Whitepaper:

SANS 20 Critical Security Controls

A guide to implementing
SANS 20 Critical Security
Controls using Unified VRM.

The SANS 20 Security Controls are prioritized mitigation steps published by the Center for Strategic International Studies (CSIS) to improve cyber security. The information in this whitepaper is intended for a technical reader and should help you understand each control, and how features in Unified VRM map to the respective control. You will read advanced-level content created by IT security engineers with hands-on experience in IT security and vulnerability management. By the end of this document you should understand the benefits of vulnerability management and be confident about the next steps to make your organization's IT infrastructure and applications more secure.

Enjoy!

A publication of NOPSEC

ABOUT NOPSEC

Unified Vulnerability Management

NopSec was founded to pursue a vision: IT security and effective vulnerability management can be a business advantage. NopSec is a technology company focused on helping businesses to proactively manage security vulnerability risks and protect their IT environment from security breaches.

For many companies, keeping on top of IT security is a real tough job. Vulnerability discovery, analysis, and filtering processes can be lengthy, cumbersome, error prone and involve many manual tasks. Penetration testing is often the first step toward implementing an ongoing and proactive process to address vulnerability management.

Our flagship software-as-a-service, Unified VRM, enables vulnerability management for applications and infrastructure that reside on premises and in the cloud. Unified VRM takes a holistic approach to finding, filtering, and fixing exploitable vulnerabilities. Our customers dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation. Streamlined reporting allows senior management to see progress being made against vulnerability risks on an ongoing basis. And our customers can help avoid potential financial losses and damage to their public reputation associated with a security breach.

At NopSec we love what we do and we are passionate about keeping your company secure.

Video Overview

Request a Demo

Share this Guide

Tweet Share +1

CONTENTS:

Introduction to the SANS Critical Security Controls

What are the SANS Critical Security Controls?

SANS is an organization dedicated to information security training and security certification. The Critical Security Controls effort focuses on prioritizing security controls that have demonstrated real world effectiveness. Standardization and automation is another top priority, to gain operational efficiencies while also improving effectiveness. You can read "A Brief History Of The 20 Critical Security Controls" and "20 Critical Security Controls - Version 4.1" using the links provided.

According to SANS, "*The US State Department has previously demonstrated more than 94% reduction in measured security risk through the rigorous automation and measurement of the Top 20 Controls.*"

In the remainder of this paper, we will outline each of the 20 controls and perform a mapping to the features and functionality in Unified VRM. In some instances, critical controls will be grouped together and we will note cases where a specific critical control may not be applicable. You will see that many actions can be automated through vulnerability risk management which will result in compliance at dramatically reduced costs. And as noted in the quote from the US State Department above, your organization is likely to achieve a significant reduction in IT security risk!

Achieving the SANS Critical Security Controls

Critical Control 1: Inventory of Authorized and Unauthorized Devices

Cyber-attackers target organizations by continuously scanning address spaces waiting for new and unprotected systems to be attached to the network. When talking about vulnerability management, it is important to define what to needs to be protected. Control 1 suggests, "*Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s)*". Believe it or not, organizations commonly do not know the answers to basic questions about how many assets they have under protection.

How does Unified VRM make it easy to take an inventory of authorized and unauthorized devices in your networks?

Inventory discovery is achieved by entering asset ranges in the backend of Unified VRM to have as much control as possible of the assets under assessment. We include IP address ranges, to be comprehensive in our detection, regardless of whether the assets are live or not.

Once a network scan is completed, Unified VRM will provide detailed information including OS fingerprinting, asset fingerprinting, open ports and the latest risk score.

A way to inventory live assets that lie outside of an IP address range is to ping-scan a network to detect responding live hosts. Unified VRM works with the de-facto standard in network mapping, the nmap network scanner. Prior to launching a network scan, the scan configuration template can be modified so that:

1. For external scans, ICMP ping-scan is disabled, since it would only be deflected by the external firewall.

2. For internal scans, ping-scan can be enabled with ICMP, TCP ping-scan, and ARP scan. Also in the nmap configuration, OS fingerprinting, Service Fingerprinting and RPC scan can also be enabled.

3. For web applications the same can be done by doing TCP applicative ping against port 80 and 443.

4. For wireless networks, Unified VRM performs a wireless network site survey detecting company-owned access points and rogue access points.

SANS Critical Control 2: Inventory of Authorized and Unauthorized Software

Most of targeted attacks to enterprises are carried out using a combination of social engineering, phishing emails and software vulnerabilities - Java, Adobe Flash and Acrobat, Firefox and Chrome plugins, 0-day client-side / browser vulnerabilities. These attacks are particularly insidious to prevent because of the proliferation of authorized and authorized software and software versions in the enterprise.

Control 2 suggests to, "*Perform regular scanning for authorized and unauthorized software and generate alerts when it is discovered on a system. A strict change-control process should also be implemented to control any changes or installation of software to any systems on the network.*" Obviously, mapping all authorized and unauthorized software across the enterprise servers and workstations can represent a daunting challenge.

How does Unified VRM help take an inventory of authorized and unauthorized software?

Software discovery is achieved by performing an authenticated scan of the entire enterprise by building a customized scan template selecting the "CPE-based inventory". (CPE provides a unique identifier for software products with a known vulnerability.) This scan template will log into every target host - providing appropriate domain admin credentials - and it will list all the software and related versions installed in the host. The result is a comprehensive inventory of installed software and related versions in all target network hosts.

Unified VRM also implements the concept of a CPE-based policy check. A configuration template can be used to match the enterprise authorized software policies, listing all authorized software and related versions. Through a configuration scan targeting all the hosts in an organization, unauthorized software will be flagged as policy violations. These exceptions can be then analyzed and remediated via Unified VRM’s automatic ticketing capabilities.

SANS Critical Control 3: Secure Configurations

Establishing, securing, enforcing and assessing a secure operating system configuration is one of the most important security controls to prevent targeted cyber-attacks and widespread malware infections. Vulnerabilities can occur when default configurations are not hardened for security, or software patches are not applied in a timely manner.

Control 3 suggests, "*Workstations, laptops, servers, and mobile devices' secure configurations should be established and reviewed using a configuration review scanner via authenticated scans*" and "*A file integrity checker that make sure that the original key files in important hosts' operating systems are not modified by kackers, trojans or other malware.*"

How does Unified VRM help implement security controls?

Configuration of security controls is achieved by running authenticated security scans against specific asset groups to make sure that their operating system configuration is in line with secure configuration standards, such as NSA, DISA, and compliance configuration standards, such as HIPAA, SOX, and PCI-DSS. The customer can also modify the applicable configuration standard he would like to use as baseline according to its secure-built configuration standards. Furthermore, Unified VRM can use the SCAP XCCDF standard to check every operating system for configuration based on corresponding operating system based OVAL definitions.

Unified VRM enables a specially-crafted scan template that can interact with Security Local Audit Daemon (SLAD), installed locally on strategic hosts. This daemon can interact and transmit the status of Tripwire's File Integrity Monitoring. This way key files within the file system can be monitored for unauthorized modification which might indicate a system compromise by a trojan, rootkit or other forms of malware.

SANS Critical Control 4: Continuous Vulnerability Assessment and Remediation

Many organizations are performing a vulnerability scan every quarter or a full penetration testing once a year. While this may meet the minimum bar for regulatory compliance, it creates some significant exposure during the periods in between tests.

Control 4 outlines the following essential steps:

1. Vulnerability intelligence service provides inputs to vulnerability scanner
2. Vulnerability scanners scan production systems
3. Vulnerability scanners report detected vulnerabilities to a vulnerability management system (VMS)
4. The VMS compares production systems to configuration baselines
5. The VMS sends information to log management correlation system
6. The VMS produces reports for management
7. A patch management system applies software updates to production systems.

How does Unified VRM address continuous vulnerability assessment and remediation?

Vulnerability scans can be performed on-demand against all core infrastructure, including wired and wireless networks and web applications. The scanning engines are production-safe, as they automatically adjust performance if they sense reduced response times from target hosts.

Vulnerability detection signatures in Unified VRM are continuously tested for quality assurance by a team of security experts at NopSec. Vulnerabilities are verified by our patent-pending artificial intelligence engine, that also prioritizes the vulnerabilities based on their impacts on the organization's infrastructure and applications.

Unified VRM tests and rates critical hosts' security configurations against best practices and compliance configuration standards. Results can be filtered and measured against key metrics and against custom-established meta-tags. Reports can easily be generated for management, auditors and technical decision-makers.

Unified VRM interacts with several commercial and open source patch management (Microsoft, Puppet) and trouble ticketing systems (Jira, Remedy) through its RESTful authenticated interface. Unified VRM also helps generate Web Application Firewall blocking and logging rules to temporarily block discovered web application vulnerabilities.

SANS Critical Control 5: Malware Defenses

Targeted hacking attacks and malware of increasing sophistication is on the rise. Botnets, trojans and exploit kits are making their round on a weekly basis continuously being updated with the latest 0-day exploits. Anti-virus companies are playing catch-up trying to update their products with the latest malware signatures. While Unified VRM is not an anti-malware or a malware detection solution, appropriately configured through a specially crafted scan template, it can interact with tools that help in malware detection.

Unified VRM Internal scan engine has an authenticated vulnerability check that logs into target systems and scans for signs of malware compromise, detecting the most famous malware including Blackhole exploit kit and Zeus trojan. In addition, Unified VRM can interact with the remote agent SLAD installed in target systems. SLAD can execute and interact with a series of malware detection and prevention tools.

Unified VRM can collect snort IDS logs from the target system, gathering evidence of malware infection. It can interact, run and collect logs from Tripwire from the target system to perform file and file system integrity checking to detect signs of malware compromises. Unified VRM can run and collect logs from the open source antivirus CLAMAV installed on the target system. Like Snort, CLAMAV has a huge community of open source developers that write open source malware detection signatures. Chkrootkit is a tool used to detect the compromise of the system by most common rootkits and trojans. Unified VRM can run and collect logs from the open source tool "chkrootkit" installed on the target system.

SANS Critical Control 6: Application Software Security

Another very important area of an organization's security program is its application security roadmap. Web and mobile applications can often be the weakest link in the security chain. Implementing security controls early on in the System Development Life Cycle (SDLC) requires investments in secure coding for developers. However, addressing issues early in the process is often a less costly option than dealing with serious flaws after-the-fact. Both internally developed and third-party application software should be tested to find security flaws.

An ongoing security vulnerability management program for web and mobile applications is required to prevent pervasive attacks such SQL injections, Cross-Site Scripting, Remote Command injections, and Cross-Site Request Forgeries, to name only a few.

Control 6 suggests, "*Web application firewalls protect connections to internal web applications; Software applications securely connect to database systems; Code analysis and vulnerability scanning tools scan application systems and database systems.*"

How does Unified VRM help with application software security?

Unified VRM achieves application security by mapping, spidering and testing web and mobile applications for OWASP Top 10 Vulnerabilities. The spidering and the fault injection phases are used to find vulnerabilities in sophisticated web applications. Unified VRM also performs manual spidering of the web applications using an on-demand proxy collecting injection points that are then used for injection later on in the process. Unified VRM has an auto-sensing technology capable of detecting login forms and session tokens in order to maintain the authenticated status in sophisticated web applications.

Unified VRM is capable of generating on-the-fly rules for a number of Web Application Firewalls (WAF) providing a virtual patching capability able to block attacks while developers work on fixes. Providing web application, web server and operating system vulnerability management and penetration testing capabilities, Unified VRM is able to correlate vulnerabilities at the application, operating system and database level providing full visibility to the web application stack in terms of security threat vectors. Unified VRM allows provide proof-of-concept exploitation for SQL injections, Command Execution and Directory Transversal.

SANS Critical Control 7: Wireless Device Control

Wireless networks have always been a "no man's land" in terms of security and configuration. Some of the most notorious security breaches happened because the security configuration of the enterprise wireless access points was not secure. Furthermore, from the security architecture standpoint, if the wireless network is located logically within the internal corporate network, a security breach of the wireless network could represent an incident with profound consequences for business continuity.

Another growing challenge is the Bring-Your-Own-Device (BYOD) trend. Personal electronic devices are brought to work (iPad, Andriod tablets, etc.) and connected to the wireless internal network, so if one of these devices is compromised the path to the core of the enterprise goes right through its wireless network.

Control 7 speaks about wireless network logical architecture and configuration. It outlines scenarios that should be tested including, wireless clients and access points with an unauthorized service set identifier configured on it, improper encryption, improper authentication, and completely rogue wireless access points.

How does Unified VRM help with wireless device control?

Wireless probes are placed in the enterprise and communicate with Unified VRM via VPN tunnels. It covers core tests such a s performing a wireless network site survey, detecting neighboring access points, as well as determining authorized access points and rogue access points.

Unified VRM tests the strength of encryption keys for WEP, WPA and WPA2 protocols. The cracking attempts are perform using first a dictionary attack and then a brute force attack. Wireless connected devices are checked for security vulnerabilities and penetration testing over wireless networks determine if it is possible to start mapping and to escalate privileges over hosts connected to the internal wired network.

In the man-in-the-middle attack mode, the wireless agent acts as a rogue access point responding to all the wireless clients’ request for connection. Once the client connects, the agent is able to sniff traffic and credentials from the unaware client.

SANS Critical Control 8 and 9: Data Recovery Capability & Security Skill Assessment

Control 8 refers to an organization's data recovery capability, the availability component of security that might come into play after a security breach occurred and the organization needs to restore its systems to their previous state.

Control 9 refers to an organization's on-going security training and security skill improvement. Security skill improvement is key in an organization that is serious at fighting the latest and greatest security threat as the attackers get more and more technically sophisticated.

How does Unified VRM help with data recovery?

Scan templates can be configured to find and report backup agents installed in the remote hosts. This is to make sure that the hosts containing key information are appropriately backed up when needed. The templates can be configured to find and report critical and confidential information, including credit card numbers and social security numbers so that they are appropriately backed up periodically.

How does Unified VRM help with security skill assessment?

Unified VRM helps this process by automating one of the most challenging parts of vulnerability management – evaluating the risk ranking of vulnerabilities. Unified VRM augments the organization’s vulnerability management skills by analyzing each discovered vulnerability against the following criteria:

- Is the reported vulnerability a false positive?
- Is the reported vulnerability really exploitable?
- Is the vulnerability reported with the correct risk rating?
- Is the vulnerability reported really a vulnerability or another piece of information posing no critical risk to the organization?

This can reduce the time investment on burdensome and redundant tasks such as manual tracking and reporting, and help the security team focus efforts on more strategic activities.

SANS Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Routers, switches and firewalls represent the backbone of an organization's network and cannot be left unconfigured or with insufficent security controls. Access exceptions are sometimes deployed and problems arise when exceptions are not reversed when the business need is no longer applicable.

Control 10 mentions testing network devices for, "*hardened device configurations, and patch management systems properly updating to production network devices*." It goes on to recommend, "*Two-factor authentication system required for administrative access to production devices and proxy/firewall/network monitoring systems analyze all connections to production network devices.*"

How does Unified VRM help secure configurations for network devices?

Unified VRM is capable of testing the external firewall for misconfigurations and open ports. Also, if the firewall brand and version has a particular reported vulnerability in both network and web application front-ends, these vulnerabilities will be discovered.

On routers and switches, Unified VRM will find default passwords, default SNMP community strings and other misconfigurations so that they can be corrected. Internal network scan and authenticated OVAL scan with SSH can be used to find classified vulnerabilities in firewall, routers, and switches. Unified VRM can also test Cisco routers, switches and firewalls based on the latest XCCDF definitions. Firewall, routers and switches hardened configurations can be customized and the targets tested through the Unified VRM.

Unified VRM can test whether the wireless network is logically located outside or inside the firewall. If there are any exploitable vulnerabilities found, Unified VRM can help in building a proof-of-concept exploitation targeted to routers, firewalls and switches.

For change control, Tripwire can be deployed on most of the firewall and it can monitor the file system for unauthorized changes. Tripwire can be then interfaced with Unified VRM to collect those unauthorized change logs periodically.

SANS Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services

Ports, protocols and services are entry points and mechanisms into a target network or system. Default installations, misconfigurations, and unauthorized services result in increased exposure. Common examples are poorly configured web servers, mail servers, file and print services, and domain name system (DNS) servers. Attackers are always on the lookout for such avenues in order to gain access to the target network or system.

Control 11 talks about tracking, controlling and limiting the use of network ports, protocols and services with the intention of reducing the attack surface. Specifically it mentions, "*scanner analyzes production systems for unauthorized ports, protocols, and services; System baselines regularly updated based on necessary/required services; Active scanner validates which ports, protocols, and services are blocked or allowed by the application firewall*"

How does Unified VRM help with ports, protocols, and services?

Unified VRM detects, aggregates and reports risks in a prioritized fashion for internal and external networks respectively. Unified VRM includes an active scanner that interacts with the target system in order to identify open ports, supported protocols and services running. Unauthorized ports, protocols or services can be disabled or uninstalled and tested by performing a rescan.

Unified VRM can be leveraged to test the application firewall's implementation. The scanner can be used to verify if the application firewall is able to block all traffic except those directed towards authorized ports and services, and generate an alert.

Host-based firewalls are implemented in addition to application firewalls to maintain a defense-in-depth strategy. Unified VRM can be directed towards business systems to identify unauthorized ports, protocols and services in the presence of a host-based firewall.

SANS Critical Control 12: Controlled Use of Administrative Privileges

In a system there is no privilege that is higher than administrator privilege. In Unix and Linux, this is often referred as having "root" privileges with UID 0. In Windows, this is referred as having "local Admin" or "Domain Admin" privileges. Systems can be compromised when a privileged user is fooled into opening a malicious e-mail attachment, downloading and opening a file from a malicious website, or simply surfing to a website hosting attacker content that can automatically exploit browsers. Another common way to obtain administrative credentials is elevation of privileges by guessing or cracking a password. If administrative privileges are prevalent, the attacker may be able to gain full control of systems.

Control 12 deals with, "*The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*"

How does Unified VRM help control use of administrative privileges?

Best-practice configuration baselines can be tested on key infrastructure servers, including Domain Controllers, Active Directory Servers, DNS Servers, DHCP servers and more to make sure that the Group Policy is appropriately applied. This will limit the administrative privileges to only a few custom accounts and willl scan systems for password files modifications which might indicate a host compromise.

Unified VRM will ensure that appropriate password policies are enforced in terms of length, complexity and change period requirements. Scan templates can be configured to test the strength of passwords for particular privileged accounts, including root via SSH and the infamous account "Administrator" which should be disabled in production environments.

Unified VRM will allow for the detection of usage of default privileged accounts, including the MS SQL Server "sa" account, which might be un-passworded or having an easily guessable password. Another option will test the strength of web applications administrative front-end password.

SANS Critical Control 13: Boundary Defense

Boundary defenses define those security controls aimed at protecting and segregating various networks with different degrees of trust. Typical examples of those defenses are firewalls, intrusion detection and prevention systems, web content filtering, network access controls, routers/switches, and proxy servers. Attackers attempt to establish a foothold on perimeter systems and, with a base of operations on these machines, move deeper inside the boundary for attacks against internal hosts.

Control 13 outlines the following steps:

1. Hardened device configurations applied to production devices
2. Two-factor authentication systems required for administrative access to production devices
3. Production network devices send events to log management and correlation system
4. Network monitoring system analyzes network traffic
5. Network monitoring system sends events to log management and correlation system
6. Outbound traffic passes through and is examined by network proxy devices
7. Network systems scanned for potential weaknesses.

How does Unified VRM help address boundary defense?

Unified VRM does not offer defensive security controls capable of blocking ongoing attacks. However, Unified VRM can help detect vulnerabilities and misconfigurations in the security controls mentioned above, thus making those stronger.

XCCDF scanning can help detect security misconfigurations in Cisco devices (firewall, routers, and switches), Solaris and various other flavors of Linux and Unix. Unified VRM can test the strength of passwords in various remote daemons (SSH, Remote Desktop, etc.) to prove the need for dual factor authentication. Unified VRM finds vulnerabilities in web applications and application proxies which might allow an attacker to escalate attack privileges.

SANS Critical Controls 14 and 15: Audit Logs and Controlled Access

Control 14 refers to audit logs for firewall, network devices, servers and hosts are most of the time the only way to determine whether or not the host has been compromised. The logs need to be aggregated, safeguarded and correlated with other relevant security events.

Control 15 deals with controlling access to data from people with the appropriate need to know. Information needs to be classified in terms of sensitivity and importance for the business. Sensitive information needs to be segregated in separate VLANs with appropriate firewall controls. File servers need to be appropriately protected and configured. Logging of those file servers operations should be maintained and information that needs to be transmitted off to public networks needs to be encrypted. Data Leak Preventions and ACLs need to be maintained to prevent sensitive information from being transmitted outside the organization.

How does Unified VRM help with audit logs and controlled access?

Unified VRM is not a log aggregation solution. However, relevant and verified vulnerability information can be exported into log aggregation systems and Security Information and Event Management (SIEM) systems to enable the correlation with intrusion detection and other log data.

Unified VRM can be used to verify that file servers are appropriately patched and configured according to best practice industry standards. Furthermore, Unified VRM can help verify that firewall rules are appropriately implemented and networks are appropriately segregated via VLAN. Active Directory group policies application can be verified via Unified VRM by performing authenticated vulnerability scans.

SANS Critical Control 16: Account Monitoring and Control

Protecting privileged user and administrative accounts is very important to prevent widespread intrusions. Domain administrator accounts, default administrative accounts, guest accounts, and contractors' accounts needs to be protected with appropriate passwords and monitored for appropriate use. Dormant accounts needs to be disabled after a reasonable amount of time and default administrative accounts need to be renamed. Attackers can exploit legitimate but inactive user accounts to impersonate legitimate users and avoid detection.

Control 16 deals with protection and monitoring of privileged user accounts and with the domain group policies to appropriately protect and monitor such accounts.

How does Unified VRM help with account monitoring and control?

Unified VRM, with its authenticated scan capabilities, helps determine the target host group policies in terms of default account enablement, no or easily guessable password on default account, password expiration, account lockout policy, policy on password renewal, and activity logging and auditing. This can be accomplished with both the standard network scanner as well as with the OVAL scanning capabilities. Authenticated standard scan and XCCDF capabilities enable the administrator to review target host configurations against best practices standards, such as XCCDF, NIST, compliance standards, and more.

Unified VRM can also help auditing password strength against various dictionary sizes, especially for the administrative privilege accounts which might allow an attacker to mount a widespread attack over the entire internal network.

SANS Critical Controls 17, 18 and 19: Data Loss Prevention, Incident Response and Management, Secure Network Engineering

Data Loss Prevention control has jumped on most organizations' CISOs' radar screens because of the recent whistle-blowing revelations in the press. It is paramount for every organization to prevent leakage by employees of confidential information to the outside world. Most of the work for setting up this control involves cataloging corporate information in various categories based on sensitivity and importance for the organization. Once the information classification is in place, access controls as discussed in control 15 need to be implemented. Moreover, a data leakage prevention technical control needs to be set up at the gateway so sensitive information is not released to the outside world.

How does Unified VRM help data loss prevention and incident response?

Unified VRM can help in this process with a customized scan template to identify confidential and sensitive information such as credit card information and social security numbers. The same thing can be accomplished for web applications. Both methods mentioned work with or without credentials.

No intrusion detection, prevention or SIEM system can substitute for a well-structured incident response procedure. Unified VRM can help in mimicking the most advanced penetration testing techniques which are instrumental in testing security incident response procedures. A well-structured vulnerability management and penetration testing process can help formalize the incident response procedures to meet the organizations' business goals.

Security controls alone cannot prevent advanced intrusion techniques without a robust architecture of the organization's wired, wireless, and mobile networks. Unified VRM can help test network infrastructure, firewalls, web applications, application gateways, SOCKS proxies, and RADIUS servers against security misconfigurations and vulnerabilities. Also, Unified VRM can mimic exploitation techniques on wired and wireless networks as the ultimate test of appropriate network security architectures.

SANS Critical Control 20: Penetration Tests and Red Team Exercises

Attackers compromise systems through any number of techniques discussed earlier in this document. Control 20 defines, “*Penetration testing involves mimicking the actions of computer attackers to identify vulnerabilities in a target organization, and exploiting them to determine what kind of access an attacker can gain. Penetration tests typically provide a deeper analysis of security flaws than a vulnerability assessment*." The common approach is through social engineering and by exploiting vulnerable software and hardware.

Penetration testing is a monitoring control, which periodically checks the efficiency of the vulnerability management process. If vulnerability management is done right, penetration testing should turn out to be a "blank report". Vulnerability management, by contrast, is a continuous control aimed at managing information assets, detecting and analyzing vulnerabilities, and prioritizing and applying fixes.

Red teaming is more comprehensive than penetration and aimed at testing the organization's security emergency response procedures and preparedness. According to SANS: "*The goals of red team exercises are to improve organizational readiness, improve training for defensive practitioners, and inspect current performance levels*."

In terms of compliance, penetration testing engagements are a requirement for organizations that would like to be compliant with the following regulations: PCI standards - Standard 11.3, SOX, HIPAA, GLBA and other banking regulations.

How does Unified VRM address penetration tests?

NopSec has been performing manual penetration testing engagements for various asset classes, including external, internal, wireless, web and mobile applications, social engineering, VoIP, etc. since 2008. Unified VRM grew out of our experience performing penetration tests and, as a result, covers the same asset classes you would expect from a human-powered test or real attack.

Unified VRM automates the process of vulnerability verification, prioritization and false positive elimination. This means no need to perform extra analysis and work on hundreds of pages of a vulnerability report. Attackers and penetration testers perform their attacks across the enterprise assets including networks, web applications, and other attack vectors.

Unified VRM offers a proof-of-concept exploitation framework capable of showing that the identified vulnerabilities are indeed exploitable to take control of the targeted hosts. An extensive database of publicly available exploits is matched with the discovered vulnerabilities based on Common Vulnerabilities and Exposures (CVE). The exploitation can also be extended to the wireless network after a site survey has been performed and a target access point's encrypted key has been discovered.

SANS Critical Security Controls Recommendations

How should you prepare for implementing the SANS Critical Security Controls?

You should have a plan for implementing the SANS Critical Security Controls. It can be a significant undertaking in terms of time and resources. It is not necessary to approach all controls at the same time, and it can be effective to prioritize and address areas that are the greatest risk for your specific organization. Regardless of where you start, vulnerability management is a commitment to decreasing the risk of a security breach and ensuring compliance with your company security policies. It is an assurance to your company, your partners and your customers.

You need to gain the support and commitment to implementing security controls from company leadership, since this undertaking will require the diligence and participation of employees across all areas of the business.

Depending on how you choose to implement a security controls, it may require IT staff to assist with deployment. It is vital that everyday operations of your organization will not be disrupted in the implementation of the process. In the case of vulnerability management, management it should be considered an ongoing effort; so ensure that your time and resources are budgeted appropriately.

How should you select a provider to assist you?

Your choice needs to incorporate your budget and resource considerations. Because you are protecting your organization's most valuable assets from security breaches, you will want to select a vendor that balances a solid track record of performance with cutting-edge security innovations.

You should seek out a provider that understands the unique needs of your IT environment and has the flexibility to deliver a customized solution. With efficient and effective remediation being the end goal, having a provider that integrates well with your existing security and management tools should be a strong consideration.

You should consider asking the provider for a list of references from organizations with a similar profile to yours. You may also ask the vendor for examples of similar projects they have undertaken in the past. There are common accreditations in the IT security industry and you can ask to confirm the credentials and experience of the individuals who will oversee the vulnerability management services for your company.

Get started today!

You are ready to take the next step to toward less risk and a more secure IT environment for your organization! If you think we may have missed something in the whitepaper or you need additional clarification, please do not hesitate to reach out to our security specialists. The controls described in this paper are better seen than read, and we would be happy to provide a personalized demo of how Unified VRM can help you proactively manage IT security.

GET STARTED WITH NOPSEC

Contact us to schedule an initial consultation
(646) 502-7900
questions@nopsec.com.

A publication of NOPSEC