting manufacturing operations such as quality assurance and R&D are interspersed throughout the facility. Most manufacturing processes are managed and controlled by technicians. Operational Technology (OT) is minimal as the various mixing processes are primarily achieved by hand. Technicians rely on Windows systems mainly for tracking, shipping, and mixing compounds. Wireless networking is available throughout the facility. The company is not currently subject to any regulatory requirements with respect to cybersecurity. In 2022 the company experienced a concerning network breach, which was later determined to be a network anomaly and is now even more motivated to reduce its risk and gain more visibility into its network and operations.

The IT environment is receiving an overhaul in 2023. The main office productivity suite will shift from Google G Suite to Microsoft 365. The legacy ERP system will be upgraded to a PaaS Cloud based solution. Asset tracking will shift to Microsoft Intune. These changes will have a positive impact on the [redacted] IT environment by eliminating many shortfalls described below, but also introduce new challenges to the IT department.

Observations

Security associates from Affinity IT Security visited the [redacted] headquarters on April 25th and April 26th, 2023, to inspect the facilities and interview staff. The following are observations from those visits.

IT Support

- IT support is conducted in-house.
- Office and email applications are currently utilizing Google G Suite but will shift to Microsoft 365 for applications and Microsoft Intune for asset management by the end of summer 2023.
- The [redacted] database relies on a heavily customized legacy AS400/S2K ERP system. The AS/400 is the platform and S2K is the ERP software itself.
- Rbase software is used for labeling and hazard markings and for import/export documents.

Physical Security

- The [redacted] premises are fenced and gated. Access through the gate must be granted via intercom, but Affinity IT observed that no challenge/inquiry of our visit was issued, as we were granted access to premises without verification or identification.
- Access to the main office building is granted via intercom. A challenge was issued during our visit. In addition, visitors must have a scheduled visit and a point of contact within the company to enter the building.
- All employees are required to access the building via magnetic RFID cards which are role and time-based.
- The building is equipped with a fire and burglar alarm system. A total of 19 management team members have access to this alarm to enable and disable it, with 4 (of 19) individuals having remote access to enable or disable the alarm. Front door access is restricted until an "alarm user" has swiped their card to open the door.
- There are over 100 cloud-based security cameras deployed throughout the exterior and interior of the premises. Cameras are located in the office, production, warehouse, garlic room, and outdoors. IT has full admin access and Human Resources has full read access. Other teams (Manufacturing production, Quality/Regulatory) have access to view cameras in their respective areas. Footage is stored on each camera for 30 days and then indefinitely in Verkada’s cloud solution (when video is archived).

Information Security Policies

- [redacted] Information Security Policies, dated December 12, 2022, were provided to Affinity IT on 4/27, 2023. These policies were analyzed along with the Employee Handbook, and recommendations were issued in a separate report entitled "Information Security Policy Gap Analysis".

Access Control

- The password policy is 8 characters, alpha numeric and one upper case character. This is not formally documented in the [redacted] official security policy.
- Password rotation is enforced every 180 days. This is not formally documented in the [redacted] official security policy.
- Users are placed in Role-based access control groups, permitting access to resources they are allowed. This is not formally documented in the [redacted] official security policy. Each department has a security group as well as more specialized groups (i.e., Bulking View).
- There is no specific password policy. Users are instructed to utilize separate passwords for workstations and applications. Forbidding the sharing of passwords is noted in section 12 of the HR policy.
- The Customer Care Department shares email inbox passwords. When someone from the Customer Care Department is absent, others in Customer Care need to be able to access the email account of the individual that is not available, to follow up on customer issues that he or she may have been actively working.

- Desktop passwords are shared in the test lab for 3 workstations running bench software for logging and GCMS testing purposes.
- Desktop passwords are also shared in the production environment with only label printing workstations sharing a password. Two users in the production office currently share passwords but will be switching to their own login.
- On multiple occasions we observed users often leaving their desktops unlocked and unattended. This violates the “Clean Desk Guidelines" of [redacted]s Information Security Policy:

  “[redacted] owned computing devices must be session locked when not in use or when left unattended. A password must be required to unlock session lock.”

- Remote access to the internal network is achieved via a VPN. Users are required to provide a login and password as well as complete a two-factor authentication challenge.
- No two-factor authentication challenge is required for access to the Paycom HCM application which is cloud delivered and accessed from anywhere. This application is used to house HR and payroll information. Multi-factor authentication is required, however, for management access.
- Two-factor authentication is currently required for access to email, and Microsoft 365. Multi-factor authentication will be implemented for the new ERP systems through Single-Sign-On. Presently, there is no specific multi-factor authentication policy.

Employee Cybersecurity Awareness

- Phishing campaigns are conducted regularly, but interviewed employees indicated there is a lack of feedback from conducted campaigns. Interviewees expressed interest in campaign data and general information on how to better identify phishing emails.

Confidentiality

- There is no mechanism in place for individuals who would like to send an encrypted email. In addition, there is no policy or procedure in place for email encryption.
- Laptops are encrypted via BitLocker, referred to in section 4 of the Information Security Policy.

Business Continuity and Disaster Recovery

- Backups are tested only with the “AS400” ERP system, and not with the overall network operations.
- BCP and DR are not yet formally documented.
- There is a DR plan for the existing ERP system. But a more comprehensive plan needs to be developed for the entire organization. This is one of the tasks that is currently backlogged.

Incident Response

- Incident response is also not yet formally documented.

Logging and Monitoring

- There is currently no logging policy. Native logs are rolled over on the source systems as needed. SentinelOne logging capabilities are being examined as a possible permanent login solution.

Governance

- There is no Governance Policy defined or implemented within the firm.

Asset Management

- Mobile Device Management for issued work phones is achieved through AirWatch. This will be switching to Microsoft Intune in the near future.
- There are 23 issued cell phones with which users are allowed to install any/all applications from the application store. There is no application black/whitelisting in place.
- Windows assets are tracked on Google Sheets and Microsoft Intune in the near future.

Network Management

- The current network configuration is characterized by a lack of redundancy. There are many single points of failure.
    - There is a single ingress/egress firewall (Cisco 1140) for the entire network.
    - There is a single core network switch that is past end-of-life (i.e., no longer supported by the manufacturer). Should this switch fail, all productivity would halt, including the manufacturing floor.
    - All the Intermediate distribution frame (IDF) switches as well as the Wi-Fi access points are end-of-life.
- Networking equipment that can be updated are updated. Devices that are at the end of life are not. This is documented in section 3.6 of the Information Security policy.
- A newly connected device added to the network would not be detected.
- During our visit it was observed that one access point had a security setting configured to Wired Equivalent Privacy (WEP) and was accessible from the parking lot.
- There are no redundancies regarding the Internet Service Provider servicing the facility.
- There is no power backup for the IT environment.
    - The server room is not covered by the building generator. The servers support only a 2-hour battery backup.
- There are sporadic Wi-Fi drops that occur on the manufacturing floor. The reason for the outages is not known. The issue is usually addressed within several hours. Two Wi-Fi outages have occurred over the last 6 months.

- The current network configuration does not employ proper network segmentation. The network is flat. Of particular concern is that the OT network is separated from the IT network via VLANs. There is no secure subnetwork for critical assets.
- The OT systems utilize on-premises Active Directory except for one machine. One "Mass Spec" machine is only local user by vendor design.
- The SentinelOne S1 platform is deployed across all OT Systems except for the "Mass Spec" machine. The vendor will not allow third party applications to be installed.
- QC and GC PCs have one login to gain access to the controlling program. The controlling app can only be opened once on the computer which is why a shared login is utilized.
- There are no special considerations for the OT/Lab machines at this time (for example stricter firewall rules)? The current plan for a network upgrade includes tighter VLAN separation.
- The label printing workstations have a shared account with a password that changes every 120 days (about 4 months). There are also three Kiosk workstations that have web access to company portals (HR related). There is no password to access these workstations, however after 20 minutes of inactivity it is logged out, history and cache cleared and waits for a new user to log back in. The user also has the option to log out themselves as well.
- There is one account for each label printing workstation that all of production knows the password to. This is a limited account for label printing purposes. There are 4 of these label printing workstations. The Kiosk has no log on password.
- Access to all network closets is strictly controlled.
- Port security is not implemented. All ethernet network ports are active throughout the [redacted] facility. During our walkthrough of the production hanger, we observed easily accessible IDF switches located next to workstations. These devices were not secured in any way and could be easily compromised given that many of the physical ports were open.
- The Guest Wi-Fi is tracked and utilizes the same ISP but is logically separated from the IT network. There is currently no Wi-Fi policy. For employees, anyone who has an MDM managed device is granted Wi-Fi access. Guests are allowed access to the Guest Wi-Fi network upon formal request and access remains for the duration of their visit.

Data Security

- Currently all data and applications reside on premises, but this will soon change as the legacy ERP system will migrate to the Cloud third-party provider (within the next 6 months). The ERP System is backed up on tape daily. It is then taken off-site to an employee's home residence.
- There are no policies that define the offsite backup process but there are procedures.
- User files are stored on local PCs, on the cloud and on network attached storage.

Patch Management

- Windows updates are pushed via WSUS. For remote laptops once a VPN connection is made to the internal network, the patch state is checked, and the system is updated if needed.
- Server updates are applied automatically on Sundays unless manual intervention is needed.
- The AS400 ERP is updated quarterly.
- ERP data is encrypted both at rest and in transit.

Vulnerability Management

- Vulnerability assessments are conducted annually by third party IT security firms.

Endpoint Security

- At the time of our visit, the hosts were secured by Symantec Endpoint Security, but this has since changed to Sentinel One EDR.

Risk Summary and Recommendations

This section summarizes the major categories of cybersecurity risk that we believe are relevant to the firm, charted with the perceived likelihood of occurrence and severity of impact. Each category is described below along with the rationale for the risk/impact ratings and remediation recommendations.

Network Redundancy

- Risk: High
- Impact: High

We identified network uptime as the highest single point-of-failure in the [redacted] network due to several compounding factors:

- The existing network lacks redundancies on multiple levels.
  - If the main ingress/egress firewall should fail or become comprised, all productivity would cease.
  - If the Core networking switch, which is End-of-Life (EOL), should fail or become comprised all productivity would also cease.
- Intermediate distribution frame (IDF) switches that are distributed throughout the [redacted] network are also EOL. If any of these physical devices fail due to age, not only will productivity be affected in the immediate area, but WI-FI access point connectivity, attached to that specific IDF, will also lose connectivity. This in turn would halt manufacturing floor production in the affected areas.

  - There is a plan in place to deploy additional wireless access points on the manufacturing floor for greater Wi-Fi coverage, which may affect throughput of EOL IDF switches and introduce more intermittent loss of connectivity.
- There is currently no ISP redundancy. If the Internet Service Provider should lose connectivity all internet access would cease.
- [redacted] utilizes two ISP vendors [redacted] for redundancy. Both fiber lines travers the same utility poles from [redacted] This could prove problematic should a pole or line become damaged as it would disrupt both ISP connections.
- There is no backup generator for IT resources.
- There is no network detection capability to identify newly connected assets.

Recommendation(s):

1. Fortify the redundancy of the network by deploying additional failover network devices starting with the core network switch. At a minimum the core switch should be modernized, and a second switch should be added for redundancy. This process should flow to the remaining network IDF switches and end at the wireless access points. Lastly, an additional external firewall should be added to further high availability and redundancy. These improvements would also provide the additional data throughput needed as the network grows in the coming years.
2. Install a backup generator for IT systems.
3. Ensure Internet Service Provider (ISP) availability by installing an ISP line that connects to the building from a different geographical location, ensuring high availability should one of the utility poles/lines become damaged.

DISPOSITION: The IT department is looking into different vendors ([redacted] that would each take a different path into [redacted].

Compounding all these factors is that the [redacted] database is moving from an on-premises solution to a Cloud-based solution, putting further reliance on the single ISP. Having no backup generator for IT systems as well as the need to expand the internal wireless network throughout the production area, could further strain outdated network switching equipment.

Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

- Risk: High
- Impact: High

There is no BCP in place nor is it practiced. This is also addressed in the “IS Policy Gap Analysis” report but is re-emphasized here. The lack of a BCP and Disaster Recovery Plan (DRP) places the survival of the organization in jeopardy should serious process impacting events occur.

Recommendation(s):

1. A realistic, practical, and effective BCP should be developed and tested as soon as possible.

Incident Response Management

- Risk: High
- Impact: High

The lack of a plan to deal with cybersecurity incidents means that the response will be ad-hoc, slower and less efficient than if it had been anticipated and properly planned. It also suggests that mistakes will be made in the absence of pre-planned clear thoughtful direction. This increases the likelihood that a containable event will become more widespread, and that forensic evidence will be lost.

Recommendation(s):

1. A realistic, practical, and effective Incident Response should be developed and tested as soon as possible.

Wireless Security

- Risk: Low
- Impact: High

One wireless access point on the production floor was identified as using the Wired Equivalent Privacy (WEP) security algorithm. WEP is an outdated standard that can be compromised within minutes. Additionally, concerning is that the WEP signal reached the parking lot, which would allow a malicious actor to easily hack into the production network from the comfort of his car. Given that we were not challenged at the gate, it would have been trivial to pull up near the production area, drop all active WEP connections, record the reconnect sequence and obtain full access to the production network.

Recommendation(s):

1. Immediately change the security setting to WPA2 or higher, even if it means replacing the existing wireless access point to achieve that level of security.

No Significant Security Event Logging Mechanism

- Risk: Low
- Impact: High

There is no significant security event logging mechanism in place to allow for investigating security breaches. There was a network security incident recently detected but since no significant security event logging management solution was in place, it was impossible to determine the source of the event. Event logging details were available for only 2 or 3 days.

Recommendation(s):

1. At a minimum, increase logging capture to as long as the storage capability allows. A good place to start is 30 days, after which, log rotation can start to occur. Alternatively, implementing a security event log management (SIEM) solution is an option, but implementing such a solution requires higher financial and manpower resources.

DISPOSITION: The recent deployment of Sentinel One EDR should provide great visibility into Windows machines.

Network Segmentation

- Risk: Low
- Impact: High

The [redacted] network is flat with no Demilitarized Zone (DMZ) for hosts and a secure subnetwork for critical database systems and OT systems. Should an IT host become compromised through a phishing campaign, there are no further internal barriers (internal firewalls) protecting the ERP system or the OT network, segmented on a separate VLAN. In addition, many of the network switches are EOF, which could allow hackers to "VLAN hop" to the OT network.

Recommendation(s):

1. Separate the critical systems by deploying a secure subnetwork located behind an additional firewall. The risk level is low given that [redacted] will soon be transitioning to a Cloud ERP solution.

Port Security

- Risk: Low
- Impact: High

During our visit it was observed that all network ports were active and port security was not enabled.

Anyone with access to a network port could deploy a personal or rouge network device. The same was observed on the production floor at which some workstations had small 4-6 port hubs/switches easily accessible for anyone to tamper with.

Recommendation(s):

1. Port security can be a challenge in a "live" network. At minimum, we would encourage locking down access to all hubs/switches. If feasible, software MAC filtering should be enabled. If not, physically disabling ("un-patching") unused ports should be considered.

Phishing training and user feedback

- Risk: Low
- Impact: High

Some employees mentioned that they had not received anti-phishing training. In one instance an employee was successfully phished without ever receiving remedial training or feedback on how to identify phishing emails. Other employees expressed interest in phishing email campaign results to learn and identify malicious phishing techniques.

Recommendation(s):

1. In addition to annual phishing campaigns, [redacted] should consider providing their employees with a review of how well the company performed as a whole and illuminate them to the latest techniques used by phishing scammers.

DISPOSITION: The company sends out periodic informational emails with tips and tricks how to identify phishing emails and is currently looking into further leveraging their KnowBe4 license for user training.

Unlocked Workstations

- Risk: Low
- Impact: High

Walking through the office space, we observed many users leaving their workstations unlocked and unattended, potentially allowing anyone access to their account/data. This violates the "Clean Desk Guidelines" of [redacted]s Information Security Policy.

"[redacted] owned computing devices must be session locked when not in use or when left unattended. A password must be required to unlock session lock."

Recommendation(s):

1. Ensure all employees understand and observe organizational policies and procedures.
2. Provide reminders in the form of informational emails, and remedial training for repeat offenders.

DISPOSITION: The IT department has pushed out the issue to employees via informational emails, posts on company monitors/intranet as well as individual consulting.

Lack of Policy/Documentation

- Risk: Low
- Impact: High

The following Policies were missing:

- Password Policy
- Roles and permissions Policy
- No logging Policy
- Backup Policy
- Wi-Fi Policy

- Email Encryption Policy

Information on Information Security (IS) Gap analysis will be addressed in a separate document.

Physical Access Control

- Risk: Medium
- Impact: Medium

Upon our entrance to the [redacted] premises, we were not challenged over the intercom as to the purpose of our visit. The main gate was opened without question or challenge. We were however challenged at the building entrance intercom, at which we had to state the purpose of our visit and provide a point of contact.

Recommendation(s):

1. Anyone without permitted access to the premises should be challenged at the entrance gate and turned away if not scheduled for a visit.

Mobile Device Application Whitelisting

- Risk: Medium
- Impact: Medium

The company provided cell phones have the application store unlocked. There is no application black/whitelisting in place. Considering that not all applications are safe, and users utilize the devices for business purposes, the IT team should consider locking down the "App store".

Recommendation(s):

1. Do not allow users to install applications on the company devices by locking down the application store.

Account Sharing

- Risk: Low
- Impact: Medium

During our interview process, we identified that members of the Customer Care department share email inbox accounts/passwords. Account sharing is bad practice as it introduces a lack of accountability and attribution.

Recommendation(s):

1. Construct a general account for the Customer Care department that can be shared amongst users.
2. Ensure proper policies are in place and enforced, clearly stating that account sharing is not allowed.

DISPOSITION: IT is currently working with Customer Care to resolve the password sharing issue by use of delegated mailbox access.

No Email Encryption

- Risk: Low
- Impact: Low

While not all [redacted] employees require email encryption, there are some that identified the need for it during our interview process. Email encryption helps protect private information, sensitive data, and can enhance the security of communication between client apps and servers. In essence, when your data is encrypted, even if an unauthorized person or entity gains access to it, they will not be able to read it.

Recommendation(s):

1. Provide mechanisms, training, policy, and procedures for users that require secure email transfer.

Summary and Conclusion

Improving cybersecurity is an ongoing process of diligence, assessment, and remediation. The relative risk of several cybersecurity concerns has been characterized and documented, yielding a prioritized strategy for improving cybersecurity posture. These priorities should guide the selection of remediation and improvement strategies and order their implementation.

Appendix C: Sample Technical Report

External Network Security Report [redacted]

Prepared Exclusively for:

[redacted]

Affinity IT
SECURITY SERVICES

AFFINITY-IT-SECURITY.COM
(800) 840-2335
1243 SUSSEX TURNPIKE, RANDOLPH, NJ 07869

This confidential document has been produced by Affinity IT Security Services exclusively for [redacted]

This report details the results of network security testing performed in accordance with the corresponding Consulting Services Agreement (CSA). The findings and recommendations provided in this report reflect the state of the client network at the time of testing. Although every effort is made to maximize vulnerability detection, results must never be considered fully comprehensive of all security issues due to the volatile nature of networks and potential vulnerabilities.

Questions may be directed to:

Affinity IT Security Services
1243 Sussex Turnpike, Suite #1
Randolph, NJ 07869
(800) 840-2335
info@affinity-it.com

Table of Contents

Executive Summary

Introduction

This report details the results of Network Penetration Testing conducted by Affinity IT Security for [redacted] in April 2023. The assessment entailed the remote scanning of external (publicly accessible) servers, network devices, and web-based applications. The work was performed with permission as an ethical hacking exercise to gain insight into any exposed security vulnerabilities.

This report contains sensitive information and should be treated accordingly. This report potentially describes significant un-remediated vulnerabilities that could be used to compromise the confidentiality, availability, or integrity of information or servers.

This report reflects the findings and opinions of the assessment team with the goal of presenting actionable findings whose remediation will significantly reduce the risk of breach to the client.

The IP Range scanned was:

- [redacted]
- [redacted]
- [redacted]

There were:

- **3** Hosts detected
- **4** Total Findings
- **1** High priority findings detected
- **3** Medium priority findings detected

These results demonstrate inadequate hardening processes by the administer of the external hosts.

Our observation is that the [redacted] external network, as observed during the course of our testing, represents some cybersecurity risk to the organization, and the High severity finding (i.e. SNMP enumeration) should be addressed as soon as possible.

Note that periodic testing and evaluations are always recommended to recognize new vulnerabilities and risks that may emerge over time, as well as configuration and infrastructure changes.

Assessment Team

The following individuals participated in the assessment process and the preparation of this report:

Name	Signature
Joseph W. Fisher, CEH	
Konrad P. Gawronski, CEH	

Acknowledgments

We would like to thank [redacted] for support and time in facilitating the testing on the client side.

Summary of Scope

The following IPs were examined in the course of this assessment and the following (3) hosts were detected and scanned:

Host(s) Detected:

IP	Critical	High	Medium	Notes
[redacted]	0	0	0	
[redacted]	0	1	1	
[redacted]	0	0	1	
Total	**0**	**1**	**2**	

Summary of Scanned Ports (By Server)

The following ports and associated services were discovered during the discovery.

Server	OS	Ports	Service	Notes*
[redacted]		tcp/80	www-http	
		tcp/443	https	
[redacted]		udp/161	snmp	SNMP v1, v2c, v3 detected.
		tcp/443	https	
[redacted]		tcp/80	www-http	
		tcp/443	https	

***Notes:** The scan detected hundreds of ports open, which have been omitted from this report for the sake of brevity. We believe this is due to the firewall configuration. Whether this is a security configuration or those services are enabled we are not able to determine. For a full list of ports, please refer to raw Nessus scan document.

Summary of Significant Findings (By Server)

IP	Finding ID	Severity	Description
[redacted]	1	Medium	SSL Certificate Cannot Be Trusted
	3	High	SNMP Agent Default Community Name (public)
	4	Medium	SSL Self-Signed Certificate
[redacted]	1	Medium	SSL Certificate Cannot Be Trusted
	2	Medium	HSTS Missing From HTTPS Server (RFC 6797)

Summary of Vulnerabilities (By Vulnerability)

Finding ID	Severity	Description	Affected Server
1	Medium	SSL Certificate Cannot Be Trusted	[redacted] [redacted]
2	Medium	HSTS Missing From HTTPS Server (RFC 6797)	[redacted]
3	High	SNMP Agent Default Community Name (public)	[redacted]
4	Medium	SSL Self-Signed Certificate	[redacted]

Vulnerability Details and Remediation

In each of the following scenarios, **the general remediation is to install the latest released version of the software or OS possible**. Alternatively, another option is to **remove applications that are no longer used** or needed. For those situations in which that is not possible or practical, we provide the specific patch information relevant to the given vulnerability.

1.	**SSL Certificate Cannot Be Trusted** The SSL certificate for this service cannot be trusted. (51192)	
Risk	Recommendation(s)	CVSS Score
M	Purchase or generate a proper SSL certificate for this service.	6.5 (v3B)

2.	**HSTS Missing From HTTPS Server (RFC 6797)** The remote web server is not enforcing HSTS, as defined by RFC 6797. (142960)	
Risk	Recommendation(s)	CVSS Score
M	Configure the remote web server to use HSTS.	6.5 (v3B)

3.	**SNMP Agent Default Community Name (public)** The community name of the remote SNMP server can be guessed. (41028)	
Risk	Recommendation(s)	CVSS Score
H	Disable the SNMP service on the remote host if you do not use it.	7.5 (v2B)

	OR Filter incoming UDP packets going to this port, OR Change the default community string.	
Relevant CVE's: CVE-1999-0517		

4.	**SSL Self-Signed Certificate** The SSL certificate chain for this service ends in an unrecognized self-signed certificate. ([redacted]	
Risk	Recommendation(s)	CVSS Score
M	Purchase or generate a proper SSL certificate for this service.	6.5 (v3B)

Additional Testing Notes and Informational Findings

- We attempted to write/alter data into the SNMPv1 configuration, but were not successful.

Tools Utilized

The following tools were employed during the course of the assessment and penetration testing effort:

Tool	Version
• Nessus Professional	8.5.1
• nmap	7.91
• Kali Linux Suite (nmapauthenticator)	2023
• ReportGen	0.3.3

References

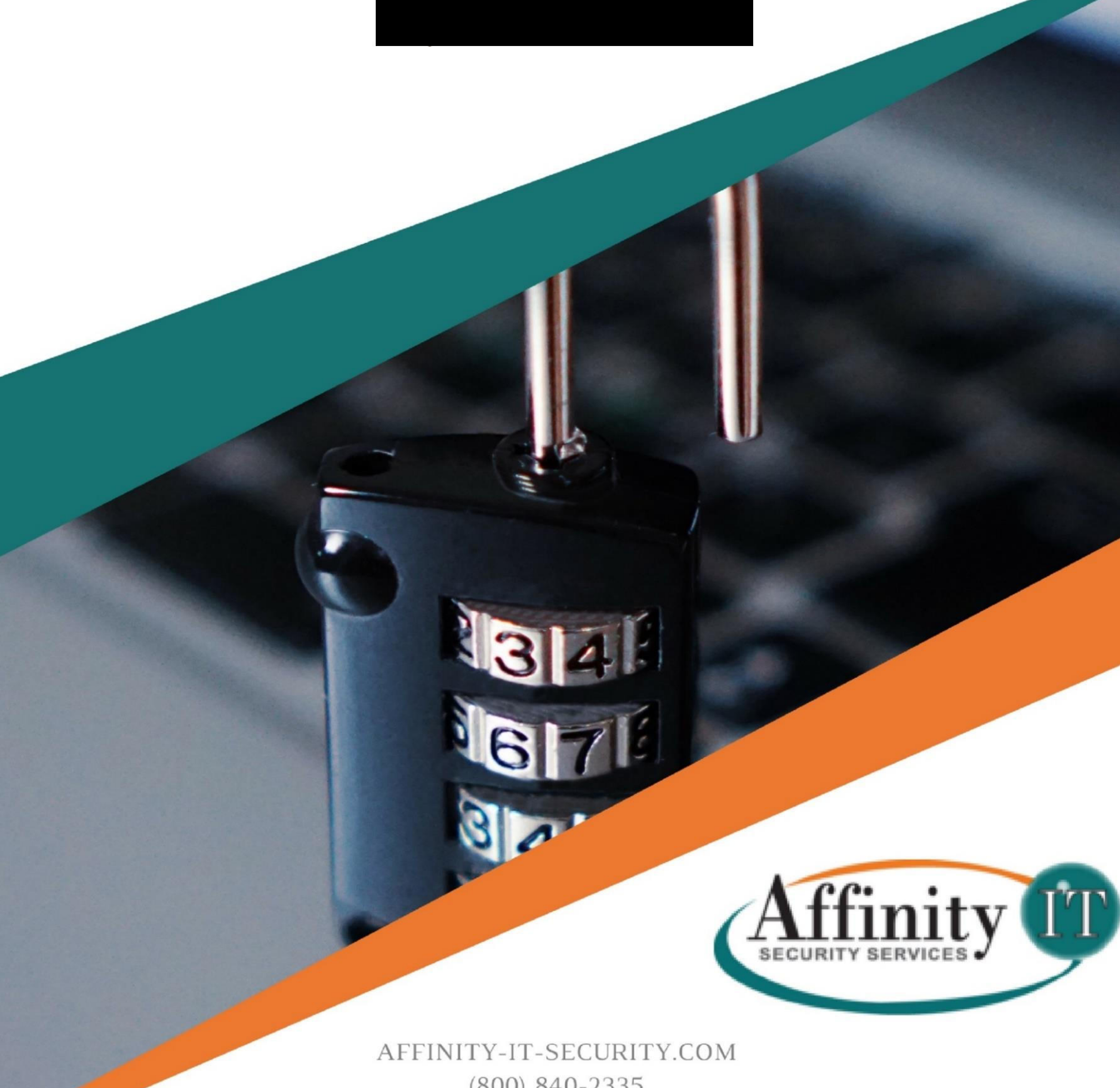
Document	**Link**
1. Common Vulnerability Scoring System v3.0: Specification Document	https://www.first.org/cvss/specification-document

Internal Network Security Report [redacted]

Critical Severity Findings

Prepared Exclusively for:

[redacted]



Affinity IT
SECURITY SERVICES

AFFINITY-IT-SECURITY.COM
(800) 840-2335
1243 SUSSEX TURNPIKE, RANDOLPH, NJ 07869

This confidential document has been produced by Affinity IT Security Services exclusively for the [redacted]

This report details the results of network security testing performed in accordance with the corresponding Consulting Services Agreement (CSA). The findings and recommendations provided in this report reflect the state of the client network at the time of testing. Although every effort is made to maximize vulnerability detection, results must never be considered fully comprehensive of all security issues due to the volatile nature of networks and potential vulnerabilities.

Questions may be directed to:

Affinity IT Security Services
1243 Sussex Turnpike, Suite #1
Randolph, NJ 07869
(800) 840-2335
info@affinity-it.com

Table of Contents

[redacted]

Executive Summary

Introduction

This report details the results of Internal Credentialed Vulnerability Scanning conducted by Affinity IT Security for The [redacted] ([redacted] in April 2023. The assessment entailed the scanning of internal servers, network devices, and workstations. The work was performed with permission as an ethical hacking exercise to gain insight into any exposed security vulnerabilities.

This report contains sensitive information and should be treated accordingly. This report potentially describes significant un-remediated vulnerabilities that could be used to compromise the confidentiality, availability, or integrity of information or servers.

This report reflects the findings and opinions of the assessment team with the goal of presenting actionable findings whose remediation will significantly reduce the risk of breach to the client.

The IP Range scanned was:

[redacted]

There were:

- **436** Hosts detected
- **357** Total Findings
- **357** Critical priority findings detected

These results demonstrate inadequate patching and hardening processes by the client of internal hosts.

Our observation is that the internal ([redacted] network, as observed during the course of our testing,poses a significant cybersecurity risk to the organization.

Note that periodic testing and evaluations are always recommended to recognize new vulnerabilities and risks that may emerge over time, as well as configuration and infrastructure changes.

Assessment Team

The following individuals participated in the assessment process and the preparation of this report:

Name	Signature
Joseph W. Fisher, CEH	
Konrad P. Gawronski, CEH	

Acknowledgments

We would like to thank [redacted] for their support and time in facilitating the testing on the client side.

Summary of Scope

The following IPs were examined in the course of this assessment and the following (436) hosts were detected and scanned:

Host(s) Detected:

IP	Critical	High	Medium	Notes
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	6	114	68	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	32	52	33	
[redacted]	0	0	0	
[redacted]	1	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	1	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	

[redacted]	6	116	75	
[redacted]	6	112	69	
[redacted]	5	112	69	
[redacted]	0	0	0	
[redacted]	6	113	70	
[redacted]	0	0	0	
[redacted]	19	101	97	
[redacted]	0	0	0	
[redacted]	6	112	70	
[redacted]	0	0	0	
[redacted]	7	114	69	
[redacted]	0	0	0	
[redacted]	23	103	90	
[redacted]	0	0	0	
[redacted]	49	85	58	
[redacted]	5	112	68	
[redacted]	5	112	69	
[redacted]	6	115	69	
[redacted]	0	0	0	
[redacted]	6	114	68	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	41	56	33	
[redacted]	6	123	79	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	6	114	69	
[redacted]	6	112	68	
[redacted]	18	47	35	
[redacted]	8	116	80	
[redacted]	0	0	0	
[redacted]	20	102	99	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	6	112	68	
[redacted]	5	112	68	
[redacted]	0	0	0	
[redacted]	8	113	76	
[redacted]	0	0	0	

[redacted]	0	0	0	
[redacted]	19	101	92	
[redacted]	6	113	68	
[redacted]	6	120	80	
[redacted]	6	111	69	
[redacted]	6	112	68	
[redacted]	7	115	69	
[redacted]	0	0	0	
[redacted]	27	104	92	
[redacted]	5	112	69	
[redacted]	0	0	0	
[redacted]	5	112	68	
[redacted]	17	47	27	
[redacted]	0	0	0	
[redacted]	6	112	70	
[redacted]	0	0	0	
[redacted]	5	116	73	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	6	116	74	
[redacted]	18	104	78	
[redacted]	6	113	70	
[redacted]	0	0	0	
[redacted]	32	219	65	
[redacted]	6	112	68	
[redacted]	6	112	69	
[redacted]	0	0	0	
[redacted]	5	112	68	
[redacted]	5	112	68	
[redacted]	0	0	0	
[redacted]	5	112	70	
[redacted]	29	136	82	
[redacted]	20	97	72	
[redacted]	7	113	70	
[redacted]	6	112	69	
[redacted]	0	0	0	
[redacted]	30	51	40	
[redacted]	5	113	70	
[redacted]	0	0	0	

[redacted]	6	112	68	
[redacted]	12	117	71	
[redacted]	20	105	92	
[redacted]	19	101	93	
[redacted]	8	115	71	
[redacted]	6	113	72	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	0	0	0	
[redacted]	6	114	69	
[redacted]	5	112	70	
[redacted]	5	113	69	
[redacted]	0	0	0	
[redacted]	6	112	70	
[redacted]	39	127	77	
[redacted]	5	112	68	
[redacted]	6	116	70	
[redacted]	6	112	69	
[redacted]	8	116	72	
[redacted]	33	51	33	
[redacted]	0	0	0	
[redacted]	7	115	69	
[redacted]	5	112	68	
[redacted]	23	99	93	
[redacted]	5	112	71	
[redacted]	0	0	0	
[redacted]	5	113	70	
[redacted]	6	112	69	
[redacted]	19	104	93	
[redacted]	20	104	98	
[redacted]	0	0	0	
[redacted]	7	114	70	
[redacted]	0	0	0	
[redacted]	23	98	84	
[redacted]	27	110	104	
[redacted]	19	105	90	
[redacted]	0	0	0	
[redacted]	19	102	93	
[redacted]	7	113	72	
[redacted]	6	113	81	

Top 25 Findings by Count

The following table contains the top 25 findings ordered by Count.

Finding ID	Risk	Count	Percentage of All Findings
16	Critical	1734	6.5
19	Critical	1462	5.48
23	Critical	1428	5.36
18	Critical	1258	4.72
25	Critical	1122	4.21
17	Critical	1020	3.83
7	Critical	938	3.52
20	Critical	816	3.06
15	Critical	782	2.93
14	Critical	714	2.68
27	Critical	680	2.55
3	Critical	444	1.67
148	Critical	348	1.31
26	Critical	312	1.17
86	Critical	270	1.01
154	Critical	260	0.98
156	Critical	255	0.96
33	Critical	245	0.92
35	Critical	240	0.9
37	Critical	225	0.84
152	Critical	212	0.8
150	Critical	196	0.74
147	Critical	195	0.73
303	Critical	186	0.7
155	Critical	180	0.68

Summary of Significant Findings (By Server)

IP	Finding ID	Severity	Description
[redacted]	2	Critical	Microsoft Internet Explorer Unsupported Version Detection
	3	Critical	Security Updates for Microsoft Office Products (November 2019)
	4	Critical	Security Updates for Microsoft Office Products (August 2022)
	5	Critical	Security Updates for Microsoft Word Products (February 2023)
	6	Critical	Security Updates for Outlook (March 2023)
	236	Critical	BitDefender Endpoint Security Tools Status (Windows)
[redacted]	8	Critical	Mozilla Foundation Unsupported Application Detection
	9	Critical	Adobe Flash Player Unsupported Version Detection
	10	Critical	Unsupported Windows OS (remote)
	11	Critical	Microsoft Windows 7 / Server 2008 R2 Unsupported Version Detection
	12	Critical	Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability (ADV200006)
	14	Critical	KB4586805: Windows 7 and Windows Server 2008 R2 November 2020 Security Update
	15	Critical	KB5000851: Windows 7 and Windows Server 2008 R2 March 2021 Security Update
	16	Critical	KB5012649: Windows 7 and Windows Server 2008 R2 Security Update (April 2022)
	17	Critical	KB5016679: Windows 7 and Windows Server 2008 R2 Security Update (August 2022)
	18	Critical	KB5017373: Windows Server 2008 R2 Security Update (September 2022)
	19	Critical	KB5018479: Windows Server 2008 R2 Security Update (October 2022)
	20	Critical	KB5020013: Windows Server 2008 R2 Security Update (November 2022)
	21	Critical	Security Updates for Microsoft .NET Framework (December 2022)
	23	Critical	KB5022339: Windows Server 2008 R2 Security Update (January 2023)
	25	Critical	KB5022874: Windows Server 2008 R2 Security Update (February 2023)
	27	Critical	KB5023759: Windows Server 2008 R2 Security Update (March 2023)
	242	Critical	Microsoft Office Unsupported Version Detection
	247	Critical	Microsoft Access Unsupported Version Detection
	293	Critical	Adobe Reader Unsupported Version Detection

	295	Critical	Adobe Reader 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-15)
	297	Critical	Adobe Reader = 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-24)
	299	Critical	Adobe Reader 11.0.14 / 15.006.30119 / 15.010.20056 Multiple Vulnerabilities (APSB16-02)
	300	Critical	Oracle Java SE Multiple Vulnerabilities (January 2016 CPU) (SLOTH)
	301	Critical	Adobe Reader 11.0.15 / 15.006.30121 / 15.010.20060 Multiple Vulnerabilities (APSB16-09)
	302	Critical	Oracle Java SE Multiple Vulnerabilities (April 2016 CPU)
	303	Critical	Adobe Reader 11.0.16 / 15.006.30172 / 15.016.20039 Multiple Vulnerabilities (APSB16-14)
	304	Critical	Adobe Reader 11.0.17 / 15.006.30198 / 15.017.20050 Multiple Vulnerabilities (APSB16-26)
	305	Critical	Adobe Reader 11.0.18 / 15.006.30243 / 15.020.20039 Multiple Vulnerabilities (APSB16-33)
	306	Critical	Adobe Reader 11.0.19 / 15.006.30279 / 15.023.20053 Multiple Vulnerabilities (APSB17-01)
	307	Critical	Adobe Reader 11.0.20 / 2015.006.30306 / 2017.009.20044 Multiple Vulnerabilities (APSB17-11)
	308	Critical	Adobe Reader 11.0.21 / 2015.006.30355 / 2017.011.30066 / 2017.012.20098 Multiple Vulnerabilities (APSB17-24)
	309	Critical	Adobe Reader 11.0.23 / 2015.006.30392 / 2017.011.30068 / 2018.009.20044 Multiple Vulnerabilities (APSB17-36)
[redacted]	2	Critical	Microsoft Internet Explorer Unsupported Version Detection
	2	Critical	Microsoft Internet Explorer Unsupported Version Detection
	1	Critical	VMware ESX / ESXi Unsupported Version Detection
	1	Critical	VMware ESX / ESXi Unsupported Version Detection
	1	Critical	VMware ESX / ESXi Unsupported Version Detection
	1	Critical	VMware ESX / ESXi Unsupported Version Detection
	1	Critical	VMware ESX / ESXi Unsupported Version Detection
[redacted]	2	Critical	Microsoft Internet Explorer Unsupported Version Detection
	3	Critical	Security Updates for Microsoft Office Products (November 2019)
	4	Critical	Security Updates for Microsoft Office Products (August 2022)
	5	Critical	Security Updates for Microsoft Word Products (February 2023)
	6	Critical	Security Updates for Outlook (March 2023)
	7	Critical	Google Chrome 112.0.5615.49 Multiple Vulnerabilities
[redacted]	3	Critical	Security Updates for Microsoft Office Products (November 2019)
	4	Critical	Security Updates for Microsoft Office Products (August 2022)

	5	Critical	Security Updates for Microsoft Word Products (February 2023)
	6	Critical	Security Updates for Outlook (March 2023)
	7	Critical	Google Chrome 112.0.5615.49 Multiple Vulnerabilities
	8	Critical	Mozilla Foundation Unsupported Application Detection
	9	Critical	Adobe Flash Player Unsupported Version Detection
	10	Critical	Unsupported Windows OS (remote)
	11	Critical	Microsoft Windows 7 / Server 2008 R2 Unsupported Version Detection
	12	Critical	Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability (ADV200006)
	13	Critical	Zoom Client for Meetings 4.6.19253.0401 Multiple Vulnerabilities
	14	Critical	KB4586805: Windows 7 and Windows Server 2008 R2 November 2020 Security Update
	15	Critical	KB5000851: Windows 7 and Windows Server 2008 R2 March 2021 Security Update
	16	Critical	KB5012649: Windows 7 and Windows Server 2008 R2 Security Update (April 2022)
	17	Critical	KB5016679: Windows 7 and Windows Server 2008 R2 Security Update (August 2022)
	18	Critical	KB5017373: Windows Server 2008 R2 Security Update (September 2022)
	19	Critical	KB5018479: Windows Server 2008 R2 Security Update (October 2022)
	20	Critical	KB5020013: Windows Server 2008 R2 Security Update (November 2022)
	21	Critical	Security Updates for Microsoft .NET Framework (December 2022)
	22	Critical	Zoom Client for Meetings 5.3.0 Vulnerability (ZSB-21003)
	23	Critical	KB5022339: Windows Server 2008 R2 Security Update (January 2023)
	24	Critical	Google Chrome 110.0.5481.77 Multiple Vulnerabilities
	25	Critical	KB5022874: Windows Server 2008 R2 Security Update (February 2023)
	26	Critical	Google Chrome 111.0.5563.64 Multiple Vulnerabilities
	27	Critical	KB5023759: Windows Server 2008 R2 Security Update (March 2023)
	28	Critical	Google Chrome 111.0.5563.110 Multiple Vulnerabilities
[redacted]	2	Critical	Microsoft Internet Explorer Unsupported Version Detection
	3	Critical	Security Updates for Microsoft Office Products (November 2019)
	4	Critical	Security Updates for Microsoft Office Products (August 2022)
	5	Critical	Security Updates for Microsoft Word Products (February 2023)

	6	Critical	Security Updates for Outlook (March 2023)
[redacted]	2	Critical	Microsoft Internet Explorer Unsupported Version Detection
	3	Critical	Security Updates for Microsoft Office Products (November 2019)
	4	Critical	Security Updates for Microsoft Office Products (August 2022)
	5	Critical	Security Updates for Microsoft Word Products (February 2023)
	6	Critical	Security Updates for Outlook (March 2023)
	29	Critical	Adobe Acrobat Unsupported Version Detection
[redacted]	2	Critical	Microsoft Internet Explorer Unsupported Version Detection
	3	Critical	Security Updates for Microsoft Office Products (November 2019)
	4	Critical	Security Updates for Microsoft Office Products (August 2022)
	5	Critical	Security Updates for Microsoft Word Products (February 2023)
	6	Critical	Security Updates for Outlook (March 2023)
	7	Critical	Google Chrome 112.0.5615.49 Multiple Vulnerabilities
[redacted]	2	Critical	Microsoft Internet Explorer Unsupported Version Detection
[redacted]	1	Critical	VMware ESX / ESXi Unsupported Version Detection
[redacted]	7	Critical	Google Chrome 112.0.5615.49 Multiple Vulnerabilities
	21	Critical	Security Updates for Microsoft .NET Framework (December 2022)
	24	Critical	Google Chrome 110.0.5481.77 Multiple Vulnerabilities
	26	Critical	Google Chrome 111.0.5563.64 Multiple Vulnerabilities
	28	Critical	Google Chrome 111.0.5563.110 Multiple Vulnerabilities
	31	Critical	Microsoft SQL Server Unsupported Version Detection
	32	Critical	Microsoft SQL Server Unsupported Version Detection (remote check)
	33	Critical	KB5018476: Windows Server 2012 R2 Security Update (October 2022)
	34	Critical	KB5020010: Windows Server 2012 R2 Security Update (November 2022)
	35	Critical	KB5022346: Windows Server 2012 R2 Security Update (January 2023)
	36	Critical	KB5022894: Windows Server 2012 R2 Security Update (February 2023)
	37	Critical	KB5023764: Windows Server 2012 R2 Security Update (March 2023)
[redacted]	9	Critical	Adobe Flash Player Unsupported Version Detection
	31	Critical	Microsoft SQL Server Unsupported Version Detection
	38	Critical	Flash Player = 10.3.183.14 / 11.1.102.55 Multiple Vulnerabilities (APSB12-03)
	39	Critical	Flash Player = 10.3.183.22 / 11.4.402.264 Multiple Vulnerabilities (APSB12-19)

	16	Critical	KB5012649: Windows 7 and Windows Server 2008 R2 Security Update (April 2022)
	17	Critical	KB5016679: Windows 7 and Windows Server 2008 R2 Security Update (August 2022)
	18	Critical	KB5017373: Windows Server 2008 R2 Security Update (September 2022)
	19	Critical	KB5018479: Windows Server 2008 R2 Security Update (October 2022)
	20	Critical	KB5020013: Windows Server 2008 R2 Security Update (November 2022)
	21	Critical	Security Updates for Microsoft .NET Framework (December 2022)
	23	Critical	KB5022339: Windows Server 2008 R2 Security Update (January 2023)
	25	Critical	KB5022874: Windows Server 2008 R2 Security Update (February 2023)
	27	Critical	KB5023759: Windows Server 2008 R2 Security Update (March 2023)
	165	Critical	Microsoft XML Parser (MSXML) and XML Core Services Unsupported
	213	Critical	Mozilla Firefox 96.0
	214	Critical	Mozilla Firefox 97.0
	215	Critical	Mozilla Firefox 97.0.2
	216	Critical	Mozilla Firefox 98.0
	217	Critical	Mozilla Firefox 100.0
	218	Critical	Mozilla Firefox 100.0.2
	219	Critical	Mozilla Firefox 101.0
	220	Critical	Mozilla Firefox 102.0
	221	Critical	Mozilla Firefox 103.0
	222	Critical	Mozilla Firefox 104.0
	223	Critical	Mozilla Firefox 105.0
	224	Critical	Mozilla Firefox 106.0
	225	Critical	Mozilla Firefox 107.0
	226	Critical	Mozilla Firefox 108.0
	356	Critical	Apple QuickTime Unsupported on Windows

Summary of Vulnerabilities (By Vulnerability)

Finding ID	Severity	Description	Affected Server
1	Critical	VMware ESX / ESXi Unsupported Version Detection	[redacted]
2	Critical	Microsoft Internet Explorer Unsupported Version Detection	[redacted]

			[redacted]

			[redacted]

[redacted]

			[redacted]

			[redacted]
3	Critical	Security Updates for Microsoft Office Products (November 2019)	[redacted]

29	Critical	Adobe Acrobat Unsupported Version Detection	[redacted]
30	Critical	MS16-120: Security Update for Microsoft Graphics Component (3192884)	[redacted]
31	Critical	Microsoft SQL Server Unsupported Version Detection	[redacted]
32	Critical	Microsoft SQL Server Unsupported Version Detection (remote check)	[redacted]
33	Critical	KB5018476: Windows Server 2012 R2 Security Update (October 2022)	[redacted]
34	Critical	KB5020010: Windows Server 2012 R2 Security Update (November 2022)	[redacted]
35	Critical	KB5022346: Windows Server 2012 R2 Security Update (January 2023)	[redacted]

			[redacted]
36	Critical	KB5022894: Windows Server 2012 R2 Security Update (February 2023)	[redacted]
37	Critical	KB5023764: Windows Server 2012 R2 Security Update (March 2023)	[redacted]
38	Critical	Flash Player = 10.3.183.14 / 11.1.102.55 Multiple Vulnerabilities (APSB12-03)	[redacted]
39	Critical	Flash Player = 10.3.183.22 / 11.4.402.264 Multiple Vulnerabilities (APSB12-19)	[redacted]
40	Critical	Flash Player = 10.3.183.23 / 11.4.402.278 Multiple Vulnerabilities (APSB12-22)	[redacted]
41	Critical	Flash Player = 10.3.183.29 / 11.4.402.287 Multiple Vulnerabilities (APSB12-24)	[redacted]
42	Critical		[redacted]

321	Critical	KB4467703: Windows 8.1 and Windows Server 2012 R2 November 2018 Security Update	[redacted]
322	Critical	KB4471322: Windows 8.1 and Windows Server 2012 R2 December 2018 Security Update	[redacted]
323	Critical	KB4512489: Windows 8.1 and Windows Server 2012 R2 August 2019 Security Update	[redacted]
324	Critical	KB4534309: Windows 8.1 and Windows Server 2012 R2 January 2020 Security Update	[redacted]
325	Critical	KB4586823: Windows 8.1 and Windows Server 2012 R2 November 2020 Security Update	[redacted]
326	Critical	KB5000853: Windows 8.1 and Windows Server 2012 R2 March 2021 Security Update	[redacted]
327	Critical	KB5012670: Windows Server 2012 R2 Security Update (April 2022)	[redacted]
328	Critical	KB5014746: Windows Server 2012 R2 Security Update (June 2022)	[redacted]
329	Critical	KB4457145: Windows 7 and Windows Server 2008 R2 September 2018 Security Update	[redacted]
330	Critical	KB4467106: Windows 7 and Windows Server 2008 R2 November 2018 Security Update	[redacted]
331	Critical	KB4471328: Windows 7 and Windows Server 2008 R2 December 2018 Security Update	[redacted]
332	Critical	KB4499175: Windows 7 and Windows Server 2008 R2 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout) (BlueKeep)	[redacted]
333	Critical	KB4512486: Windows 7 and Windows Server 2008 R2 August 2019 Security Update	[redacted]
334	Critical	KB4534314: Windows 7 and Windows Server 2008 R2 January 2020 Security Update	[redacted]
335	Critical	Microsoft Office 365 Unsupported Channel Version Detection	[redacted]

336	Critical	Microsoft Edge (Chromium) 99.0.1150.46 Multiple Vulnerabilities	[redacted]
337	Critical	Microsoft Edge (Chromium) 100.0.1185.44 Multiple Vulnerabilities	[redacted]
338	Critical	Microsoft Edge (Chromium) 101.0.1210.32 Multiple Vulnerabilities	[redacted]
339	Critical	Microsoft Edge (Chromium) 101.0.1210.47 Multiple Vulnerabilities	[redacted]
340	Critical	Microsoft Edge (Chromium) 102.0.1245.41 Multiple Vulnerabilities	[redacted]
341	Critical	Microsoft Edge (Chromium) 103.0.1264.71 Multiple Vulnerabilities	[redacted]
342	Critical	Microsoft Edge (Chromium) 104.0.1293.47 Multiple Vulnerabilities	[redacted]
343	Critical	Microsoft Edge (Chromium) 104.0.1293.63 Multiple Vulnerabilities	[redacted]
344	Critical	Microsoft Edge (Chromium) 105.0.1343.42 Multiple Vulnerabilities	[redacted]
345	Critical	Microsoft Edge (Chromium) 106.0.1370.34 Multiple Vulnerabilities	[redacted]
346	Critical	Microsoft Edge (Chromium) 106.0.1370.47 Multiple Vulnerabilities	[redacted]
347	Critical	Microsoft Edge (Chromium) 107.0.1418.24 Multiple Vulnerabilities	[redacted]
348	Critical	Microsoft Edge (Chromium) 107.0.1418.42 Multiple Vulnerabilities	[redacted]
349	Critical	Microsoft Edge (Chromium) 108.0.1462.54 Multiple Vulnerabilities	[redacted]
350	Critical	KB5022282: Windows 10 Version 20H2 / Windows 10 Version 21H2 / Windows 10 Version 22H2 Security Update (January 2023)	[redacted]
351	Critical	Microsoft Edge (Chromium) 109.0.1518.49 / 108.0.1462.83 Multiple Vulnerabilities	[redacted]
352	Critical	Microsoft Edge (Chromium) 109.0.1343.27 Multiple Vulnerabilities	[redacted]
353	Critical	Microsoft Edge (Chromium) 109.0.1518.70 / 108.0.1462.95 Multiple Vulnerabilities	[redacted]
354	Critical	Security Updates for Microsoft Word Products C2R (February 2023)	[redacted]
355	Critical	Security Updates for Outlook C2R Elevation of Privilege (March 2023)	[redacted]
356	Critical	Apple QuickTime Unsupported on Windows	[redacted]
357	Critical	Windows DNS Server RCE (CVE-2020-1350)	[redacted]

Vulnerability Details and Remediation

In each of the following scenarios, **the general remediation is to install the latest released version of the software or OS possible**. Alternatively, another option is to **remove applications that are no longer used** or needed. For those situations in which that is not possible or practical, we provide the specific patch information relevant to the given vulnerability.

1.	**VMware ESX / ESXi Unsupported Version Detection** The remote host is running an unsupported version of a virtualization application. (56997)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to a version of VMware ESX / ESXi that is currently supported.	10.0 (v3B)

2.	**Microsoft Internet Explorer Unsupported Version Detection** The remote host contains an unsupported version of Internet Explorer. (22024)	
Risk	Recommendation(s)	CVSS Score
C	Either Upgrade to a version of Internet Explorer that is currently supported or disable Internet Explorer on the target device.	10.0 (v3B)

3.	**Security Updates for Microsoft Office Products (November 2019)** The Microsoft Office Products are affected by multiple vulnerabilities. (130913)	
Risk	Recommendation(s)	CVSS Score
C	Microsoft has released the following security updates to address this issue: -KB4484152 -KB4484160 -KB4484148 -KB4484127 -KB4484113 -KB4484119 For Office 365, Office 2016 C2R, or Office 2019,	9.8 (v3B)

	ensure automatic updates are enabled or open any office app and manually perform an update.	
Relevant CVE's: CVE-2019-1402, CVE-2019-1446, CVE-2019-1448, CVE-2019-1449		

4.	**Security Updates for Microsoft Office Products (August 2022)** The Microsoft Office Products are affected by a remote code execution vulnerability. (163950)	
Risk	Recommendation(s)	CVSS Score
C	Microsoft has released the following security updates to address this issue: -KB4462148 -KB4462142 For Office 365, Office 2016 C2R, or Office 2019, ensure automatic updates are enabled or open any office app and manually perform an update.	8.8 (v3B)
Relevant CVE's: CVE-2022-34717		

5.	**Security Updates for Microsoft Word Products (February 2023)** The Microsoft Word Products are missing a security update. (171449)	
Risk	Recommendation(s)	CVSS Score
C	Microsoft has released the following security updates to address this issue: -KB5002316 -KB5002323 For Office 365, Office 2016 C2R, or Office 2019, ensure automatic updates are enabled or open any office app and manually perform an update.	9.8 (v3B)
Relevant CVE's: CVE-2023-21716		

6.	**Security Updates for Outlook (March 2023)** The Microsoft Outlook application installed on the remote host is missing a security update. (172527)	

Risk	Recommendation(s)	CVSS Score
C	Microsoft has released the following security updates to address this issue: -KB5002265 -KB5002254 For Office 365, Office 2016 C2R, or Office 2019, ensure automatic updates are enabled or open any office app and manually perform an update.	9.8 (v3B)
Relevant CVE's: CVE-2023-23397		

7.	**Google Chrome 112.0.5615.49 Multiple Vulnerabilities** A web browser installed on the remote Windows host is affected by multiple vulnerabilities. (173836)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Google Chrome version 112.0.5615.49 or later.	9.8 (v3B)
Relevant CVE's: CVE-2023-1810, CVE-2023-1811, CVE-2023-1812, CVE-2023-1813, CVE-2023-1814, CVE-2023-1815, CVE-2023-1816, CVE-2023-1817, CVE-2023-1818, CVE-2023-1819, CVE-2023-1820, CVE-2023-1821, CVE-2023-1822, CVE-2023-1823		

8.	**Mozilla Foundation Unsupported Application Detection** The remote host contains one or more unsupported applications from the Mozilla Foundation. (40362)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to a version that is currently supported.	10.0 (v3B)

9.	**Adobe Flash Player Unsupported Version Detection** The remote host contains an unsupported version of Adobe Flash Player. (59196)	
Risk	Recommendation(s)	CVSS Score
C	Remove the unsupported software.	10.0 (v2B)

10.	**Unsupported Windows OS (remote)**	

	The remote OS or service pack is no longer supported. (108797)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to a supported service pack or operating system	10.0 (v3B)

11.	**Microsoft Windows 7 / Server 2008 R2 Unsupported Version Detection** The remote operating system is no longer supported. (122615)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to a version of Microsoft Windows that is currently supported.	10.0 (v3B)

12.	**Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability (ADV200006)** The remote Windows host is affected by a font parsing vulnerability. (134942)	
Risk	Recommendation(s)	CVSS Score
C	Microsoft has provided additional details and guidance in the ADV200006 advisory.	9.8 (v3B)

13.	**Zoom Client for Meetings 4.6.19253.0401 Multiple Vulnerabilities** The remote host has an application installed that is affected by multiple vulnerabilities. (135188)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Zoom Client for Meetings 4.6.19253.0401 or later.	9.6 (v3B)

14.	**KB4586805: Windows 7 and Windows Server 2008 R2 November 2020 Security Update** The remote Windows host is affected by multiple vulnerabilities. (142683)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Only update KB4586805 or Cumulative Update KB4586827.	9.8 (v3B)

Relevant CVE's: CVE-2020-1599, CVE-2020-16997, CVE-2020-17000, CVE-2020-17001, CVE-2020-17004, CVE-2020-17011, CVE-2020-17014, CVE-2020-17029, CVE-2020-17036, CVE-2020-17038, CVE-2020-17042, CVE-2020-17043, CVE-2020-17044, CVE-2020-17045, CVE-2020-17047, CVE-2020-17051, CVE-2020-17052, CVE-2020-17068, CVE-2020-17069, CVE-2020-17087, CVE-2020-17088

15.	**KB5000851: Windows 7 and Windows Server 2008 R2 March 2021 Security Update** The remote Windows host is affected by multiple vulnerabilities. (147231)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Only update KB5000851 or Cumulative Update KB5000841.	9.8 (v3B)
Relevant CVE's: CVE-2021-1640, CVE-2021-24107, CVE-2021-26411, CVE-2021-26861, CVE-2021-26862, CVE-2021-26869, CVE-2021-26872, CVE-2021-26873, CVE-2021-26875, CVE-2021-26877, CVE-2021-26878, CVE-2021-26881, CVE-2021-26882, CVE-2021-26893, CVE-2021-26894, CVE-2021-26895, CVE-2021-26896, CVE-2021-26897, CVE-2021-26898, CVE-2021-26899, CVE-2021-26901, CVE-2021-27063, CVE-2021-27077		

16.	**KB5012649: Windows 7 and Windows Server 2008 R2 Security Update (April 2022)** The remote Windows host is affected by multiple vulnerabilities. (159672)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Only update KB5012649 or Cumulative Update KB5012626.	9.8 (v3B)
Relevant CVE's: CVE-2022-21983, CVE-2022-24474, CVE-2022-24481, CVE-2022-24485, CVE-2022-24492, CVE-2022-24493, CVE-2022-24494, CVE-2022-24498, CVE-2022-24499, CVE-2022-24500, CVE-2022-24521, CVE-2022-24527, CVE-2022-24528, CVE-2022-24530, CVE-2022-24533, CVE-2022-24534, CVE-2022-24536, CVE-2022-24540, CVE-2022-24541, CVE-2022-24542, CVE-2022-24544, CVE-2022-26787, CVE-2022-26790, CVE-2022-26792, CVE-2022-26794, CVE-2022-26796, CVE-2022-26797, CVE-2022-26798, CVE-2022-26801, CVE-2022-26802, CVE-2022-26803, CVE-2022-26807, CVE-2022-26809, CVE-2022-26810, CVE-2022-26812, CVE-2022-26813, CVE-2022-26815, CVE-2022-26819, CVE-2022-26820, CVE-2022-26821, CVE-2022-26822, CVE-2022-26827, CVE-2022-26829, CVE-2022-26831, CVE-2022-26903, CVE-2022-26904, CVE-2022-26915, CVE-2022-26916, CVE-2022-26917, CVE-2022-26918, CVE-2022-26919		

17.	**KB5016679: Windows 7 and Windows Server 2008 R2 Security Update (August 2022)** The remote Windows host is affected by multiple vulnerabilities. (163952)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Update 5016679 or Cumulative Update 5016676	9.8 (v3B)

Relevant CVE's: CVE-2022-30133, CVE-2022-30194, CVE-2022-34689, CVE-2022-34690, CVE-2022-34691, CVE-2022-34701, CVE-2022-34702, CVE-2022-34706, CVE-2022-34707, CVE-2022-34708, CVE-2022-34713, CVE-2022-34714, CVE-2022-35743, CVE-2022-35744, CVE-2022-35745, CVE-2022-35747, CVE-2022-35750, CVE-2022-35751, CVE-2022-35752, CVE-2022-35753, CVE-2022-35756, CVE-2022-35758, CVE-2022-35759, CVE-2022-35760, CVE-2022-35767, CVE-2022-35768, CVE-2022-35769, CVE-2022-35793, CVE-2022-35795, CVE-2022-35820

18.	**KB5017373: Windows Server 2008 R2 Security Update (September 2022)** The remote Windows host is affected by multiple vulnerabilities. (165002)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Update 5017373 or Cumulative Update 5017361	9.8 (v3B)
Relevant CVE's: CVE-2022-26929, CVE-2022-30170, CVE-2022-30200, CVE-2022-33647, CVE-2022-33679, CVE-2022-34718, CVE-2022-34719, CVE-2022-34720, CVE-2022-34721, CVE-2022-34722, CVE-2022-34724, CVE-2022-34726, CVE-2022-34727, CVE-2022-34728, CVE-2022-34729, CVE-2022-34730, CVE-2022-34731, CVE-2022-34732, CVE-2022-34733, CVE-2022-34734, CVE-2022-35803, CVE-2022-35830, CVE-2022-35832, CVE-2022-35833, CVE-2022-35834, CVE-2022-35835, CVE-2022-35836, CVE-2022-35837, CVE-2022-35840, CVE-2022-37955, CVE-2022-37956, CVE-2022-37958, CVE-2022-37964, CVE-2022-37969, CVE-2022-38004, CVE-2022-38005, CVE-2022-38006		

19.	**KB5018479: Windows Server 2008 R2 Security Update (October 2022)** The remote Windows host is affected by multiple vulnerabilities. (166024)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Update 5018479 or Cumulative Update 5018454	8.8 (v3B)
Relevant CVE's: CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-33635, CVE-2022-33645, CVE-2022-35770, CVE-2022-37975, CVE-2022-37976, CVE-2022-37977, CVE-2022-37978, CVE-2022-37981, CVE-2022-37982, CVE-2022-37985, CVE-2022-37986, CVE-2022-37987, CVE-2022-37988, CVE-2022-37989, CVE-2022-37990, CVE-2022-37991, CVE-2022-37993, CVE-2022-37994, CVE-2022-37997, CVE-2022-37999, CVE-2022-38000, CVE-2022-38022, CVE-2022-38026, CVE-2022-38029, CVE-2022-38031, CVE-2022-38032, CVE-2022-38033, CVE-2022-38034, CVE-2022-38037, CVE-2022-38038, CVE-2022-38040, CVE-2022-38041, CVE-2022-38042, CVE-2022-38043, CVE-2022-38044, CVE-2022-38047, CVE-2022-38051, CVE-2022-41033, CVE-2022-41081		

20.	**KB5020013: Windows Server 2008 R2 Security Update (November 2022)** The remote Windows host is affected by multiple vulnerabilities. (167103)	
Risk	Recommendation(s)	CVSS Score

C	Apply Security Update 5020013 or Cumulative Update 5020000	8.8 (v3B)
Relevant CVE's: CVE-2022-23824, CVE-2022-37966, CVE-2022-37967, CVE-2022-37992, CVE-2022-38023, CVE-2022-41039, CVE-2022-41044, CVE-2022-41045, CVE-2022-41047, CVE-2022-41048, CVE-2022-41053, CVE-2022-41056, CVE-2022-41057, CVE-2022-41058, CVE-2022-41073, CVE-2022-41086, CVE-2022-41090, CVE-2022-41095, CVE-2022-41097, CVE-2022-41098, CVE-2022-41109, CVE-2022-41116, CVE-2022-41118, CVE-2022-41128		

21.	**Security Updates for Microsoft .NET Framework (December 2022)** The Microsoft .NET Framework installation on the remote host is missing a security update. (168745)	
Risk	Recommendation(s)	CVSS Score
C	Microsoft has released security updates for Microsoft .NET Framework.	8.8 (v3B)
Relevant CVE's: CVE-2022-41089		

22.	**Zoom Client for Meetings 5.3.0 Vulnerability (ZSB-21003)** The remote host has an application installed that is affected by a vulnerability. (168821)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Zoom Client for Meetings 5.3.0 or later.	9.8 (v3B)
Relevant CVE's: CVE-2021-33907		

23.	**KB5022339: Windows Server 2008 R2 Security Update (January 2023)** The remote Windows host is affected by multiple vulnerabilities. (169781)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Update 5022339 or Cumulative Update 5022338	9.1 (v3B)
Relevant CVE's: CVE-2023-21524, CVE-2023-21525, CVE-2023-21527, CVE-2023-21532, CVE-2023-21537, CVE-2023-21541, CVE-2023-21542, CVE-2023-21543, CVE-2023-21546, CVE-2023-21548, CVE-2023-21549, CVE-2023-21552, CVE-2023-21555, CVE-2023-21556, CVE-2023-21557, CVE-2023-21560, CVE-2023-21561, CVE-2023-21563, CVE-2023-21675, CVE-2023-21678, CVE-2023-21679, CVE-2023-21680, CVE-2023-21681, CVE-2023-21682, CVE-2023-21726, CVE-2023-21728, CVE-2023-21730, CVE-2023-21732, CVE-2023-21746, CVE-2023-21747, CVE-2023-21748, CVE-2023-21749, CVE-2023-21750, CVE-2023-21752, CVE-2023-21754, CVE-2023-21757, CVE-2023-21760, CVE-2023-21765, CVE-2023-21772, CVE-2023-21773, CVE-2023-21774, CVE-2023-21776		

24.	**Google Chrome 110.0.5481.77 Multiple Vulnerabilities** A web browser installed on the remote Windows host is affected by multiple vulnerabilities. (171321)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Google Chrome version 110.0.5481.77 or later.	8.8 (v3B)
Relevant CVE's: CVE-2023-0696, CVE-2023-0697, CVE-2023-0698, CVE-2023-0699, CVE-2023-0700, CVE-2023-0701, CVE-2023-0702, CVE-2023-0703, CVE-2023-0704, CVE-2023-0705		

25.	**KB5022874: Windows Server 2008 R2 Security Update (February 2023)** The remote Windows host is affected by multiple vulnerabilities. (171440)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Update 5022874 or Cumulative Update 5022872	9.8 (v3B)
Relevant CVE's: CVE-2023-21684, CVE-2023-21685, CVE-2023-21686, CVE-2023-21688, CVE-2023-21689, CVE-2023-21690, CVE-2023-21691, CVE-2023-21692, CVE-2023-21693, CVE-2023-21694, CVE-2023-21695, CVE-2023-21697, CVE-2023-21699, CVE-2023-21700, CVE-2023-21701, CVE-2023-21702, CVE-2023-21797, CVE-2023-21798, CVE-2023-21799, CVE-2023-21800, CVE-2023-21801, CVE-2023-21802, CVE-2023-21805, CVE-2023-21811, CVE-2023-21812, CVE-2023-21813, CVE-2023-21816, CVE-2023-21817, CVE-2023-21818, CVE-2023-21820, CVE-2023-21822, CVE-2023-21823, CVE-2023-23376		

26.	**Google Chrome 111.0.5563.64 Multiple Vulnerabilities** A web browser installed on the remote Windows host is affected by multiple vulnerabilities. (172221)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Google Chrome version 111.0.5563.64 or later.	8.8 (v3B)
Relevant CVE's: CVE-2023-1213, CVE-2023-1214, CVE-2023-1215, CVE-2023-1216, CVE-2023-1217, CVE-2023-1218, CVE-2023-1219, CVE-2023-1220, CVE-2023-1221, CVE-2023-1222, CVE-2023-1223, CVE-2023-1224, CVE-2023-1225, CVE-2023-1226, CVE-2023-1227, CVE-2023-1228, CVE-2023-1229, CVE-2023-1230, CVE-2023-1231, CVE-2023-1232, CVE-2023-1233, CVE-2023-1234, CVE-2023-1235, CVE-2023-1236		

27.	**KB5023759: Windows Server 2008 R2 Security Update (March 2023)** The remote Windows host is affected by multiple vulnerabilities. (172517)	

Risk	Recommendation(s)	CVSS Score
C	Apply Security Update 5023759 or Cumulative Update 5023769	9.8 (v3B)
Relevant CVE's: CVE-2023-21708, CVE-2023-23385, CVE-2023-23394, CVE-2023-23401, CVE-2023-23402, CVE-2023-23405, CVE-2023-23407, CVE-2023-23409, CVE-2023-23410, CVE-2023-23414, CVE-2023-23415, CVE-2023-23420, CVE-2023-23421, CVE-2023-23422, CVE-2023-23423, CVE-2023-24861, CVE-2023-24862, CVE-2023-24869, CVE-2023-24908, CVE-2023-24910		

28.	**Google Chrome 111.0.5563.110 Multiple Vulnerabilities** A web browser installed on the remote Windows host is affected by multiple vulnerabilities. (173059)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Google Chrome version 111.0.5563.110 or later.	9.8 (v3B)
Relevant CVE's: CVE-2023-1528, CVE-2023-1529, CVE-2023-1530, CVE-2023-1531, CVE-2023-1532, CVE-2023-1533, CVE-2023-1534		

29.	**Adobe Acrobat Unsupported Version Detection** The remote host contains an unsupported version of Adobe Acrobat. (56212)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to a version of Adobe Acrobat that is currently supported.	9.8 (v3B)

30.	**MS16-120: Security Update for Microsoft Graphics Component (3192884)** The remote host is affected by multiple vulnerabilities. (94017)	
Risk	Recommendation(s)	CVSS Score
C	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. Additionally, Microsoft has released a set of patches for Office 2007, Office 2010, Word Viewer, Skype for Business 2016, Lync 2010, Lync 2013, Live Meeting 2007 Console, .NET Framework 3.0 SP2, .NET Framework 3.5, .NET	9.8 (v3B)

	Framework 3.5.1, .NET Framework 4.5.2, .NET Framework 4.6, and Silverlight 5.	
Relevant CVE's: CVE-2016-3209, CVE-2016-3262, CVE-2016-3263, CVE-2016-3270, CVE-2016-3393, CVE-2016-3396, CVE-2016-7182		

31.	**Microsoft SQL Server Unsupported Version Detection** An unsupported version of a database server is running on the remote host. (64784)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to a version of Microsoft SQL Server that is currently supported.	10.0 (v3B)

32.	**Microsoft SQL Server Unsupported Version Detection (remote check)** An unsupported version of a database server is running on the remote host. (73756)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to a version of Microsoft SQL Server that is currently supported.	10.0 (v3B)

33.	**KB5018476: Windows Server 2012 R2 Security Update (October 2022)** The remote Windows host is affected by multiple vulnerabilities. (166030)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Update 5018476 or Cumulative Update 5018474	8.8 (v3B)
Relevant CVE's: CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-33635, CVE-2022-33645, CVE-2022-35770, CVE-2022-37965, CVE-2022-37975, CVE-2022-37976, CVE-2022-37977, CVE-2022-37978, CVE-2022-37981, CVE-2022-37982, CVE-2022-37984, CVE-2022-37985, CVE-2022-37986, CVE-2022-37987, CVE-2022-37988, CVE-2022-37989, CVE-2022-37990, CVE-2022-37991, CVE-2022-37993, CVE-2022-37994, CVE-2022-37996, CVE-2022-37997, CVE-2022-37999, CVE-2022-38000, CVE-2022-38022, CVE-2022-38026, CVE-2022-38027, CVE-2022-38028, CVE-2022-38029, CVE-2022-38031, CVE-2022-38032, CVE-2022-38033, CVE-2022-38034, CVE-2022-38037, CVE-2022-		

38038, CVE-2022-38040, CVE-2022-38041, CVE-2022-38042, CVE-2022-38043, CVE-2022-38044, CVE-2022-38045, CVE-2022-38047, CVE-2022-38051, CVE-2022-41033, CVE-2022-41081

34.	**KB5020010: Windows Server 2012 R2 Security Update (November 2022)** The remote Windows host is affected by multiple vulnerabilities. (167109)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Update 5020010 or Cumulative Update 5020023	8.8 (v3B)
Relevant CVE's: CVE-2022-23824, CVE-2022-37966, CVE-2022-37967, CVE-2022-37992, CVE-2022-38023, CVE-2022-41039, CVE-2022-41045, CVE-2022-41047, CVE-2022-41048, CVE-2022-41053, CVE-2022-41056, CVE-2022-41057, CVE-2022-41058, CVE-2022-41073, CVE-2022-41086, CVE-2022-41088, CVE-2022-41090, CVE-2022-41093, CVE-2022-41095, CVE-2022-41097, CVE-2022-41098, CVE-2022-41100, CVE-2022-41109, CVE-2022-41118, CVE-2022-41125, CVE-2022-41128		

35.	**KB5022346: Windows Server 2012 R2 Security Update (January 2023)** The remote Windows host is affected by multiple vulnerabilities. (169789)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Update 5022346 or Cumulative Update 5022352	9.1 (v3B)
Relevant CVE's: CVE-2023-21524, CVE-2023-21525, CVE-2023-21527, CVE-2023-21532, CVE-2023-21535, CVE-2023-21537, CVE-2023-21541, CVE-2023-21542, CVE-2023-21543, CVE-2023-21546, CVE-2023-21548, CVE-2023-21549, CVE-2023-21552, CVE-2023-21555, CVE-2023-21556, CVE-2023-21557, CVE-2023-21558, CVE-2023-21560, CVE-2023-21561, CVE-2023-21563, CVE-2023-21674, CVE-2023-21675, CVE-2023-21677, CVE-2023-21678, CVE-2023-21679, CVE-2023-21680, CVE-2023-21681, CVE-2023-21682, CVE-2023-21683, CVE-2023-21726, CVE-2023-21728, CVE-2023-21730, CVE-2023-21732, CVE-2023-21739, CVE-2023-21746, CVE-2023-21747, CVE-2023-21748, CVE-2023-21749, CVE-2023-21750, CVE-2023-21754, CVE-2023-21757, CVE-2023-21760, CVE-2023-21765, CVE-2023-21767, CVE-2023-21772, CVE-2023-21773, CVE-2023-21774, CVE-2023-21776		

36.	**KB5022894: Windows Server 2012 R2 Security Update (February 2023)** The remote Windows host is affected by multiple vulnerabilities. (171453)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Update 5022894 or Cumulative Update 5022899	9.8 (v3B)
Relevant CVE's: CVE-2023-21684, CVE-2023-21685, CVE-2023-21686, CVE-2023-21688, CVE-2023-21689, CVE-2023-21690, CVE-2023-21691, CVE-2023-21692, CVE-2023-21693, CVE-2023-21694, CVE-2023-21695, CVE-2023-21697, CVE-2023-21699, CVE-2023-21700, CVE-2023-21701, CVE-2023-21702,		

CVE-2023-21797, CVE-2023-21798, CVE-2023-21799, CVE-2023-21801, CVE-2023-21802, CVE-2023-21804, CVE-2023-21805, CVE-2023-21811, CVE-2023-21812, CVE-2023-21813, CVE-2023-21816, CVE-2023-21817, CVE-2023-21818, CVE-2023-21820, CVE-2023-21822, CVE-2023-21823, CVE-2023-23376

37.	**KB5023764: Windows Server 2012 R2 Security Update (March 2023)** The remote Windows host is affected by multiple vulnerabilities. (172535)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Update 5023764 or Cumulative Update 5023765	9.8 (v3B)
Relevant CVE's: CVE-2023-21708, CVE-2023-23385, CVE-2023-23394, CVE-2023-23400, CVE-2023-23401, CVE-2023-23402, CVE-2023-23403, CVE-2023-23404, CVE-2023-23405, CVE-2023-23406, CVE-2023-23407, CVE-2023-23409, CVE-2023-23410, CVE-2023-23412, CVE-2023-23413, CVE-2023-23414, CVE-2023-23415, CVE-2023-23416, CVE-2023-23420, CVE-2023-23421, CVE-2023-23422, CVE-2023-23423, CVE-2023-24856, CVE-2023-24857, CVE-2023-24858, CVE-2023-24859, CVE-2023-24861, CVE-2023-24862, CVE-2023-24863, CVE-2023-24864, CVE-2023-24865, CVE-2023-24866, CVE-2023-24867, CVE-2023-24868, CVE-2023-24869, CVE-2023-24870, CVE-2023-24872, CVE-2023-24876, CVE-2023-24906, CVE-2023-24907, CVE-2023-24908, CVE-2023-24909, CVE-2023-24910, CVE-2023-24911, CVE-2023-24913		

38.	**Flash Player = 10.3.183.14 / 11.1.102.55 Multiple Vulnerabilities (APSB12-03)** The remote Windows host has a browser plugin that is affected by multiple vulnerabilities. (58001)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Adobe Flash version 10.3.183.15 / 11.1.102.62 or later.	10.0 (v2B)
Relevant CVE's: CVE-2012-0751, CVE-2012-0752, CVE-2012-0753, CVE-2012-0754, CVE-2012-0755, CVE-2012-0756, CVE-2012-0767		

39.	**Flash Player = 10.3.183.22 / 11.4.402.264 Multiple Vulnerabilities (APSB12-19)** The remote Windows host has a browser plugin that is affected by multiple vulnerabilities. (61622)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Adobe Flash Player version 10.3.183.23, 11.4.402.265 or later, or Google Chrome PepperFlash 11.3.31.230 or later.	10.0 (v2B)
Relevant CVE's: CVE-2012-4163, CVE-2012-4164, CVE-2012-4165, CVE-2012-4167, CVE-2012-4168, CVE-2012-4171, CVE-2012-5054		

40.	**Flash Player = 10.3.183.23 / 11.4.402.278 Multiple Vulnerabilities (APSB12-22)** The remote Windows host has a browser plugin that is affected by multiple vulnerabilities. (62480)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Adobe Flash Player version 10.3.183.29, 11.4.402.287 or later, or Google Chrome PepperFlash 11.4.31.110 or later.	10.0 (v2B)
Relevant CVE's: CVE-2012-5248, CVE-2012-5249, CVE-2012-5250, CVE-2012-5251, CVE-2012-5252, CVE-2012-5253, CVE-2012-5254, CVE-2012-5255, CVE-2012-5256, CVE-2012-5257, CVE-2012-5258, CVE-2012-5259, CVE-2012-5260, CVE-2012-5261, CVE-2012-5262, CVE-2012-5263, CVE-2012-5264, CVE-2012-5265, CVE-2012-5266, CVE-2012-5267, CVE-2012-5268, CVE-2012-5269, CVE-2012-5270, CVE-2012-5271, CVE-2012-5272, CVE-2012-5285, CVE-2012-5286, CVE-2012-5287, CVE-2012-5673		

41.	**Flash Player = 10.3.183.29 / 11.4.402.287 Multiple Vulnerabilities (APSB12-24)** The remote Windows host has a browser plugin that is affected by multiple vulnerabilities. (62836)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Adobe Flash Player version 10.3.183.43, 11.5.502.110 or later, or Google Chrome PepperFlash 11.5.31.2 or later.	10.0 (v2B)
Relevant CVE's: CVE-2012-5274, CVE-2012-5275, CVE-2012-5276, CVE-2012-5277, CVE-2012-5278, CVE-2012-5279, CVE-2012-5280		

42.	**Flash Player = 10.3.183.43 / 11.5.502.110 Multiple Vulnerabilities (APSB12-27)** The remote Windows host has a browser plugin that is affected by multiple vulnerabilities. (63242)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Adobe Flash Player version 10.3.183.48 / 11.5.502.135 or later, or Google Chrome PepperFlash 11.5.31.5 or later.	10.0 (v2B)
Relevant CVE's: CVE-2012-5676, CVE-2012-5677, CVE-2012-5678		

43.	**Flash Player = 10.3.183.48 / 11.5.502.135 Buffer Overflow (APSB13-01)**

	The remote Windows host has a browser plugin that is affected by buffer overflow vulnerability. (63450)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Adobe Flash Player version 10.3.183.50 / 11.5.502.146 or later, or Google Chrome PepperFlash 11.5.31.137 or later.	10.0 (v2B)
Relevant CVE's: CVE-2013-0630		

44.	**Flash Player = 10.3.183.51 / 11.5.502.149** **Multiple Vulnerabilities (APSB13-05)** The remote Windows host has a browser plugin that is affected by multiple vulnerabilities. (64584)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Adobe Flash Player version 10.3.183.63 / 11.6.602.168 or later, or Google Chrome PepperFlash 11.6.602.167 or later.	10.0 (v2B)
Relevant CVE's: CVE-2013-0637, CVE-2013-0638, CVE-2013-0639, CVE-2013-0642, CVE-2013-0644, CVE-2013-0645, CVE-2013-0647, CVE-2013-0649, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, CVE-2013-1373, CVE-2013-1374		

45.	**Flash Player = 10.3.183.63 / 11.6.602.168** **Multiple Vulnerabilities (APSB13-08)** The remote Windows host has a browser plugin that is affected by multiple vulnerabilities. (64916)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Adobe Flash Player version 10.3.183.67 / 11.6.602.171 or later, or Google Chrome PepperFlash 11.6.602.171 or later.	10.0 (v2B)
Relevant CVE's: CVE-2013-0504, CVE-2013-0643, CVE-2013-0648		

46.	**Flash Player = 10.3.183.67 / 11.6.602.171** **Multiple Vulnerabilities (APSB13-09)** The remote Windows host has a browser plugin that is affected by multiple vulnerabilities. (65219)	
Risk	Recommendation(s)	CVSS Score

C	Upgrade to Adobe Flash Player version 10.3.183.68 / 11.6.602.180 or later, or Google Chrome PepperFlash 11.6.602.180 or later.	10.0 (v2B)
Relevant CVE's: CVE-2013-0646, CVE-2013-0650, CVE-2013-1371, CVE-2013-1375		

47.	**Flash Player = 10.3.183.68 / 11.6.602.180 Multiple Vulnerabilities (APSB13-11)** The remote Windows host has a browser plugin that is affected by multiple vulnerabilities. (65910)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Adobe Flash Player version 10.3.183.75 / 11.7.700.169 or later, or Google Chrome PepperFlash 11.7.700.179 or later.	10.0 (v2B)
Relevant CVE's: CVE-2013-1378, CVE-2013-1379, CVE-2013-1380, CVE-2013-2555		

48.	**Flash Player = 10.3.183.75 / 11.7.700.169 Multiple Vulnerabilities (APSB13-14)** The remote Windows host has a browser plugin that is affected by multiple vulnerabilities. (66445)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Adobe Flash Player version 10.3.183.86 / 11.7.700.202 or later, or Google Chrome PepperFlash 11.7.700.202 or later.	10.0 (v2B)
Relevant CVE's: CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, CVE-2013-3335		

49.	**Flash Player = 10.3.183.86 / 11.7.700.202 Memory Corruption (APSB13-16)** The remote Windows host has a browser plugin that is affected by a memory corruption vulnerability. (66872)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Adobe Flash Player version 10.3.183.90 / 11.7.700.224 or later, or Google Chrome PepperFlash 11.7.700.225 or later.	10.0 (v2B)
Relevant CVE's: CVE-2013-3343		

[redacted]

C	Upgrade to Microsoft Edge version 108.0.1462.54 or later.	8.8 (v3B)
Relevant CVE's: CVE-2022-4436, CVE-2022-4437, CVE-2022-4438, CVE-2022-4439, CVE-2022-4440		

350.	**KB5022282: Windows 10 Version 20H2 / Windows 10 Version 21H2 / Windows 10 Version 22H2 Security Update (January 2023)** The remote Windows host is affected by multiple vulnerabilities. (169787)	
Risk	Recommendation(s)	CVSS Score
C	Apply Security Update 5022282	9.1 (v3B)
Relevant CVE's: CVE-2023-21524, CVE-2023-21525, CVE-2023-21527, CVE-2023-21532, CVE-2023-21535, CVE-2023-21536, CVE-2023-21537, CVE-2023-21539, CVE-2023-21540, CVE-2023-21541, CVE-2023-21543, CVE-2023-21546, CVE-2023-21547, CVE-2023-21548, CVE-2023-21549, CVE-2023-21550, CVE-2023-21551, CVE-2023-21552, CVE-2023-21555, CVE-2023-21556, CVE-2023-21557, CVE-2023-21558, CVE-2023-21559, CVE-2023-21560, CVE-2023-21561, CVE-2023-21563, CVE-2023-21674, CVE-2023-21675, CVE-2023-21676, CVE-2023-21677, CVE-2023-21678, CVE-2023-21679, CVE-2023-21680, CVE-2023-21681, CVE-2023-21682, CVE-2023-21683, CVE-2023-21724, CVE-2023-21726, CVE-2023-21728, CVE-2023-21730, CVE-2023-21732, CVE-2023-21733, CVE-2023-21739, CVE-2023-21746, CVE-2023-21747, CVE-2023-21748, CVE-2023-21749, CVE-2023-21750, CVE-2023-21752, CVE-2023-21754, CVE-2023-21755, CVE-2023-21757, CVE-2023-21758, CVE-2023-21759, CVE-2023-21760, CVE-2023-21765, CVE-2023-21766, CVE-2023-21767, CVE-2023-21771, CVE-2023-21772, CVE-2023-21773, CVE-2023-21774, CVE-2023-21776		

351.	**Microsoft Edge (Chromium) 109.0.1518.49 / 108.0.1462.83 Multiple Vulnerabilities** The remote host has an web browser installed that is affected by multiple vulnerabilities. (170007)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Microsoft Edge version 109.0.1518.49 / 108.0.1462.83 or later.	8.8 (v3B)
Relevant CVE's: CVE-2023-0129, CVE-2023-0130, CVE-2023-0131, CVE-2023-0132, CVE-2023-0133, CVE-2023-0134, CVE-2023-0135, CVE-2023-0136, CVE-2023-0138, CVE-2023-0139, CVE-2023-0140, CVE-2023-0141		

352.	**Microsoft Edge (Chromium) 109.0.1343.27 Multiple Vulnerabilities** The remote host has an web browser installed that is affected by multiple vulnerabilities. (170725)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Microsoft Edge version 109.0.1343.27 or later.	8.8 (v3B)

Relevant CVE's: CVE-2023-0471, CVE-2023-0472, CVE-2023-0473, CVE-2023-0474

353.	**Microsoft Edge (Chromium) 109.0.1518.70 / 108.0.1462.95 Multiple Vulnerabilities** The remote host has an web browser installed that is affected by multiple vulnerabilities. (171332)	
Risk	Recommendation(s)	CVSS Score
C	Upgrade to Microsoft Edge version 109.0.1518.70 / 108.0.1462.95 or later.	8.8 (v3B)
Relevant CVE's: CVE-2023-0471, CVE-2023-0472, CVE-2023-0473, CVE-2023-0474		

354.	**Security Updates for Microsoft Word Products C2R (February 2023)** The Microsoft Word Products are missing a security update. (171554)	
Risk	Recommendation(s)	CVSS Score
C	For Office 365, Office 2016 C2R, or Office 2019, ensure automatic updates are enabled or open any office app and manually perform an update.	9.8 (v3B)
Relevant CVE's: CVE-2023-21716		

355.	**Security Updates for Outlook C2R Elevation of Privilege (March 2023)** The Microsoft Outlook application installed on the remote host is missing a security update. (172607)	
Risk	Recommendation(s)	CVSS Score
C	For Office 365, Office 2016 C2R, or Office 2019, ensure automatic updates are enabled or open any office app and manually perform an update.	9.8 (v3B)
Relevant CVE's: CVE-2023-23397		

356.	**Apple QuickTime Unsupported on Windows** Apple QuickTime is installed on the remote Windows host. (90544)	
Risk	Recommendation(s)	CVSS Score
C	Uninstall Apple QuickTime.	10.0 (v2B)

357.	**Windows DNS Server RCE (CVE-2020-1350)**	

	The remote Windows host is affected by multiple vulnerabilities. (138600)	
Risk	Recommendation(s)	CVSS Score
C	Apply the appropriate security update or mitigation as described in the Microsoft advisory.	10.0 (v3B)
Relevant CVE's: CVE-2020-1350		

Summary of Scanned Ports (By Server – Top 1024 Ports)

The following ports and associated services were discovered during the discovery.

Server	OS	Ports	Service	Notes
[redacted]		tcp/22	ssh	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		udp/123	ntp	
		tcp/135	epmap	
		udp/137	netbios-ns	
		udp/138	netbios-dgm	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
		udp/500	isakmp	
[redacted]		tcp/0		
		tcp/22	ssh	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		udp/123	ntp	
		tcp/135	epmap	
		udp/137	netbios-ns	
		udp/138	netbios-dgm	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
		udp/500	isakmp	
		tcp/623	oob-ws-http	
[redacted]		tcp/0		
		tcp/22	ssh	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/22	ssh	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/135	epmap	

[redacted]		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/21	ftp	
		tcp/23	telnet	
		tcp/80	www-http	
		tcp/139	netbios-ssn	
		tcp/515	printer	
		tcp/631	ipps	
[redacted]		tcp/135	epmap	
[redacted]		tcp/0		
[redacted]		tcp/0		
		tcp/443	https	
[redacted]		tcp/0		
[redacted]		tcp/0		
[redacted]		tcp/0		
[redacted]		tcp/0		
[redacted]		tcp/0		
[redacted]		tcp/0		
[redacted]		tcp/0		
[redacted]		tcp/0		
[redacted]		tcp/0		
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
[redacted]		tcp/0		
		tcp/23	telnet	
		tcp/515	printer	
		tcp/631	ipps	
[redacted]		tcp/0		
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/445	microsoft-ds	
[redacted]		tcp/135	epmap	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	

[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/139	netbios-ssn	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/21	ftp	
		tcp/80	www-http	
		tcp/139	netbios-ssn	
[redacted]		tcp/0		
		tcp/22	ssh	
[redacted]		tcp/0		
		tcp/22	ssh	
		tcp/443	https	
[redacted]		tcp/0		
		tcp/22	ssh	
		tcp/80	www-http	
		tcp/427	svrloc	
		tcp/443	https	
		tcp/902	ideafarm-door	
[redacted]		tcp/0		
		tcp/23	telnet	
		udp/67	bootps	
		udp/68	bootpc	
		udp/161	snmp	
		udp/521	ripng	
[redacted]		tcp/0		
		tcp/22	ssh	
		tcp/23	telnet	
		udp/67	bootps	
		tcp/80	www-http	
[redacted]		tcp/0		
		tcp/22	ssh	
		tcp/80	www-http	
		tcp/427	svrloc	
		tcp/443	https	
		tcp/902	ideafarm-door	
[redacted]		tcp/0		
		tcp/22	ssh	
		tcp/80	www-http	
		tcp/427	svrloc	

[redacted]		tcp/443	https	
		tcp/902	ideafarm-door	
[redacted]		tcp/0		
		tcp/80	www-http	
		tcp/427	svrloc	
		tcp/443	https	
		tcp/902	ideafarm-door	
[redacted]		tcp/0		
		tcp/80	www-http	
		tcp/427	svrloc	
		tcp/443	https	
		tcp/902	ideafarm-door	
[redacted]		tcp/0		
		tcp/25	smtp	
		tcp/443	https	
		tcp/705	agentx	
[redacted]		tcp/0		
[redacted]		tcp/0		
		tcp/80	www-http	
		tcp/443	https	
		tcp/554	rtsp	
[redacted]		tcp/0		
		tcp/25	smtp	
		tcp/80	www-http	
		udp/137	netbios-ns	
		tcp/139	netbios-ssn	
		tcp/443	https	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/23	telnet	
		udp/67	bootps	
		tcp/80	www-http	
[redacted]		tcp/0		
		tcp/80	www-http	
		tcp/443	https	
[redacted]		tcp/0		
		tcp/80	www-http	
		tcp/554	rtsp	
		tcp/555	dsf	
		tcp/556	remotefs	
		tcp/557	openvms-sysipc	
		tcp/558	sdnskmp	
[redacted]		tcp/0		
		tcp/80	www-http	
		tcp/554	rtsp	
		tcp/555	dsf	
		tcp/556	remotefs	
		tcp/557	openvms-sysipc	
		tcp/558	sdnskmp	
[redacted]		tcp/0		

[redacted]		tcp/445	microsoft-ds	
		udp/500	isakmp	
[redacted]		tcp/0		
		udp/123	ntp	
		tcp/135	epmap	
		udp/137	netbios-ns	
		udp/138	netbios-dgm	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
		udp/500	isakmp	
[redacted]		tcp/0		
		tcp/80	www-http	
		tcp/427	svrloc	
		tcp/443	https	
		tcp/902	ideafarm-door	
[redacted]		tcp/0		
		tcp/22	ssh	
[redacted]		tcp/0		
		tcp/22	ssh	
[redacted]		tcp/0		
		tcp/23	telnet	
		tcp/80	www-http	
[redacted]		tcp/0		
		udp/123	ntp	
		tcp/135	epmap	
		udp/137	netbios-ns	
		udp/138	netbios-dgm	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
		udp/500	isakmp	
		tcp/623	oob-ws-http	
[redacted]		tcp/0		
		tcp/21	ftp	
		tcp/23	telnet	
		udp/53	domain	
		tcp/80	www-http	
		tcp/111	sunrpc	
		udp/137	netbios-ns	
		udp/138	netbios-dgm	
		tcp/139	netbios-ssn	
		udp/161	snmp	
		tcp/443	https	
		tcp/514	shell	
		tcp/515	printer	
		tcp/631	ipps	
		tcp/1022	exp2	
		tcp/1023		
[redacted]		tcp/0		
		udp/123	ntp	
		tcp/135	epmap	

[redacted]		udp/137	netbios-ns	
		udp/138	netbios-dgm	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
		udp/500	isakmp	
		tcp/623	oob-ws-http	
[redacted]		tcp/0		
		tcp/80	www-http	
		udp/137	netbios-ns	
		udp/161	snmp	
		tcp/443	https	
		tcp/515	printer	
		tcp/631	ipps	
[redacted]		tcp/0		
		tcp/21	ftp	
		tcp/23	telnet	
		udp/53	domain	
		tcp/80	www-http	
		udp/137	netbios-ns	
		udp/138	netbios-dgm	
		tcp/139	netbios-ssn	
		udp/161	snmp	
		tcp/443	https	
		tcp/514	shell	
		tcp/515	printer	
		tcp/631	ipps	
[redacted]		tcp/0		
		tcp/21	ftp	
		tcp/23	telnet	
		udp/53	domain	
		tcp/80	www-http	
		tcp/111	sunrpc	
		udp/137	netbios-ns	
		udp/138	netbios-dgm	
		tcp/139	netbios-ssn	
		udp/161	snmp	
		tcp/443	https	
		tcp/514	shell	
		tcp/515	printer	
		tcp/631	ipps	
		tcp/1022	exp2	
		tcp/1023		
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		

[redacted]		tcp/135	epmap	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		udp/123	ntp	
		tcp/135	epmap	
		udp/137	netbios-ns	
		udp/138	netbios-dgm	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
		udp/500	isakmp	
		tcp/623	oob-ws-http	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/445	microsoft-ds	
[redacted]		tcp/0		
		udp/123	ntp	
		tcp/135	epmap	
		udp/137	netbios-ns	
		udp/138	netbios-dgm	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
		udp/500	isakmp	
		tcp/623	oob-ws-http	
[redacted]		tcp/0		
		tcp/80	www-http	
[redacted]		tcp/0		
		udp/123	ntp	
		tcp/135	epmap	
		udp/137	netbios-ns	
		udp/138	netbios-dgm	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	
		udp/500	isakmp	
[redacted]		tcp/0		
		tcp/80	www-http	
[redacted]		tcp/0		
		tcp/135	epmap	
		tcp/139	netbios-ssn	
		tcp/445	microsoft-ds	

Tools Utilized

The following tools were employed during the course of the assessment and penetration testing effort:

Tool	Version
• Nessus Professional	8.14.0
• AIT ReportGen	0.3.4

References

Document	Link
1. Common Vulnerability Scoring System v3.0: Specification Document	https://www.first.org/cvss/specification-document

Appendix D: Sample Phishing Campaign Report

Appendix 2: Sample Phishing Campaign Report

This is an actual client report summarizing a Phishing campaign where some of the information has been redacted for the purpose of confidentiality.

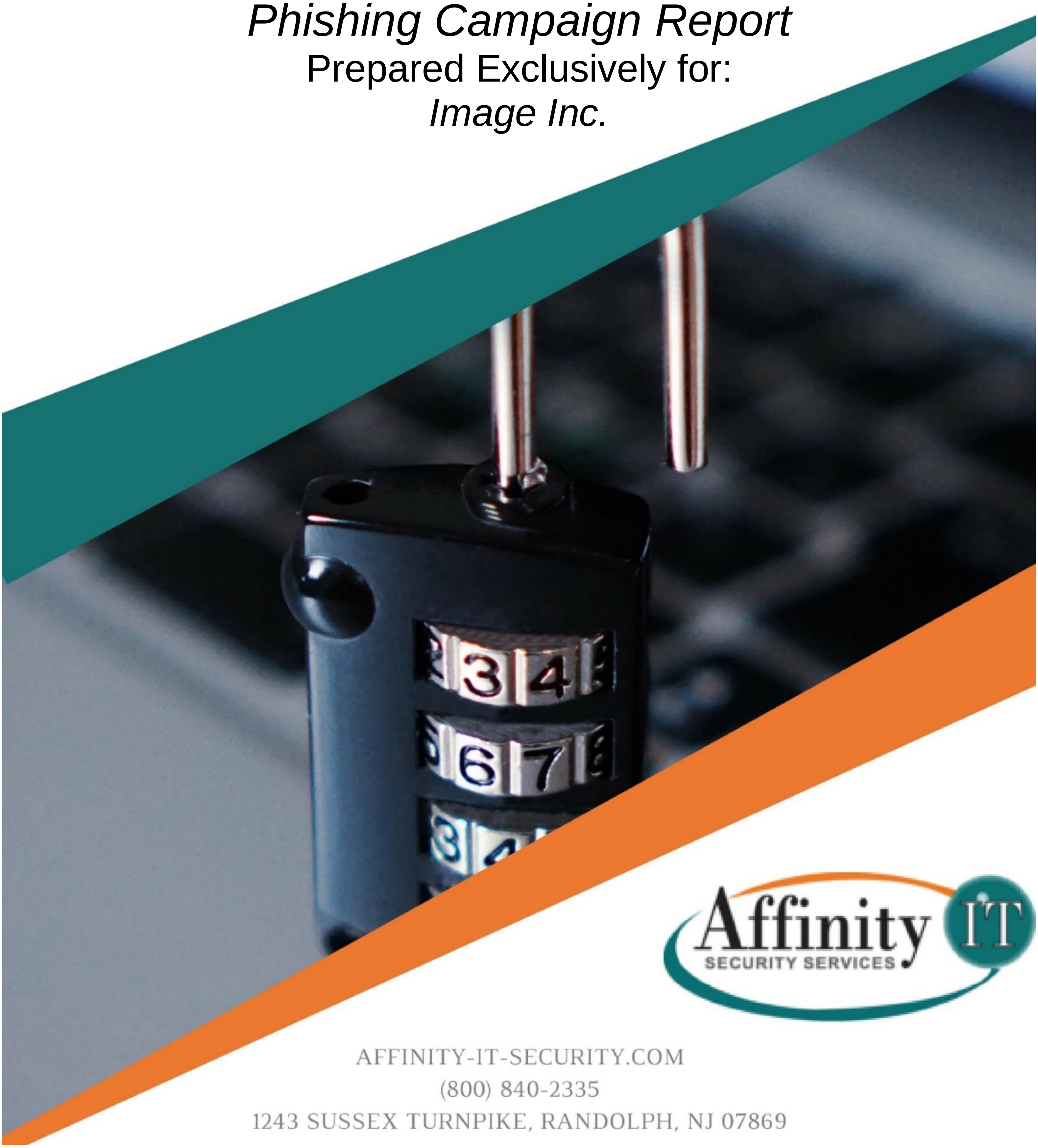
“Image Inc” is a fictional company, used to make the sample report more readable.

As you review the report, we ask that you note:

- The clarity and conciseness of the presentation of results
- The explanation of the simulated phish with an emphasis on what should have been “red flags”.

Phishing Campaign Report

Prepared Exclusively for:
Image Inc.



AFFINITY-IT-SECURITY.COM
(800) 840-2335
1243 SUSSEX TURNPIKE, RANDOLPH, NJ 07869

Executive Summary

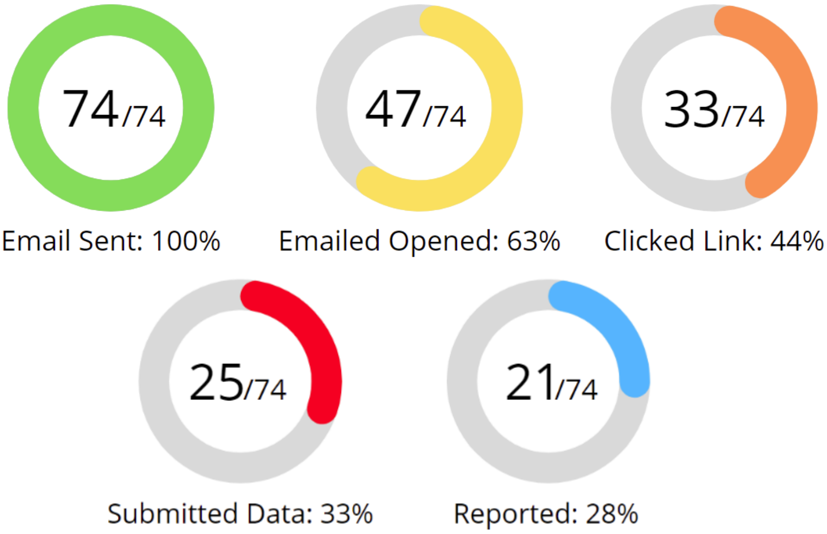
Affinity IT Security Services has been engaged to conduct phishing[1] testing against the employees and staff of Image Inc. To that end, phishing emails have been sent to a target list provided by the client, and this report details the response to those emails. Image has an anti-spam solution in place, and it was necessary to whitelist the origination of the phishing emails for the test to proceed. The purpose of a phishing exercise is to quantify and baseline the organizational response to phishing, and thus indirectly reflect its vulnerability to malicious email. The insights yielded by this exercise, especially when paired with educational/awareness initiatives, can help to significantly reduce the click-rate response to phishes.

Over the course of this initiative, one phishing email blast (i.e., “campaign”) was sent. In the campaign, the same personally addressed email content was sent to all recipients, and each communication was designed to include only publicly available information. The content of each email can be found in the Phishing Campaign Analysis of this report.

Summary Statistics:

On February 15th, 2022:

- **74** emails were sent out, of which:
  - **47 (~63%)** individuals opened the email
  - **33 (~44%)** clicked the link
    - ➢ **25 (~32%)** submitted data (credentials)[2]
  - **21 (~28%)** recipients reported the phish as suspicious



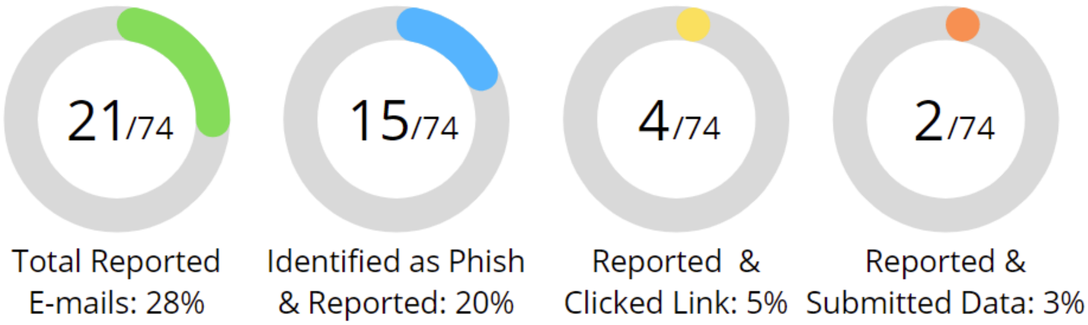
[1] **See:** A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person (source: https://csrc.nist.gov/).

[2] **See:** The individuals who submitted data also are counted in the sum of the ‘Clicked Link’ individuals.

Reported

Reported E-mail statistics:

- **21 (~28%)** total reported the E-mail as suspicious
  - **15 (~20%)** correctly identified the E-mail as a Phish without any further interaction with the message
  - **4 (~5%)** reported the E-mail after clicking the link
  - **2 (~3%)** reported the E-mail after submitting credentials

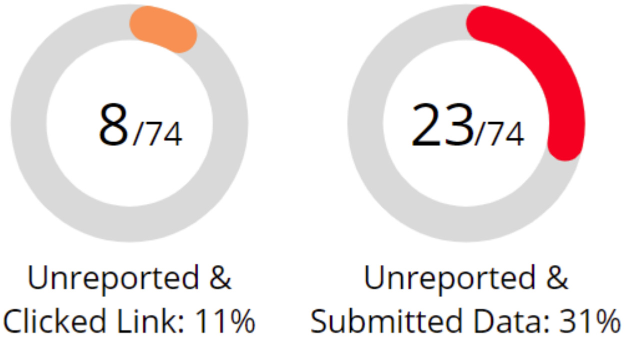


Unreported

Total unreported and successfully phished users:

- **8 (11%)** clicked the link
- **23 (31%)** clicked the link and surrendered their credentials

This is cause for concern



The response rate to the campaign was more than the industry average of 31.4%[3]. This rate is high enough to be concerning, as it suggests a targeted attack against the organization to harvest credentials or potentially compromise devices could be successful.

[3] **See:** https://blog.knowbe4.com/knowbe4s-2021-phishing-by-industry-benchmarking-report-reveals-that-31.4-of-untrained-end-users-will-fail-a-phishing-test

Scoring

Risk in this context represents the susceptibility of an individual to click on a link contained in a phishing email OR surrender their account credentials. A numeric risk "score" between -2 and 2 is calculated for each individual receiving phishes, and values ≤ 0 are considered low risk whereas value ≥ 2 are considered higher risk. **An individual's "Risk Score" always represents their cumulative behavior** with respect to test phishes.

Low Risk	Moderate Risk	High Risk
0 ≤	1	≥ 2

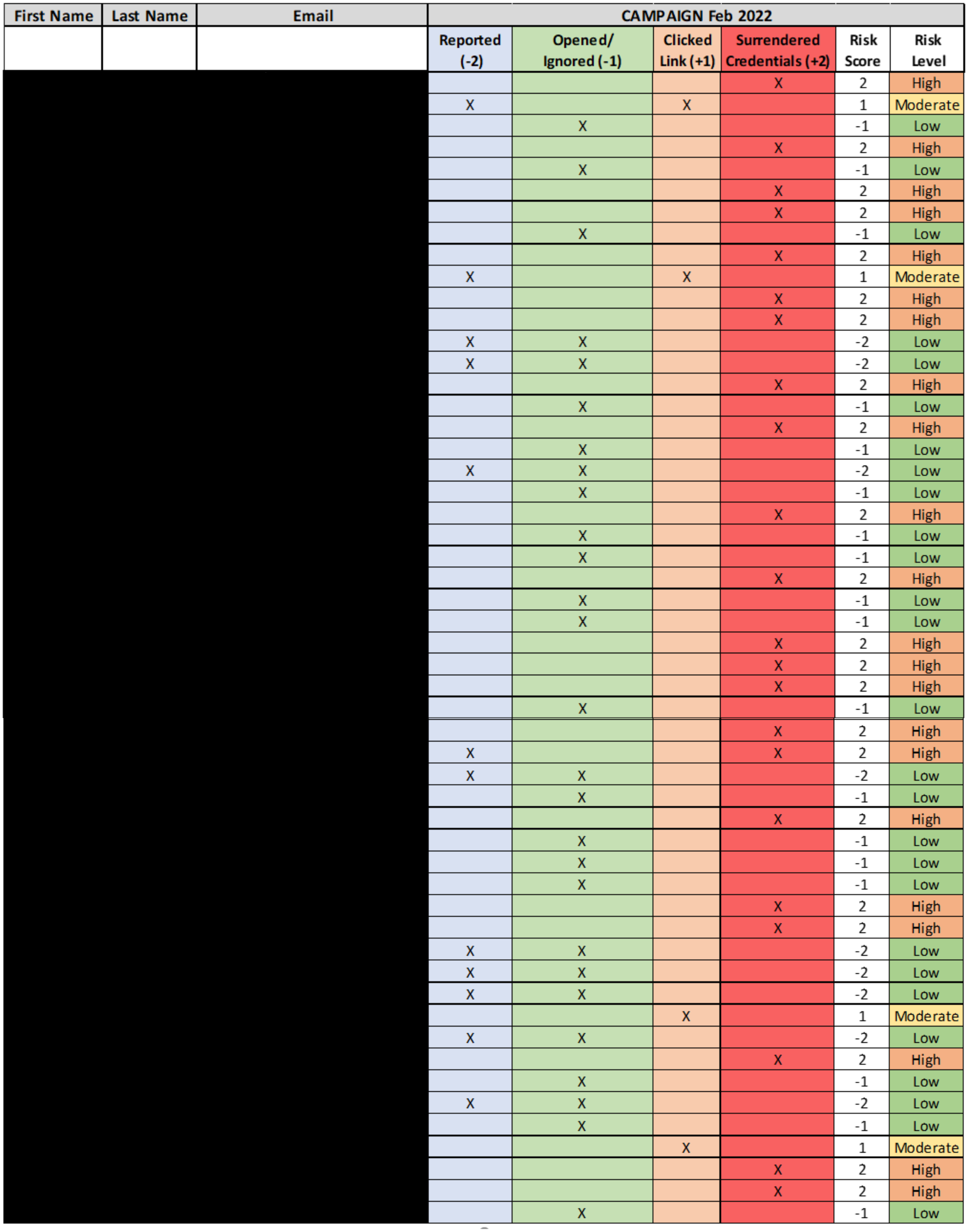
Reported (-2)
Reported the email as suspicious

Clicked Link (+1)
Read E-mail and clicked the the embedded link

Opened/Ignored (-1)
Ignored or read the E-mail and took no further action

Surrendered Credentials (+2)
Read E-mail clicked the the embedded link and input

First Name	Last Name	Email	CAMPAIGN Feb 2022					
			Reported (-2)	Opened/ Ignored (-1)	Clicked Link (+1)	Surrendered Credentials (+2)	Risk Score	Risk Level
[redacted]	[redacted]	[redacted]	X		X		1	Moderate
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]			X		1	Moderate
[redacted]	[redacted]	[redacted]	X			X	2	High
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]	X		X		1	Moderate
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]	X		X		1	Moderate
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]			X		1	Moderate
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]		X			-1	Low



First Name	Last Name	Email	CAMPAIGN Feb 2022					
			Reported (-2)	Opened/ Ignored (-1)	Clicked Link (+1)	Surrendered Credentials (+2)	Risk Score	Risk Level
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]	X		X		1	Moderate
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]	X		X		1	Moderate
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]	X			X	2	High
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]			X		1	Moderate
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]	X	X			-2	Low
[redacted]	[redacted]	[redacted]		X			-1	Low
[redacted]	[redacted]	[redacted]			X		1	Moderate
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]				X	2	High
[redacted]	[redacted]	[redacted]		X			-1	Low

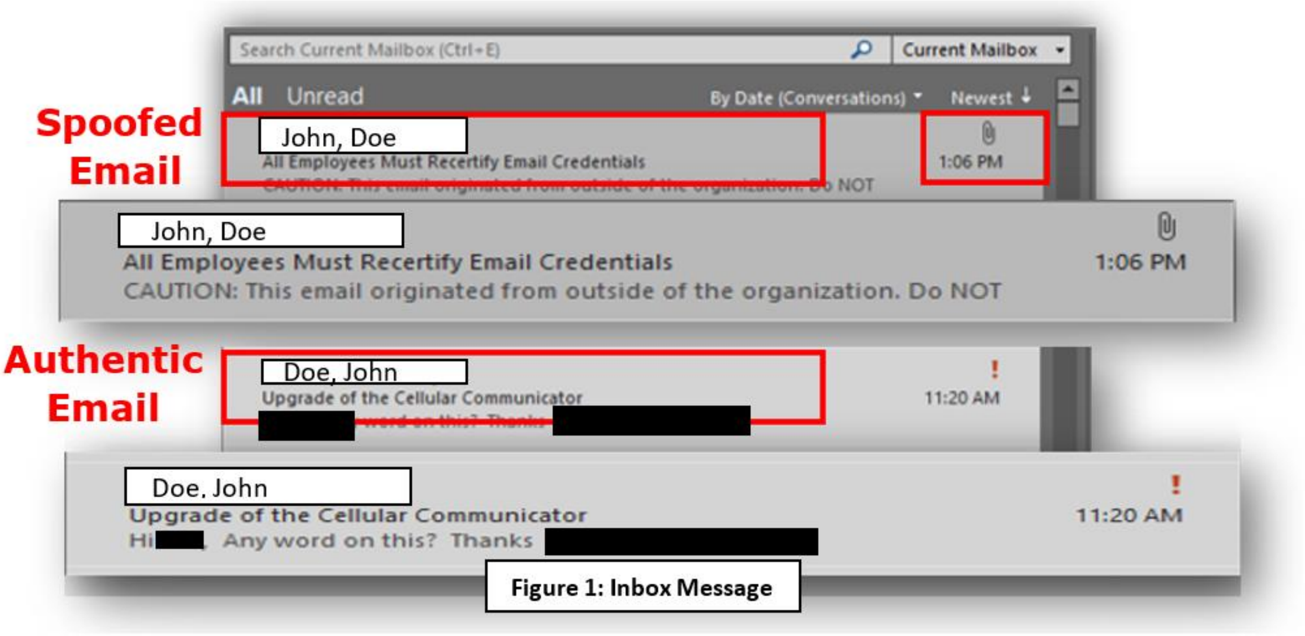
Phishing Campaign Analysis

The analysis of the phishing E-mail is a breakdown of the many indicators and/or flags that could help the user make an informed decision whether to trust the source of the message. What makes our campaign particularly more dangerous than regular spam is that the hacker is using the spear-phishing method, meaning the message is not a generic E-mail informing you that “your car warranty is about to expire”, but has in depth knowledge of who to pose as, to make his message seem more legitimate, who to target, E-mail banners, E-mail signature etc. There is motive behind a spear-phish E-mail which could be anything from ransomware to extortion or unauthorized access to Image IT resources.

If anything seems off about the message and the user is not sure about the legitimacy of the E-mail, it is important to contact IT staff for clarification. In the instance of erroneously clicking a malicious link, informing the IT staff of the mistake as soon as possible is crucial.[4]

Inbox Display

The phish E-mail indicates that there is an attachment, but the only attached file is the company logo. Normally company logos should not be an attachment. They are an embedded image that does not come through as an attached file. Additionally, recipients should be on the lookout for inconsistencies in the name formatting of the sender (if there is a standard format), as well as the grammar of the E-mail body.



John, Doe
All Employees Must Recertify Email Credentials
CAUTION: This email originated from outside of the organization. Do NOT
1:06 PM

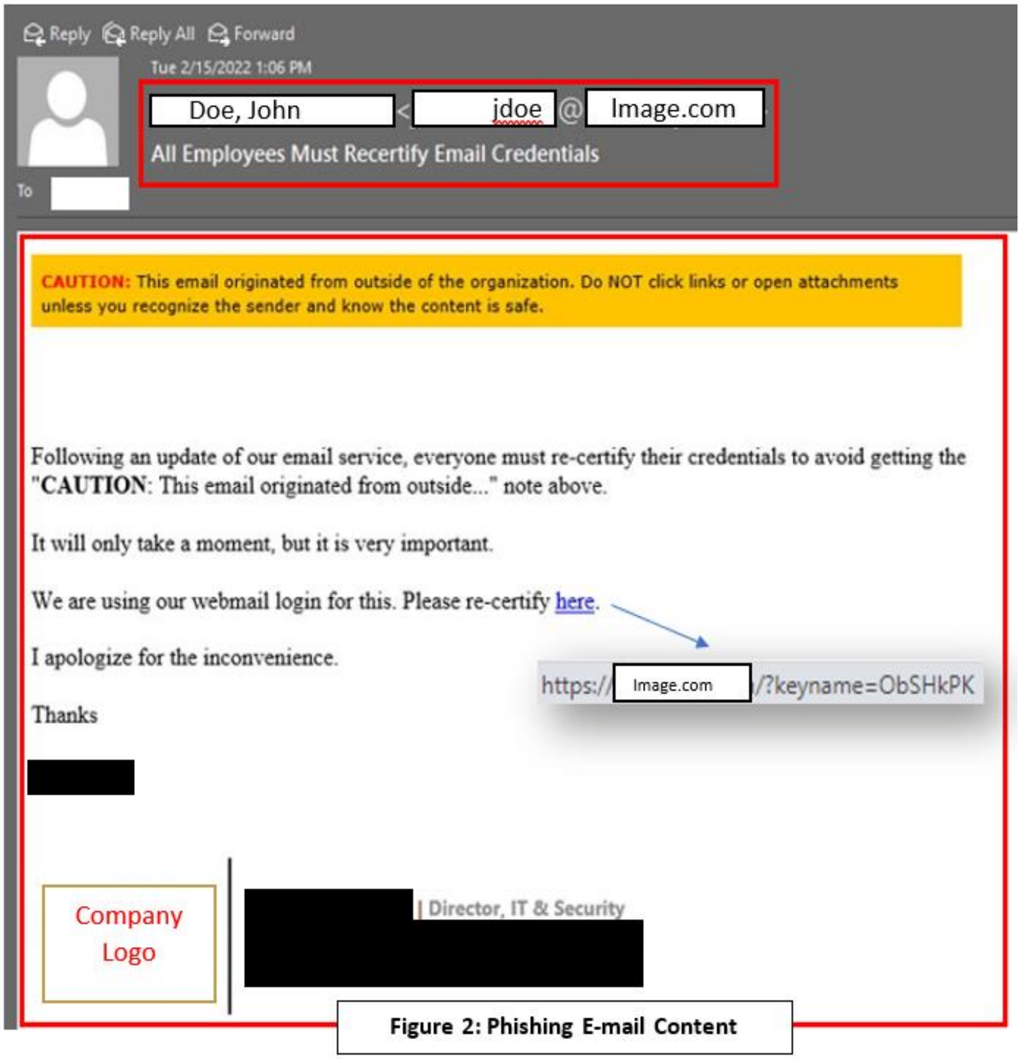
Doe, John
Upgrade of the Cellular Communicator
Hi [redacted], Any word on this? Thanks [redacted]
!
11:20 AM

Figure 1: Inbox Message

[4] **See:** Such as was the case with six individuals who either clicked, submitted, and then reported.

E-Mail Content

The sender E-mail address has been spoofed to make it look like it's coming from inside the company, but only the letter "i" in "@Image.com" was replaced by the letter "l" making it look close enough to pass the users initial inspection of the message.



Tue 2/15/2022 1:06 PM

Doe, John < jdoe @ Image.com

All Employees Must Recertify Email Credentials

CAUTION: This email originated from outside of the organization. Do NOT click links or open attachments unless you recognize the sender and know the content is safe.

Following an update of our email service, everyone must re-certify their credentials to avoid getting the "**CAUTION**: This email originated from outside..." note above.

It will only take a moment, but it is very important.

We are using our webmail login for this. Please re-certify here.

https:// Image.com /?keyname=ObSHkPK

I apologize for the inconvenience.

Thanks

[redacted]

Company Logo

[redacted] | Director, IT & Security

[redacted]

Figure 2: Phishing E-mail Content

If the E-mail came from within the company, the yellow CAUTION banner should not have displayed, even though the sender's message indicates otherwise.

In the message the attacker explains why the E-mail has a yellow CAUTION banner in an attempt to fool the user into believing the E-mail is legitimate, and then encourages the user to perform a certain action. In this case it would mean clicking on the URL link and logging in with the phished credentials.

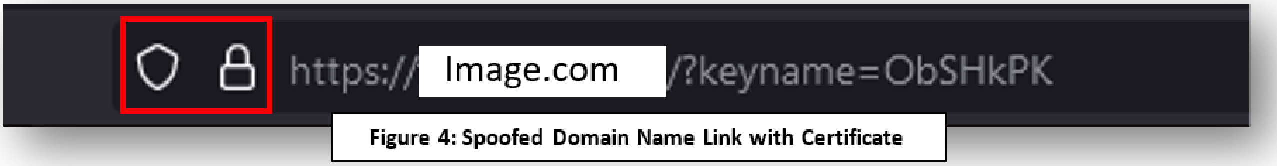
The shortened URL link redirects the user to a spoofed website that the hacker "stole"[5] from the Image.com website. Shortened links, especially those from outside of the company should not be trusted. The link itself can be inspected without clicking on it, by hovering over it with the mouse pointer. When in doubt, it is always better to operate through an official link known to be legitimate or type the URL into the address bar that you have used previously, as opposed to using a shortcut from the E-mail.

Other tell-tale signs that might tip off the user are the use of a nonstandard font type and font color, which was the case with this E-mail.

[5] **See:** The E-mail login page was cloned directly from Image.com for this exercise. For the purposes of this test, recipients who clicked were directed to a "pseudo-malicious" site controlled by Affinity-IT.

Clicking the URL

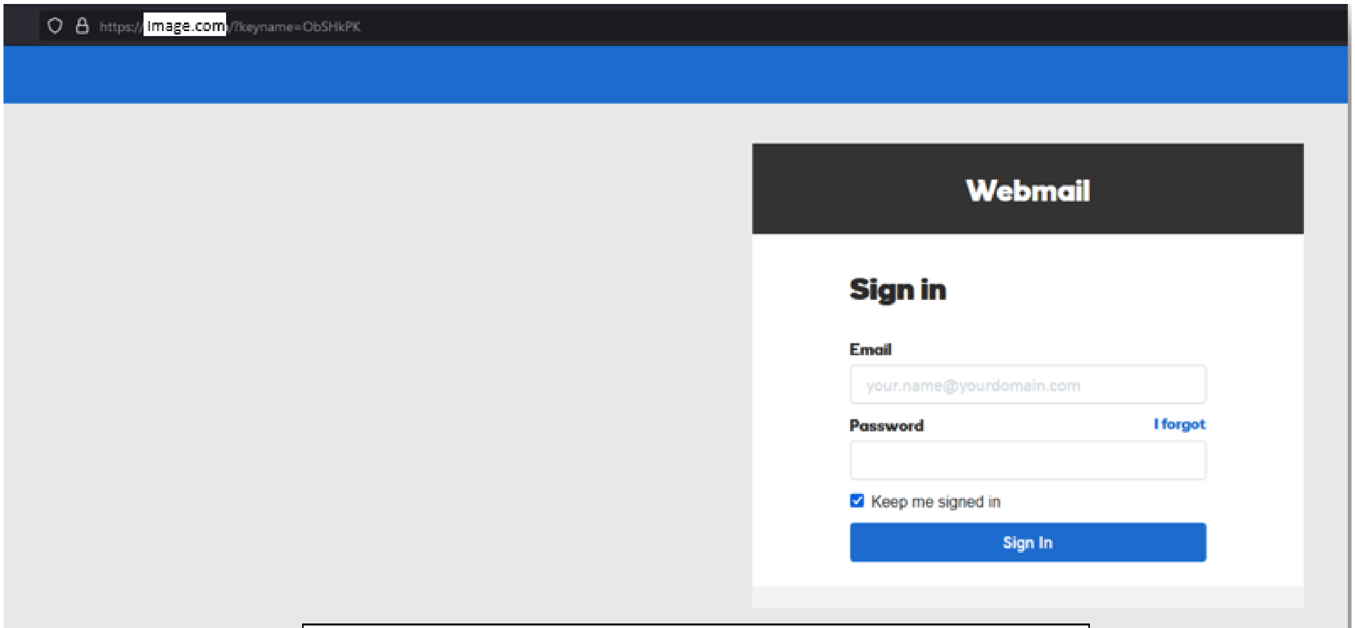
For many years, one of the primary tips for avoiding phishing sites has been to examine URLs carefully and avoid sites that do not have an SSL certificate. “HTTPS” in the URL (versus “HTTP”) signifies that a site has an SSL certificate and is protected by the HTTPS encryption protocol. However, this is no longer a reliable tactic for recognizing dubious sites. Many if not most phishing campaigns create their own SSL certificates, to make their URLs look more legitimate.



https:// Image.com /?keyname=ObSHkPK

Figure 4: Spoofed Domain Name Link with Certificate

The URL link in the E-mail did not direct the user to the Image.com E-mail portal, but rather to a spoofed Webmail login page which served as a credential capture portal for the attacker.



https:// Image.com /?keyname=ObSHkPK

Webmail

Sign in

Email

your.name@yourdomain.com

Password

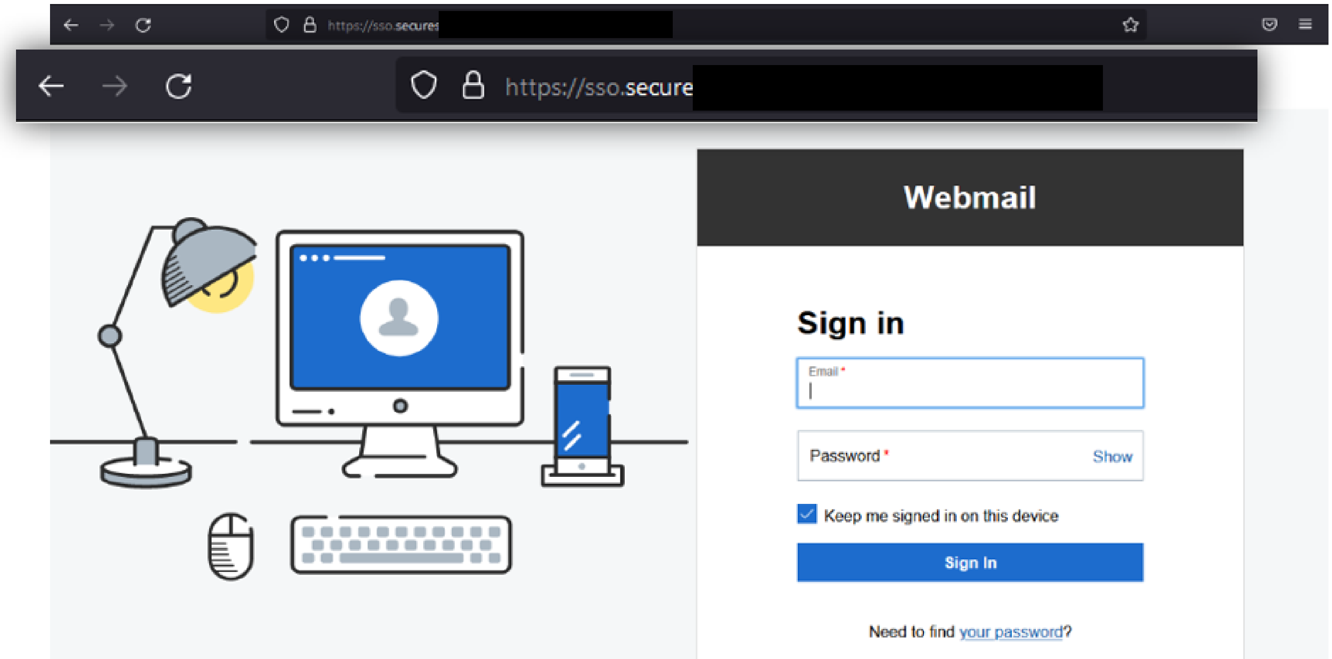
I forgot

☑ Keep me signed in

Sign In

Figure 5: Spoofed website copied from Image.com

After the user inputs their credentials, the spoofed site captures the event and redirects the user to the official Image.com login portal. The action of logging in and being redirected to another site to login once more should set off red flags for the user.



https://sso.secure[redacted]

https://sso.secure[redacted]

Webmail

Sign in

Email *

Password * Show

☑ Keep me signed in on this device

Sign In

Need to find your password?

Figure 6: Official Image.com login portal

At this point the attacker has received submitted credentials, granting them full access to the user's E-mail account, leaving the company open to further exploits, such as false payment and wire transfer scams.

Additional Insights

Affinity IT's initial efforts to the send the spear-phish E-mail were blocked by Image Inc. anti-spam solution (Proof-Point) due to several factors:

- To send a custom crafted E-mail, Affinity IT utilized a virtual private server hosted in the cloud with an automatically assigned external IP address. For that reason, whitelisting the Phishing E-mail IP was necessary.
- E-Mail reputation plays a big factor in E-mail delivery. Since conducting a new campaign is limited on time, our attack mailbox did not have enough credibility to become more reputable. This was another red flag that should have been detected.
- The domain name purchased for the spoofed E-mail delivery website (Image.com) was also newly registered, not having enough time to "age out". The longer a domain is registered, the better reputation it can have for E-mail delivery. Another red flag.

Although our attempts were blocked by the anti-spam solution, this does not mean an attacker would not have been able to penetrate the network. All these factors are easily addressed by an attacker with enough time and effort. Utilizing a "defense in depth" strategy (many security tools) is essential for security but should not give the user a false sense of security. Vigilance is key!

Conclusion

Results suggest that Image Inc. is vulnerable to phishing, and the corresponding cybersecurity risk that accompanies it. Affinity IT Security suggests ongoing anti-phishing efforts to continue, including phishing awareness training. In addition, testing should be performed until a persistent decrease in click rate has been achieved.

1243 Sussex Turnpike, Suite #1 Randolph, NJ 07869

www.Affinity-IT.com

(800) 840-2335

info@affinity-it.com

AFFINITY

SECURITY SERVICES

EXHIBIT A - Pricing Page

Item #	Section	Description of Service	*Estimated Number of Assessments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	$ 2,395 -	$ 19,160 -
2	4.2	Website Penetration Testing	8	$ 995 -	$ 7,960 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	$ 1,995 -	$ 15,960 -
4	4.4	Wireless Penetration Testing	8	$ 1,995 -	$ 15,960 -
				TOTAL BID AMOUNT	$ 59,040 -

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:	Affinity IT, LLC
Vendor Address:	1243 Sussex Turnpike, Suite #1 Randolph, NJ 07869
Email Address:	joe@affinity-it.com
Phone Number:	800-840-2335
Fax Number:	
Signature and Date:	Joseph W Fisher 3/28/2024

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)