RAPID7

The SANS Institute
Top 20 Critical Security Controls

Compliance Guide

February 2014

The Need for a Risk-Based Approach

A common factor across many recent security breaches is that the targeted enterprise was compliant, meaning they passed their Payment Card Industry (PCI) audit yet customer data was still compromised. Simply being compliant is not enough to mitigate probable attacks and protect critical information. In today's constantly evolving threat landscape, organizations need to focus on securing the business first and documenting the process to show compliance second, not the other way around. While there's no silver bullet, organizations can reduce chances of compromise by moving from a compliance-driven to a risk management approach to security.

What are the SANS Top 20 Critical Security Controls?

In 2008, the SANS Institute, a research and education organization for security professionals, developed the Top 20 Critical Security Controls (CSCs) to address the need for a risk-based approach to security. Prior to this, security standards and requirements frameworks were predominantly compliance-based, with little relevance to the real-world threats they are intended to address. The Top 20 Controls are prioritized to help organizations focus security efforts to have the greatest impact in improving their risk posture. According to the US State Department, organizations can achieve more than 94% risk reduction through rigorous automation and measurement of the Top 20 Controls.

Top 20 Controls' Two Guiding Principles

"Prevention is ideal but detection is a must"

While controls that defend networks and systems against attacks are essential, the Top 20 Controls also recommends controls that detect and thwart attackers inside a network that has already been compromised. Through fast detection of compromised machines, organizations can prevent follow-on attack activities that would have otherwise resulted in financial and reputational losses. Rapid7 UserInsight was developed to address this very need – to detect compromised users and unauthorized access quickly and effectively, thereby minimize damage from attacks.

"Offense informs defense"

The Top 20 Controls is a consensus list developed by experts with deep knowledge of actual attacks, current threats and effective defensive techniques. This ensures that only controls that can be shown to detect, prevent and mitigate known real-world attacks are included. Leveraging over 200,000 open source community members and industry-leading security researchers, Rapid7 has integrated its deep understanding of the threat landscape and attacker methodologies across its product portfolio to deliver security solutions that are effective against real-world threats.

How Rapid7 can help

Rapid7 security solutions help thwart real-world attacks by helping organizations apply the SANS Top 20 Critical Security Controls. The table below outlines how Rapid7 products align to the SANS Top 20 Critical Security Controls.

	Critical Security Control	Nexpose	Metasploit	Mobilisafe	ControlsInsight	UserInsight
1	Inventory of Authorized and Unauthorized Devices	✓		✓		
2	Inventory of Authorized and Unauthorized Software	✓		✓		
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	✓		✓		✓
4	Continuous Vulnerability Assessment and Remediation	✓		✓	✓	
5	Malware Defenses				✓	
6	Application Software Security	✓	✓			
7	Wireless Device Control	✓		✓		✓
8	Data Recovery Capability					
9	Security Skills Assessment and Appropriate Training to Fill Gaps		✓			
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	✓	✓			
11	Limitation and Control of Network Ports, Protocols, and Services	✓			✓	
12	Controlled Use of Administrative Privileges	✓	✓		✓	✓
13	Boundary Defense				✓	✓
14	Maintenance, Monitoring, and Analysis of Audit Logs					✓
15	Controlled Access Based on the Need to Know					
16	Account Monitoring and Control	✓		✓	✓	✓
17	Data Loss Prevention				✓	✓
18	Incident Response and Management					✓
19	Secure Network Engineering		✓			
20	Penetration Tests and Red Team Exercises	✓	✓			

RAPID7

SANS Top 20 and Rapid7 Solutions: In Detail

Control	Rapid7 Solutions
CSC-1 **Inventory of Authorized and Unauthorized Devices**	Nexpose: • Enables administrators to build and manage an asset inventory by performing either manual or scheduled discovery scans. • Automates the task of asset discovery and identification by scanning the entire infrastructure for all networked devices. • Assembles an inventory of every system that has an IP address on the network, including databases, desktops, laptops, servers, subnets, network equipment (routers, switches, firewalls, etc.), printers, Storage Area Networks, and Voice-over-IP (VoIP) phones. • Enables administrators to configure asset scanning and reporting using sites and asset groups based on specific criteria such as device type, software type, operating system type, or geographic location. • Provides fully customizable policy scanning to determine presence of unauthorized devices in accordance with policies for whitelisting authorized devices and blacklisting unauthorized devices. • Catalogs all devices in Nexpose as it scans and automatically sends alerts to administrators about any deviations from the expected inventory of assets on the network. Mobilisafe: • Catalogs all mobile devices accessing the corporate network.

Control	Rapid7 Solutions
CSC-2 **Inventory of Authorized and Unauthorized Software**	Nexpose: • Automates the task of assembling an inventory of software installed on every system that has an IP address by scanning the entire IT infrastructure. • Enables you to track type and version of operating system and applications installed on each system, including versions and patch levels, and create and automatically distribute reports for remediating vulnerabilities. • Provides fully customizable policy scanning to determine presence of unauthorized software and services in accordance with policies for whitelisting authorized software and blacklisting unauthorized software. • Catalogs all software as it scans, including any malicious software, by using the latest fingerprinting technologies to identify systems, services, and installed applications. Mobilisafe: • Catalogs all applications installed on mobile devices accessing the corporate network, including its version number and whether it was found in the official OS app stores. • Enables you to define unauthorized mobile applications and block devices that have a blacklisted application installed from access to the corporate network.

Control	Rapid7 Solutions
CSC-3 **Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers**	Nexpose: • Automates the task of measuring compliance of systems with corporate or regulatory policies for secure configurations such as PCI, HIPPAA, NERC or FISMA. • Provides ability to centrally manage and modify secure configuration policies using the Security Content Automation Protocol (SCAP) framework. • Provides flexible, customizable policy scanning to detect misconfigurations and identify missing patches on servers, workstations, web applications, and databases. • Enables you to validate and report on adherence to configuration policies within the asset inventory by performing either manual or scheduled policy compliance scans. Mobilisafe: • Enables you to define and deploy policies based on device attributes, vulnerability severity level and employee profile for all mobile devices accessing the corporate network. • Monitors all mobile devices accessing the corporate network to verify that they meet configuration standards, their operating systems are up-to-date, and those with blacklisted applications installed are blocked from the network. UserInsight: • Enables you to limit administrative privileges by monitoring the network for new administrative accounts, accounts with unnecessary privileges, and disabled accounts that have been re-enabled, and automatically send alerts.

Control	Rapid7 Solutions
CSC-4 **Continuous Vulnerability Assessment and Remediation**	Nexpose: • Enables you to schedule automated scans against all systems on the network to detect, assess and prioritize vulnerabilities and misconfigurations, and create and automatically distribute prioritized remediation plans. • Provides insight into the real risk of an environment by building on the CVSS score to incorporate information on exploits, malware exposure and age of vulnerabilities, and create customizable reports to track effectiveness in reducing risk. • Integrates with best-of-breed SIEM solution to correlate vulnerability scan results with event logs to determine whether an attack was targeted at a vulnerable system. • Provides end-to-end workflow support for exceptions management and policy overrides with automated approval process for accepting reasonable business risk. Mobilisafe: • Continuously monitors mobile devices accessing the corporate network for vulnerabilities, manages the risk over time associated with each device, and automatically sends notifications to users with direct links to update firmware. ControlsInsight: • Scans all workstations, desktops and laptops to verify that operating systems, web browsers and high-risk applications such as Adobe Reader and Flash, Microsoft Office, and Oracle Java are up-to-date with the latest software version.
CSC-5 **Malware Defenses**	ControlsInsight: • Enables you to detect, prevent or control the installation and execution of malicious software by automatically monitoring all workstations to verify that: ○ Anti-malware software is installed, enabled and has received the latest update ○ USB access is blocked ○ E-mail client is configured to block attachments with certain file types such as .exe ○ URL filtering and reputation scanning is enabled ○ Code execution prevention features such as Data Execution Prevention and the Enhanced Mitigation Experience Toolkit (EMET) are deployed

Control	Rapid7 Solutions
CSC-6 Application Software Security	Nexpose: • Provides ability to perform ongoing scheduled and ad hoc scanning of web applications in both test and production environments for cross-site scripting and SQL injection, and enables web form scanning using form-based authentication. • Provides ability to establish baseline configurations for assessing risk exposure after web application changes by checking for security violations in web applications, as well as in underlying database servers, including MS SQL, Oracle, MySQL, and DB2. • Automates the task of scanning all vital systems that web and enterprise applications rely on or systems that are part of critical business processes for vulnerabilities and misconfigurations, and prioritizing these threats for remediation. Metasploit: • Provides ability to audit and exploit web applications for the OWASP Top 10 to demonstrate security risk to application owners and developers.
CSC-7 Wireless Device Control	Nexpose: • Provides ability to scan the entire IT infrastructure for wireless access points connected to the network and determine presence of unauthorized access points. Mobilisafe: • Catalogs all mobile devices accessing the corporate network with detailed information including device name, model, manufacturer and operating system. • Monitors all mobile devices for compliance with configuration policies, operating systems are up-to-date, and no blacklisted applications are installed. UserInsight: • Provides real-time visibility into the number and type of mobile devices connecting to the corporate network or cloud services, including geo-location details.
CSC-9 Security Skills Assessment and Appropriate Training to Fill Gaps	Metasploit: • Allows you to conduct and manage regular phishing campaigns to measure the effectiveness of end-user security awareness training programs.

Control	Rapid7 Solutions
CSC-10 **Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**	Nexpose: • Provides fully customizable scanning to compare the configuration of network devices such as firewall, router and switches with corporate or regulatory policies. • Detects policy violations or misconfigurations of network ports, protocols and services, and provides end-to-end workflow for managing and approving exceptions. Metasploit: • Automates the task of auditing the configuration of firewall egress filtering policies using a security testing module to discover open ports that allow outbound traffic.
CSC-11 **Limitation and Control of Network Ports, Protocols, and Services**	Nexpose: • Provides fully customizable scanning to detect policy violations or misconfigurations of network ports, protocols, and services. ControlsInsight: • Enables you to automatically monitor all workstations to ensure that Windows firewall is enabled and configured correctly.

Control	Rapid7 Solutions
CSC-12 **Controlled Use of Administrative Privileges**	UserInsight • Enables you to limit administrative privileges by monitoring the network for new administrative accounts, accounts with unnecessary privileges, and disabled accounts that have been re-enabled, and automatically send alerts. • Provides visibility of service and user accounts with non-expiring passwords. ControlsInsight: • Monitors all workstations to ensure that a strong administrative password policy is enforced, and passwords are changed on a regular basis. • Detects any shared administrative passwords across all workstations. Nexpose: • Provides fully customizable policy scanning to audit password policies, including number of login attempts, password length, and allowable special characters. • Detects any network devices including routers, firewalls and wireless access points using a default password, and prioritizes for remediation. Metasploit: • Provides ability to audit administrative passwords through online brute-force attacks, offline password cracking, and security testing modules. • Finds shared administrative passwords by testing a single cracked password across the network or simulating a pass-the-hash attack using a raw password hash.
CSC-13 **Boundary Defense**	UserInsight: • Provides ability to track network traffic to malicious sites by manually adding new IPs or domains or automatically source from any threat feeds subscription service. • Monitors and analyzes network, mobile and cloud services traffic by correlating log data from multiple sources including firewall, web proxy and ActiveSync. • Detects network access from multiple geo-locations, potentially indicating malicious or unauthorized access, and automatically sends alerts. ControlsInsight: • Monitors installed browsers on all workstations to ensure that URL filtering and reputation scanning is enabled to limit traffic to known malicious IPs.

Control	Rapid7 Solutions
CSC-14 **Maintenance, Monitoring, and Analysis of Audit Logs**	UserInsight: • Provides visibility of activity across network, mobile and cloud services by aggregating log data from firewalls, web proxies, DNS servers, VPN servers, etc. • Presents a real-time map of user authentication locations to VPN, cloud services and mobile devices including any failed attempts. • Correlates and analyzes log data to detect indicators of compromise and malicious activity using built-in alerting rules based on a proprietary series of attacker behavior analysis, minimizing false positives and required maintenance resources.
CSC-16 **Account Monitoring and Control**	UserInsight • Monitors user account activity and identifies risks such as accounts with unnecessary privileges and accounts with passwords that never expire. • Detects account authentication to corporate provisioned cloud services after the related user's account is disabled in Active Directory. • Presents a real-time map of user authentication locations to VPN, cloud services and mobile devices including attempts to log in from a disabled account. • Detects unusual account usage, including network access from multiple geo-locations and first time access to a critical access, and automatically sends alerts. ControlsInsight: • Monitors all workstations to ensure that a strong local user password policy is enforced, and passwords are changed on a regular basis. Nexpose: • Provides fully customizable policy scanning to audit password policies, including password complexity, length, maximum age, and failed login attempts. Mobilisafe: • Requires that all mobile devices accessing the corporate network have a passcode.
CSC-17 **Data Loss Prevention**	UserInsight • Provides visibility into cloud services usage and, for common corporate provided applications such as Salesforce, Box and Google Apps, monitors the types of files sent to and from the cloud, and alerts on abnormal usage patterns. ControlsInsight: • Monitors all workstations to ensure that USB access is blocked.

Control	Rapid7 Solutions
CSC-18 **Incident Response and Management**	UserInsight: • Provides ability to investigate and respond to incidents quickly by tying incidents, IP addresses and assets to a specific user, and presenting additional context such as the underlying user behaviors and processes running on the endpoint.
CSC-19 **Secure Network Engineering**	Metasploit: • Provides ability to simulate targeted attacks to verify that the network is securely engineered, and systems with sensitive information are not exposed.
CSC-20 **Penetration Tests and Red Team Exercises**	Metasploit: • Automates the task of discovering all hosts and services on the network to target, with the ability to import vulnerability scans from Nexpose. • Allows exploitation of systems using the same methods attackers would use, including VPN pivoting, AV & IPS evasion, and leveraging weak and shared credentials. • Enables you to collect, filter and tag security issues found, and generate reports to share with stakeholders for remediation. • Provides ability to conduct and manage regular social engineering campaigns. Nexpose: • Discovers all assets on the network, identifies vulnerabilities and misconfigurations to guide and focus penetration testing efforts. • Provides ability to filter and report on vulnerabilities validated to be exploitable for prioritized remediation. Professional Services Organization: • Provides access to Rapid7 Penetration Testing Services to evaluate your security controls, perform internal and external testing, perform social engineering, identify gaps in your security program, and provide an actionable remediation plan.

RAPID7

About Rapid7

Rapid7's security solutions deliver visibility and insight that help you make informed decisions, create credible action plans, and monitor progress. They simplify risk management by uniquely combining contextual threat analysis with fast, comprehensive data collection across your users, assets, services and networks, whether on premise, mobile or cloud-based. Rapid7's simple and innovative solutions are used by more than 2,500 enterprises and government agencies in more than 65 countries, while the Company's free products are downloaded more than one million times per year and enhanced by more than 200,000 members of its open source security community. Rapid7 has been recognized as one of the fastest growing security companies by Inc. Magazine and as a "Top Place to Work" by the Boston Globe. Its products are top rated by Gartner® and SC Magazine. For more information about Rapid7, please visit http://www.rapid7.com.