A COMPANY'S SECURITY SUCCESS STORY BEGINS WITH VULNERABILITY ASSESSMENTS

ENTERPRISE INTEGRATION

EXECUTIVE SUMMARY

Between 2015 and 2017, Enterprise Integration's Security Operations (SecOps) team worked with a Fortune 1000 company to identify potential vulnerabilities in devices and applications. The vulnerabilities discovered included unpatched software, unnecessary open ports, misconfigured services, weak credentials, and other missing security controls. SecOps provided subject matter expertise and performed quarterly assessments to identify new vulnerabilities and areas of configuration weakness followed by specific remediation actions. As part of their recommendation for a good security program, all vulnerability assessments should be conducted once per quarter or whenever significant infrastructure changes are made. This allows companies to identify their external exposure.

CHALLENGES

TO ASSESS THE EFFECTIVENESS
OF THE CLIENT'S INFORMATION
SECURITY PROGRAM

Vulnerabilities were discovered through a series of assessments. Citrix Netscaler and Microsoft Windows systems showed possible weaknesses that could open the client's organization up to security breaches. As part of the assessment strategy, SecOps included other areas of concern such as TLS and SSL protocol configurations and other missing or inadequate security controls.

ASSESSMENT FINDINGS

For detailed information on reading graphs and vulnerability types based on severity, refer to ***Terms for Reviewing Graphs and Severity Scale section.***

During the two-year period when quarterly scans were conducted, the SecOps team found seven (7) Urgent vulnerabilities which constituted 1% of the overall assessments performed. System weaknesses estimated to be Serious only constituted 12% of the scans while 11% were considered to be of Medium risk to system security. Of the 739 scans run, 76% of the vulnerabilities were deemed Minimal.

WE WERE ABLE TO
REDUCE SERIOUS VULNERABILITIES
TO 5.4%

Exploitation of any of these vulnerabilities would have cost our client millions, however, through remediation we were able to reduce the Serious (see Figure 5) vulnerabilities to 5.4%.

To assess vulnerabilities shown in Figure 1, the public IP space provided by the customer was scanned.

When SecOps performs a scan, all findings fall into three (3) categories: Vulnerability, Potential Vulnerability, and Information Gathered and each category uses the Severity scale (see Terms for Reviewing Graphs and Severity Scales section). Information Gathered, as defined by the scanner, includes visible information about the network related to the host, such as traceroute information, ISP, or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

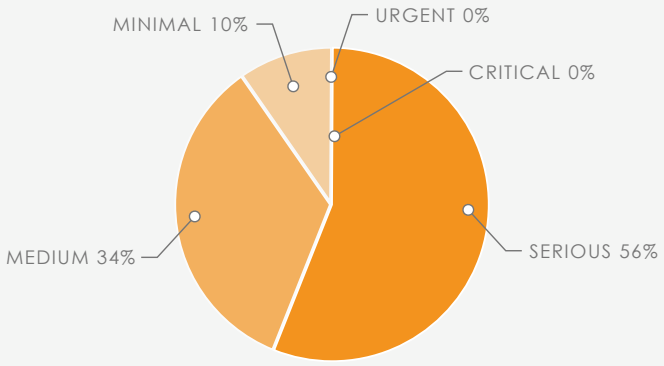
A potential vulnerability cannot be confirmed through a scan and must be manually investigated. To verify the existence of such vulnerabilities on the network would require an intrusive scan, which could result in a denial of service.

EXAMPLE: A Cross-Site Scripting Vulnerability in ASP.NET when using 'ValidateRequest Filter. The scanner can identify the version of ASP.NET version, but it cannot confirm the existence of the cross-site scripting attack.

By utilizing a comprehensive vulnerability scanning tool, SecOps scanned for potential vulnerabilities. The result was that the client had 7 Urgent vulnerabilities out of 17. If these remained unpatched (ports left open, etc.), the client would have been at greater risk of a breach which could cost the company up to $11,000 per incident if the company's systems were breached due to this vulnerability. Furthermore, the later a vulnerability is found, the more it can cost to remediate. If the breach involved sensitive data, the company could face fines costing into the millions for the breach in addition to the cost of the remediation.

VULNERABILITIES

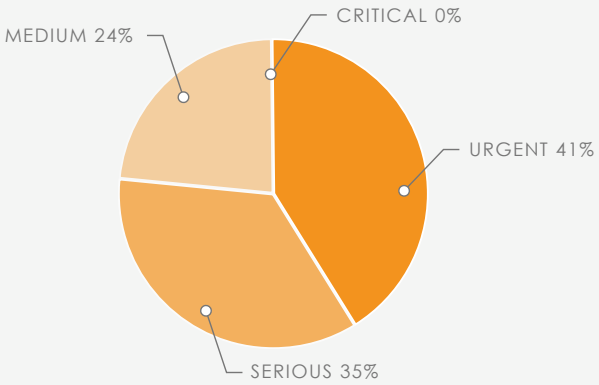
FIGURE 1. VILNERABILITIES



SEVERITY	COUNT	%
URGENT	0	0%
CRITICAL	0	0%
SERIOUS	69	56%
MEDIUM	42	34%
MINIMAL	12	10%
TOTAL	**123**	**100%**

POTENTIAL VULNERABILITIES

FIGURE 2. POTENTIAL VULNERABILITIES



SEVERITY	COUNT	%
URGENT	7	41%
CRITICAL	0	0%
SERIOUS	6	35%
MEDIUM	4	24%
MINIMAL	0	0%
TOTAL	**17**	**100%**

The Overall graph combines Vulnerabilities, Potential Vulnerabilities, and Information Gathered to display a complete picture of the findings from the scans. The results show a high-level view of the company's exposure or risk.

Overall, the client reduced their Urgent vulnerabilities from 41% (Figure 2) to 1% (Figure 4) potentially saving them up to $3 million based on the national average cost of a data breach had the company's systems been compromised due to exploitation of these vulnerabilities.

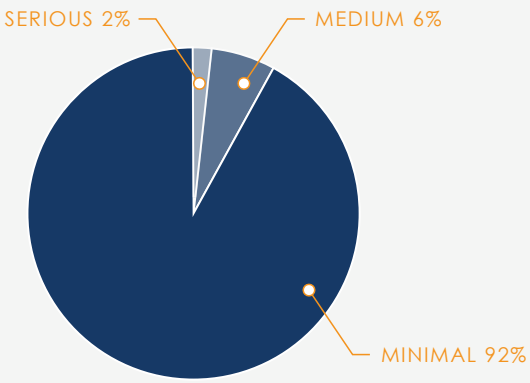
REMEDIATION

REMEDIATE KNOWN VULNERABILITIES, CONDUCT REGULAR **ASSESSMENTS**, & IMPLEMENT CONTINUOUS **MONITORING**

Enterprise Integration's Security Operations team conducted an assessment of the company's networks, servers, and desktops and then identified threats to the systems. SecOps utilized managed protective services to offer protection from spyware, viruses, and spam as well as other malware-based threats. Additional services consisted of content-based redirection and blocking to protect systems from malicious files, data loss prevention (DLP), and to handle load balancing. The team also setup single sign-on management, multi-factor authentication and automated user provisioning and

INFORMATION GATHERED

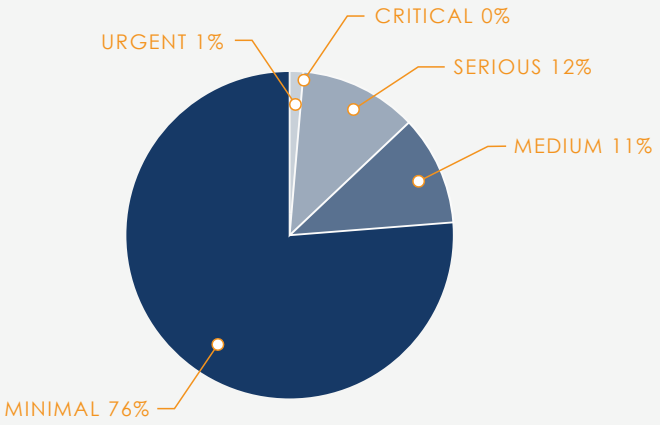
FIGURE 3. INFORMATION GATHERED



SEVERITY	COUNT	%
SERIOUS	11	2%
MEDIUM	37	6%
MINIMAL	551	92%
TOTAL	**599**	**100%**

OVERALL

FIGURE 4. VULNERABILITIES



SEVERITY	COUNT	%
URGENT	7	1%
CRITICAL	0	0%
SERIOUS	86	12%
MEDIUM	83	11%
MINIMAL	563	76%
TOTAL	**739**	**100%**

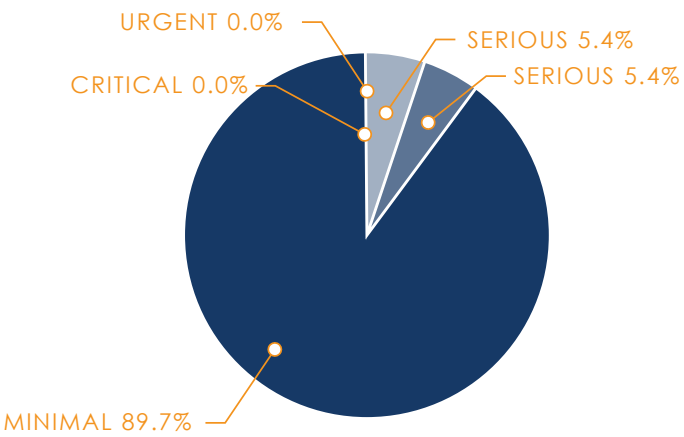
deprovisioning to complete pre-defined tasks without human intervention. These managed services included federated identity management which authorizes users to access multiple enterprise applications using the same identification. The team's cloud-based security services covered proxy-web content filtering, mobility, wireless and VPN.

Security Operations monitored, managed, and configured network devices as well as site-to-site and client LAN to LAN (L2L) connections, and provided antispam, URL/ content filtering and antivirus protection.

Through these services and multiple vulnerability scans, the team was able to remediate all but 516 confirmed and potential vulnerabilities. Only 5% were considered serious (Figure 5) and could be mitigated by applying strategic changes to specific security controls followed by enhanced monitoring.

VULNERABILITIES

FIGURE 5. POST MITIGATION VULNERABILITIES FINDINGS



SEVERITY	COUNT	%
URGENT	0	0.00%
CRITICAL	0	0.00%
SERIOUS	28	5.40%
MEDIUM	25	4.80%
MINIMAL	463	89.70%
TOTAL	**516**	**100%**

Post-Remediation Findings

RESULTS REVEAL THAT HAVING A **SECURITY OPERATIONS TEAM CAN REDUCE** A COMPANY'S **EXTERNAL EXPOSURE**

The Post-Remediation Findings Vulnerabilities graph shows the company's current risk after the remediation of the most severe findings was complete. In comparing the graph with the initial findings, it is clear that the company has greatly improved their security posture. The results reveal that having a Security Operations team provide scanning and remediation recommendations can reduce a company's external exposure.

By reducing their external exposure from 41% Urgent (Figure 2) to 0% Urgent (Figure 5), the company saved between $1 and $6 million based on the number of records that may have been breached had the risk and vulnerabilities not been identified and remediated.

RESULTS

HAVING A **COMPLETE SECURITY ASSESSMENT DETECTS VULNERABILITIES** & ALLOWS FOR **REMEDIATION OF CRITICAL FINDINGS**

Enterprise Integration's SecOps team found a Critical vulnerability with the TLS Protocol Session Renegotiation. The TLS protocol, and the SSL protocol version 3.0 and possibly earlier, did not properly associate renegotiation handshakes with an existing connection. By allowing "man-in-the-middle attacks," a hacker would be able to see the system traffic and potentially grab sensitive information such as usernames and passwords.

Another major vulnerability involved the lack of patch maintenance. The SecOps group determined that critical patches for Windows Server 2003, 2008, 2008 R2, 2012 and 2012 R2 as well as desktop systems Windows, Vista, 7, 8 and 8.1 were missing, exposing the client's environment to multiple vulnerabilities that could result in a serious breach.

Additionally, Citrix Netscaler with firmware version 10.5 or higher had the "enable secure renegotiation" setting enabled by default which exposed client communication to eavesdropping or interception. Security Operations directed the IT team to configure the "Deny SSL Renegotiation" section to "YES" to remediate the vulnerability.considered serious (Figure 5) and could be mitigated by applying strategic changes to specific security controls followed by enhanced monitoring.

THE HIDDEN COSTS OF SECURITY VULNERABILITIES

Gartner states that a large percent of all vulnerabilities are in place prior to production, therefore, having a vulnerability assessment of systems can save company millions both in remediation cost as well as fines and penalties. Per United States Computer Readiness Team (CERT), 95% of attacks are from known vulnerabilities and five malware events occur every second.

The average cost of a data breach is over $3 million. Further broken down, having an incident due to insider threat could cause damages between $200,000 and $300,000 per incident. A company that is not current on software patches and allows a hacker to obtain information through backdoors or security gaps faces losses of almost $500,000 per incident. The longer a data breach goes unnoticed, the higher the price to remediate the incident. On average, it takes over 190 days to find a data breach and over 60 days to contain it. After the breach, the cost to fix the issue is substantial. Depending on the number of records compromised, the amount can range from $2 million to $6 million.

IF THESE VULNERABILITIES HAD BEEN EXPLOITED, THE COSTS TO THE COMPANY COULD HAVE BEEN UP TO $6 MILLION DEPENDING ON THE NATURE OF THE BREACH.

Vulnerabilities found for this company included TLS Protocol Session Renegotiation where system traffic including user names and passwords would be visible. Additionally, the company had no patch maintenance schedule which led to out of date software, again, a common but costly vulnerability. If these vulnerabilities had been exploited, the costs to the company could have been up to $6 million dollars depending the nature of the breach. The exposure of usernames and passwords from the TLS vulnerability would have left them vulnerable to large scale system compromise and data exfiltration. This could have resulted in huge regulatory fines and penalties in addition to the cost of remediation. By investing in a vulnerability management product and having a qualified team do an assessment, the company protected their data saved millions in fines.

TERMS FOR REVIEWING GRAPHS AND SEVERITY SCALES

Though all security vulnerabilities constitute a potential risk to organizations, assessment findings have a range and require attention based on their level. The following list of terms details what action should be taken based on the type of vulnerability.

TYPE	DESCRIPTION	EXAMPLE
URGENT	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security.	May include full read and write access to files, remote execution of commands, and the presence of backdoors.
CRITICAL	Intruders can possibly gain controls of the host, or there may be potential leaked of highly sensitive information.	May include full read access to files, potential backdoors, or a listing of all the users on the host.
POTENTIALLY URGENT	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security.	Includes full read and write access to files, remote execution of commands, and the presence of backdoors
POTENTIALLY CRITICAL	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may potential leakage of highly sensitive information.	Includes backdoors, or a listing of all the users on the host.
SERIOUS	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders.	May include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
MEDIUM	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed.	Intruders can easily exploit known vulnerabilities specific to software versions.
MINIMAL	Intruders can collect information about the host	May utilize open ports, services to find additional vulnerabilities

REFERENCES

Analyze Vulnerabilities, Threats, Cost and Risk to Determine
How Secure Your Application Should Be. (July 18, 2006).
https://www.gartner.com/doc/494253/analyze-vulnerabilities-threats-cost-risk