WHITE PAPER: CONSENSUS AUDIT GUIDELINES AND SYMANTEC RAS

Addressing the Consensus Audit Guidelines (CAG) with the Symantec™ Risk Automation Suite (RAS)

Confidence in a connected world.

Addressing the Consensus Audit Guidelines (CAG) with the Symantec™ Risk Automation Suite (RAS)

Contents

Overview 1

Critical controls subject to automated collection, measurement, and validation. 1

Critical controls subject to manual collection, measurement, and validation 5

Conclusion 6

Overview

The Consensus Audit Guidelines are aimed at addressing the most effective countermeasures in cyber- security. A consensus among multiple industry experts, the CAG was developed with the intent to help defend our nation's intelligence and information infrastructures. It reflects 20 key control areas – a list that resulted from the collaborative work of federal CIOs, CISOs, DoD Blue Team members, FBI cybercrime teams, and forensic experts. The CAG is viewed as an effective guide for blocking well-known, high-priority attacks across government infrastructures.

Fifteen of these control areas can be continuously and automatically monitored, which facilitates awareness, analysis, and response through effective product-based solutions. The remaining five areas require governance from a well-established information security program, ideally run in parallel to the automated, continuous monitoring being provided by a technical solution. Overall, each control area encompasses individual sub-controls that provide additional detail on what preventive actions should be implemented in order to advancedefensive efforts in cyber-security.

The CAG is accompanied by three guiding principles used to develop these 20 control areas and their associated sub-controls. These principles are as follows:

- Defenses should focus on addressing the most common and damaging attack activities occurring today, and those anticipated in the near future.
- Defenses should be automated, where possible, and periodically or continuously measured using automated measurement techniques, where feasible.
- To address current attacks occurring on a frequent basis against numerous organizations, a variety of specific technical activities should be undertaken to produce a more consistent defense.

In support of these principles, this document is intended to correlate the many and varied functions of the Symantec Risk Automation Suite (RAS) in successfully addressing and supporting the 20 control areas. The total list of controls can be broken out into those that can be automatically measured (15) as well as those that require manual efforts (5). This document helps place the Symantec Risk Automation Suite in the context of fulfilling the security objectives documented by the CAG across each of the 20 control areas defined. Complementary Symantec products for the enterprise also play a significant role in addressing and/or supporting a specific control area as well.

Critical controls subject to automated collection, measurement, and validation

Control 1: Inventory of Authorized and Unauthorized Devices

- Symantec Risk Automation Suite fulfills one of the principles of our philosophy: Know Your Assets, Know Your Risk. RAS Network and Host Discovery reveals both authorized and unauthorized technology assets with ease. Alerting and remediation tasks can be automated when rogue or unauthorized assets are detected. A robust and easily managed host discovery schedule provides for continuous visibility of both authorized and unauthorized assets.

- Asset Reporting in RAS provides the ability to see various elements or properties related to both authorized and unauthorized host data. With customizable host discovery scans across all endpoints, a thorough inventory of workstations, servers, laptops, and portable media devices is a click away.

Control 2: Inventory of Authorized and Unauthorized Software

- The RAS Configuration Management module allows for insight into installed software across the enterprise, as well as the ability to designate any discovered software as either unauthorized (rogue) or authorized. Newly discovered software can be reviewed by security teams in order to determine its legitimacy. Discovered software is fingerprinted and organized into software groups, thereby fulfilling asset management efforts. Uncategorized software can be organized by administrators into new or pre-existing software classifications or assigned for remediation.
- Beyond software detection, RAS has the ability to itemize open ports and services running on target endpoints. RAS Asset Discovery engines continuously report running services on target endpoints. Simple actions via the RAS Portal UI can classify designated ports or discovered services as authorized/unauthorized.

Control 3: Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers

- It is only a matter of time before newly installed software, exceptions, or illegitimate changes disrupt the integrity of a hardened security image. Fortunately, RAS enumerates thousands of control checks that can be scheduled for continuous monitoring. RAS can build customized security standards or policies that report on compliance to secure configuration settings or patch lists across multiple platforms. From laptops to servers, RAS allows for ease in reporting hosts that violate one or more security configuration baselines. Coupled with batched or automated alerting, your security operations teams now have an ally for seeing what and who is out of synch with an established security configuration benchmark.
- With new Open Vulnerability Assessment Language (OVAL) checks published regularly, the depth of your configuration baseline can grow extensively and in line with todays latest security threats. Tying each control check to a given policy, standard, or patch allows for continuous reporting on configuration gaps.

Control 4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

- The functionality provided by RAS, in terms of monitoring workstation and server level security configurations, is also replicated in functionality for network devices. RAS has incorporated various network templates, including Cisco IOS configuration checks, to ensure that the proper security settings are in place across Layer 3/Layer 4 network devices.
- Using the RAS Policy and Controls section, building a unique network standard with network device configuration checks can quickly provide administrators with the means to identify vulnerable network assets that require improved security settings.

Control 5: Boundary Defense

- Part of the strategy for boundary defense is, first, knowing the extent of your perimeter networks. The RAS Network Discovery module allows for network administrators to better understand their threat landscape by seeing what accessible networks are in fact present within their enterprise.
- The Network Discovery module has consistently been able to find both authorized and unauthorized networks within any given enterprise in order to fully depict the scope of network boundaries for which to apply effective countermeasures. Network-level configuration checks, managed and run by the Configuration Module, discover both what boundaries are at stake and their security configurations.

Control 6: Maintenance, Monitoring, and Analysis of Security Audit Logs

- To ensure proper incident response and forensic analysis, it is critical that native logging capabilities are in place for a given host. With several checks on how log file management should behave across various file systems, The RAS Configuration Management module ensures that the proper logging levels and the security configurations aimed at protecting such logs are in place.

Control 7: Application Software Security

- An added component to the RAS platform is its Web application security module, which conducts security assessments against discovered and newly added hosts running web-sites, Web services, or Web proxies. The easy-to-use and intuitive RAS management interface takes the complexity out of those assessments and facilitates a repeatable process via its assessment scheduler.

Control 8: Controlled Use of Administrative Privileges

- Multiple control checks are present within the RAS Configuration Module to provide insight into various permission sets at the host and file levels. These checks are part of the platform's built-in capabilities for ensuring rights of least privilege across all assets that are inventoried by the platform. Listing of elevated accounts on assets, as well as access levels from existing host or domain level accounts, are easily reported and displayed in the RAS Portal.
- Reports that encompass domain-level roles, file-share settings, folder shares, and local file permissions all help ensure that a controlled use of elevated privileges is properly enforced within the enterprise.

Control 9: Controlled Access Based on Need to Know

- Access based upon a need to know is going to be unique across various industries, organizations, and business units. Fortunately, RAS enables users to customize what thresholds for data access should be measured across platforms of varying types. With thousands of OVAL- and non-OVAL-based checks, suitable need-to-know control checks can be found in order to measure access to shared drives, files, folders, or drives.

- Prior to designating access rights to any data source, an understanding of the data itself is paramount. What data is being stored? Where is it being stored? How sensitive is this data? The answers to these questions lie with an effective form of data classification across the enterprise. RAS provides the ability to effectively map information across IT assets using four distinct properties: classes, categories, business applications, and organization. Within each of these four properties, users can define numerous elements to describe the information assets.

Control 10: Continuous Vulnerability Assessment and Remediation

- The Vulnerability Module provides for a vast range of capabilities for continuous vulnerability assessments. Leveraging its ability to interface with existing vulnerability management solutions and its ability to automate thousands of OVAL-based checks, RAS fulfills yet another facet of security operations via a vulnerability module that allows for unique scan scheduling, targeted scans, and bandwidth throttling. With unique vulnerability scan schedules, different times, and targets, scan throughput can all be controlled via one common and simple-to-use UI.
- Results from each scan can be automatically assigned based on asset classification levels to users or groups integrated within RAS. This is one of many ways in which RAS facilitates remediation efforts for any vulnerabilities found. Additionally, RAS provides for easy integration with existing ticketing and remediation workflows. If those are unavailable, RAS native ticketing capabilities provide task assignment, handling, alerting, and closing of vulnerability remediation tasks.

Control 11: Account Monitoring and Control

- The Configuration Management module provides a high level of insight into how user accounts, on local hosts and in domains, are managed in terms of password settings (expiration, password length, and complexity checks), successful logins, and failed logins; it also provides an enumerated list of active accounts for the hosts and domains assessed. These and many other account-related concerns can be continuously monitored through the scheduling of continuous/repeated host-level configuration scans.
- The Policy and Controls section of the RAS Control Panel provides an easy interface for creating unique baselines for measurement. Content checks can be customized so that discrepancies in account settings can be caught and remediated on a daily basis.

Control 12: Malware Defenses

- Outdated or non-existent antivirus software continues to provide easy attack vectors across many enterprises. Knowing where malware defense gaps exist within an organization is a pivotal step. RAS provides in-depth data gathering of all hosts, allowing security managers to know if and when malware defenses have been deployed and, in some cases, to what degree. These data-gathering efforts can take place at various times and frequencies, depending on the target networks and using the RAS Configuration Management scan schedule.

- Develop a unique policy or standard where all malware-defense-related software is discovered and inventoried. From AV software to HIPS agents to FDE (full disk encryption) solutions - RAS will easily report compliance levels to whatever malware countermeasures are in place.

Control 13: Limitation and Control of Network Ports, Protocols, and Services

- The Asset Discovery module for RAS allows for both ephemeral and non-ephemeral ports to be scanned and identified as an authorized service/ application. Ports associated with valid commercial or internally developed applications can be properly labeled when discovered by the Asset Discovery module.
- With a recommended daily host discovery scan, a thorough portscan is simultaneously conducted across a customer-defined list of ports, protocols, and running services. Open ports along with running services are revealed per host as well as in enterprise-wide reports. Users can decide whether certain protocols or services should be assigned for remediation or simply listed as low risk.

Control 14: Wireless Device Control

- Through both network discovery and host discovery, RAS is able to greatly close the gap on rogue networks and network devices that were never formally approved. Using varied network and host discovery scans, RAS scanners are able to comb the network in order to reveal potential rogue technology that should never have been present. Once rogue networks or wireless network assets are identified, they automatically become listed as rogue, and users can be alerted of their presence.

Control 15: Data Loss Prevention

- Like most security efforts, effective data loss prevention stems from a combination of both effective process and technical controls. RAS provides the necessary oversight to technical controls that should be in place to prevent data loss. Encryption provides a key element of defense; however, knowing or not knowing whether or not an encryption solution is present is critical. Since RAS is able to determine software assets installed on target hosts, it is easy to see if the proper level of protection is in place. Other data loss prevention checks at the file-system level can also be easily implemented to report on data leakage.

Critical controls subject to manual collection, measurement, and validation

The remaining manual controls identified by the CAG relate to process-driven security measures which RAS supports through its ability to discover, evaluate, and report. For each one of the following five control areas, RAS is able to support these processes by determining the scope of assets to be assessed:

Control 16: Secure Network Engineering

- A secure architecture ensures that both authorized and unauthorized network assets do not adversely affect a secure network design. Knowing what network assets are present along with their configuration settings is very important in documenting a secure network architecture.

Control 17: Penetration Testing

- Part of any vulnerability management program or "red team" attack strategy is to clearly define the scope and obtain reconnaissance information which will fuel ethical hacking efforts. Using RAS ongoing discovery, vulnerability assessment, and Web application-simulated attack patterns, penetration testers will have a valuable platform om which to build .

Control 18: Incident Response Capability

- The level of information managed by RAS provides critical data across the various phases of incident response efforts. During the Identification, Containment, Eradication, and Recovery phases, scope definition as to what assets are in scope can be quickly viewed through the RAS asset management reporting interface. When malware hits and exploits known ports or services across an enterprise, RAS can also help to reveal the list of assets that may be in the scope of containment efforts. Lastly, because RAS has the ability to help classify/ categorize assets into groups, security managers have the ability to derive which assets are high- to low-impact systems across the organization, thereby assisting in strategic recovery planning.

Control 19: Data Recovery Capability

- Similar to the other three areas addressed, defining a scope and set of classifications for enterprise assets can prove useful when wanting to define the scope of information assets that require recovery efforts. If enterprise backups are conducted, RAS can also assist in ensuring that local backup software agents are in place and configured correctly. This can provide assurance that all necessary services and software have been in place and running on an endpoint in order to facilitate recovery efforts.

Control 20: Security Training

- Information provides a key basis for training. Given the various layers of security processes that are addressed, correlation can be drawn to information managed by RAS in order that training efforts can be complemented with supportive evidence coming straight from the enterprise.

Conclusion

The Consensus Audit Guidelines, developed by multiple industry experts, is an effective guide for blocking well-known, high-priority attacks across government infrastructures.

The Symantec Risk Automation Suite (RAS), directly addresses eight of the fifteen controls that can be continuously and automatically monitored, and it supports automation efforts of the other seven controls that can be continuously and automatically monitored. The remaining five controls require governance from a well established information security program, ideally run in parallel to the automated, continuous monitoring provided by a technical solution. Even with these final five controls, RAS provides evidence in support of increasing an agency's security posture, and greatly enhancing

near-real-time situational awareness. Complementary Symantec products for the enterprise also play a significant role in addressing and/or supporting specific control areas as well, and these products should be evaluated in the context of an overall solution for the Consensus Audit Guidelines.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our website.

Symantec Public Sector Headquarters
2350 Corporate Park Drive
Suite 300
Herndon, VA 20171 USA
http://go.symantec.com/federalgovernment

Symantec helps organizations secure and manage their information-driven world with **IT Compliance**, **discovery and retention management**, **data loss prevention**, and **messaging security** solutions.

5/2010 21035042