ARCHITECT'S GUIDE:

Security Automation Using TNC & SCAP Technology

February 2013

Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97006
Tel (503) 619-0562
Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

Executive Summary and Action Items

Security automation enables network and security systems to provide dynamic, responsive protection with automated handling of routine security tasks, allowing administrators to focus on critical areas such as threat analysis and policy development. This streamlined approach to enterprise security improves efficiency and reduces cost, and enhances an organization's ability to monitor and respond to increasing and targeted network attacks.

Both commercial and open source developers as well as numerous U.S government agencies have embraced standards — such as the Interface for a Metadata Access Point (IF-MAP) from the Trusted Computing Group's (TCG's) Trusted Network Connect (TNC) work group, and the National Institute of Standards and Technology's (NIST's) Security Content Automation Protocol (SCAP) — to build products ideally suited for implementing security automation.

This Architect's Guide shows enterprise security architects how they can design and deploy successful automated security solutions based on the open TNC architecture and standards along with interoperable compliance establishment through SCAP.

Critical strategies for architects include:

1. **Automate assessment and continuous monitoring** for real-time protection of the enterprise network and connected devices.
2. **Control access to sensitive resources** based on established corporate policies that can be reliably interpreted by network hardware.
3. **Coordinate communications among security systems** via open-standard protocols.
4. **Monitor and respond to potential network threats** using a combination of industry and government developed standards.

Introduction

Security automation allows network and security systems to operate with minimal human intervention. Two critical enterprise factors provide the driving force behind the automation of information security operations:

The first driver is the need for higher security efficiency and cost control. A variety of different systems performing different functions that have to be correlated manually costs money to maintain and more money to investigate an incident. For example, in a Bring Your Own Device (BYOD) environment, manually registering every employee's personal device to differentiate them from corporate assets is a significant cost to the enterprise and a huge inefficiency. In contrast, using an automated process to differentiate between a corporate asset and a personal device — rather than having a human make a decision every time — reduces the overhead through less human involvement.

A second business driver is the increase in targeted attacks with malicious purposes. These evolving attack methods make Internet communications increasingly dangerous for enterprises and individuals. Unlike malware, botnets and other traditional attacks, Advanced Persistent Threat (APT) attacks do not try to indiscriminately affect as many systems as possible — they are intended to pinpoint a particular objective in a targeted attack. Once the compromise occurs, the attackers want to stay hidden and steal as much data as possible. When this type of attack is enabled by exploiting a zero-day vulnerability — a undiscovered system weakness without a vendor patch to prevent it — detection and protection can be very difficult.

The 2011 RSA data breach[1] is an example of an APT attack using a zero-day vulnerability. A spreadsheet with a zero-day exploit, sent to an RSA employee, compromised the employee's computer when the spreadsheet was opened. Since it was an unknown vulnerability, the computer's anti-virus software did not detect or prevent the attack. Once the endpoint was compromised, the attacker used that computer as an internal operating base to penetrate other systems and steal sensitive data.

Solution Overview

When a security company such as RSA becomes a victim of cybercrime, a new approach to security needs to be considered. Security automation provides such a new approach: automating routine information security tasks to narrow the window of opportunity while freeing up human bandwidth to focus on more complex aspects of security such as policy and threat analysis.

As described in COBIT, ISO 27001, and any number of similar models, information security is a process of continuous improvement with steps that correspond to the four phases of the well-known Deming Cycle: Plan, Do, Study, and Act. As shown in *Figure 1,* these four phases when applied to information security may be labeled Configure, Detect, Analyze, and Respond.

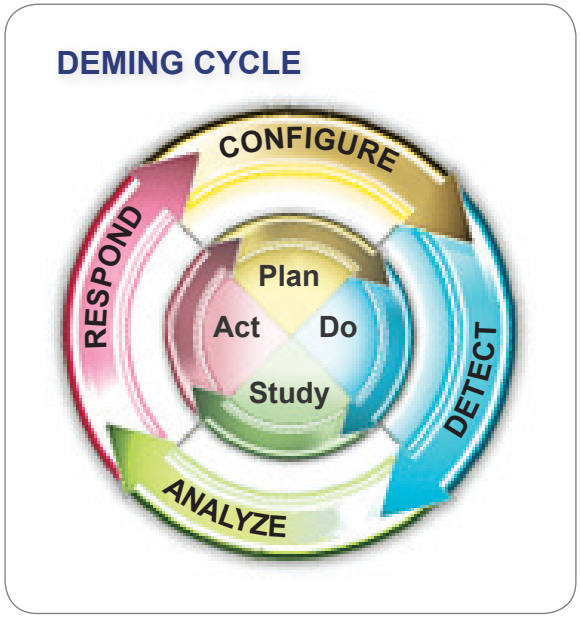

Figure 1: The four-step Deming cycle applied to the concept of security automation.

Security automation can assist with each of the steps in this cycle and with the transition from one step to the next. For example, secure system configurations can be shared and automatically verified and maintained. A security automation system can handle such routine tasks. Humans can direct the system and deal with anomalies and exceptions.

[1] http://news.cnet.com/8301-27080_3-20051071-245.html

Copyright © 2013 Trusted Computing Group All rights reserved. www.trustedcomputinggroup.org

Security Automation – Compliance

One common use for security automation is establishing endpoint compliance in order to grant appropriate access to sensitive data. One challenge for compliance is that a personal device may not have the same security controls as a corporate device. For example, a corporate device may have a self-encrypting drive (SED), which limits access to its stored data by encrypting that data, whereas personal devices are less likely to have this technology. An organization's security policy may permit access to sensitive data only via devices with SEDs; this protects the data after it is transferred to the accessing device's drive.

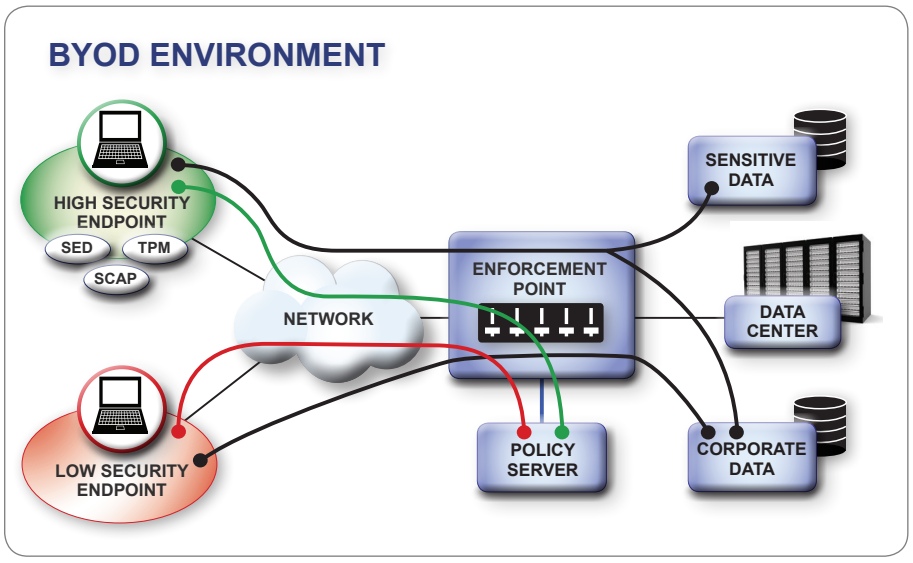

Figure 2: Compliance and appropriate user access in a BYOD environment.

As shown in *Figure 2,* a corporate asset with an SED (green) may receive full access to corporate resources. A personal device that does not have an SED (red) may receive restricted access. A user on a personal device can do some work, such as checking email, but cannot access protected data such as personal health information (PHI) in a environment regulated by Health Insurance Portability and Accountability Act (HIPAA), or financial information in a Payment Card Industry (PCI) environment. Security automation detects, analyzes, and responds to distinguish between the two devices and provide the appropriate access.

SCAP – NIST Standards for Compliance Automation

The Security Content Automation Protocol (SCAP)[2] is a collection of standard data formats, identifiers, enumerations, and scoring methods that can be used to address software inventory, configuration management and vulnerability management use cases.

Prior to the existence of SCAP, there was no standard format for expressing device configuration and compliance. SCAP allows multiple tools to exchange and use standard data, providing consistent and interoperable results for compliance and configuration checks.

Key SCAP standards include:

- **Extensible Configuration Checklist Description Format (XCCDF),** which captures descriptions of configuration settings, warnings and usage guidance, and any associated metadata
- **Open Vulnerability and Assessment Language (OVAL),** which provides low-level descriptions of configuration artifacts (such as the Windows registry)
- **Common Vulnerabilities and Exposures (CVE),** a standard enumeration for vulnerabilities
- **Common Platform Enumeration (CPE),** a standard enumeration and identifier for platforms
- **Common Configuration Enumeration (CCE),** a standard enumeration for configuration items
- **Common Vulnerability Scoring System (CVSS),** for measuring the severity of vulnerabilities
- **Common Configuration Scoring System (CCSS),** for measuring the severity of configuration issues

NIST's National Vulnerability Database (NVD) contains over 45,000 vulnerability records indexed by a CVE identifier. As part of NVD operation, NIST characterizes and has descriptions of the vulnerabilities that the identifier applies to and they associate that vulnerability with products using CPE.

Used extensively in U.S. government organizations, especially for non-classified documents, processes, and activities, special publication (SP) NIST SP 800-117 provides high-level guidance on the value of SCAP and how organizations should use it.

NIST is developing a reference architecture for security automation named the Continuous Asset Evaluation and Risk Scoring Framework Extension (CAESARS-FE).

Combined with TCG's TNC protocol standards, SCAP compliance data can be shared in a standard manner.

[2] http://scap.nist.gov/

Copyright © 2013 Trusted Computing Group All rights reserved. www.trustedcomputinggroup.org

Security Automation – Intervention

Another common use for security automation addresses rapid response for security issues such as APT mitigation and insider attacks. An automated security system is prepared to detect, analyze, and respond to problems as they occur.

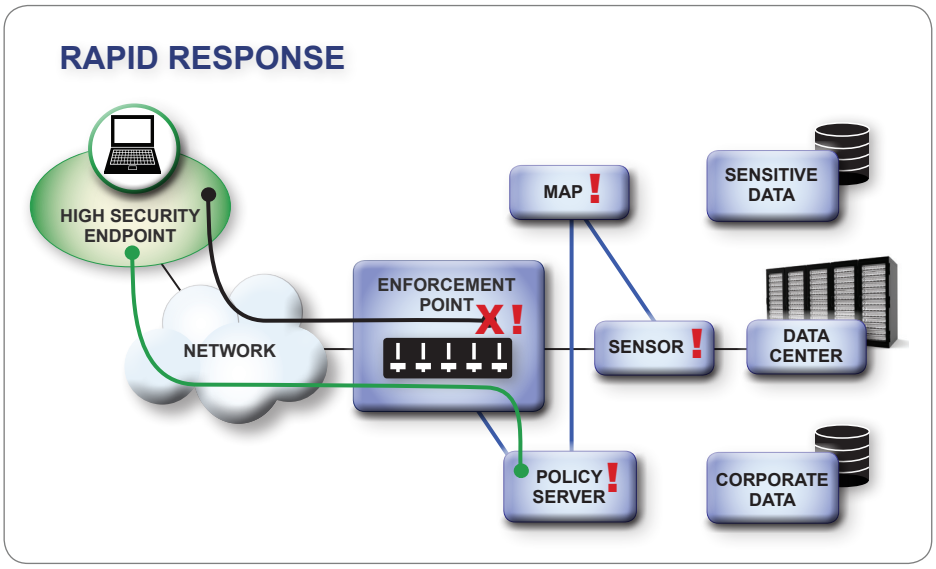

Figure 3: Rapid response to inappropriate behavior.

As shown in *Figure 3,* an authorized user on a compliant endpoint has normal network access based on the device's and user's security levels. If the endpoint is compromised by a zero-day exploit or used in an insider attack, and its behavior deviates from its expected operation in a way that is not authorized in the network, an intrusion prevention or behavior monitoring system can detect the unauthorized behavior and signal the access control system to modify the endpoint's access. Restriction of access to privileged data on the network occurs automatically. Security automation detects, analyzes, and quickly responds to unexpected changes to the network and provides the appropriate access or restrictions to the endpoint.

TNC and IF-MAP

Trusted Network Connect (TNC)[3] is an open architecture and set of network security standards created by the Trusted Computing Group (TCG).

IF-MAP, the Interface to a Metadata Access Point, is the TNC standard most essential for security automation. IF-MAP provides a standard way for information security products to rapidly share and respond to information about a variety of security-related topics and events.

IF-MAP is a client-server protocol that enables MAP Clients to publish "metadata" to a Metadata Access Point (MAP), which functions as a database. Other MAP Clients can query the MAP or subscribe to changes.

In the example illustrated in *Figure 3,* endpoint misbehavior is detected by a Sensor, which uses the IF-MAP protocol to publish an event to the MAP. The MAP notifies the Policy Server of this event (because of a previous subscription request) and the Policy Server responds by blocking further misbehavior using the Enforcement Point.

Users of IF-MAP enabled products can implement more effective, integrated security systems, gaining the following benefits:

- Coordinated security response across multiple products from multiple vendors
- Stronger security with lower operating costs since sensors (e.g. IDS) can be tied automatically into flow controllers (e.g. firewalls), reducing the need for human intervention and accelerating security responses
- Easier integration of data from multiple vendors and devices into security event management (SEM) and other logging and reporting systems
- Fewer false alarms (and therefore lower operating costs) since sensors can tune their detection algorithms based on user and machine identity and role
- Simpler, more intuitive policies based on user identity and role instead of IP address
- More comprehensible incident reports from sensors since they can include user identity

Common uses of IF-MAP in the enterprise today include:

- Security automation
- Integration of physical and logical access control
- Seamless remote and local access control
- Industrial control system and SCADA security
- Network enforcement for legacy devices
- Integration of behavioral detection with NAC

[3] http://www.trustedcomputinggroup.org/solutions/network_access_and_identity

Copyright © 2013 Trusted Computing Group All rights reserved. www.trustedcomputinggroup.org

Solution Architecture

The TNC/SCAP architecture solution consists of two parts: (1) compliance analysis and (2) detection and response. SCAP provides a rigorous approach to compliance. Compliance includes health checking interfaces, such as a TNC client that checks the status of the endpoint, a policy server that validates the endpoint and an enforcement point that determines the resulting actions.

For detection and response, the sensing devices that monitor the network and detect unauthorized behavior use the Metadata Access Point (MAP) service to share information with policy and enforcement components.

As shown in *Figure 4,* the IF-MAP information bus provides the critical link between sensors, such as a Security Information & Event Manager (SIEM) , an SCAP scanner, or a Intrusion Prevention System (IPS); enforcers, such as a Unified Threat Management (UTM) device or a Next-Generation Firewall (NGFW); and a Security Operations Center (SOC) or security administration user. Once the system is configured, the automated aspect minimizes the involvement of the human operator except in abnormal instances detected by the automated system.

The system sensors signal the MAP service when they detect unauthorized behavior. If this occurs, the MAP service notifies the policy server that authorized that device's network access. Even if the device is compliant and an authorized user is operating it, the device can be quarantined or disconnected because of its exhibited inappropriate behavior.

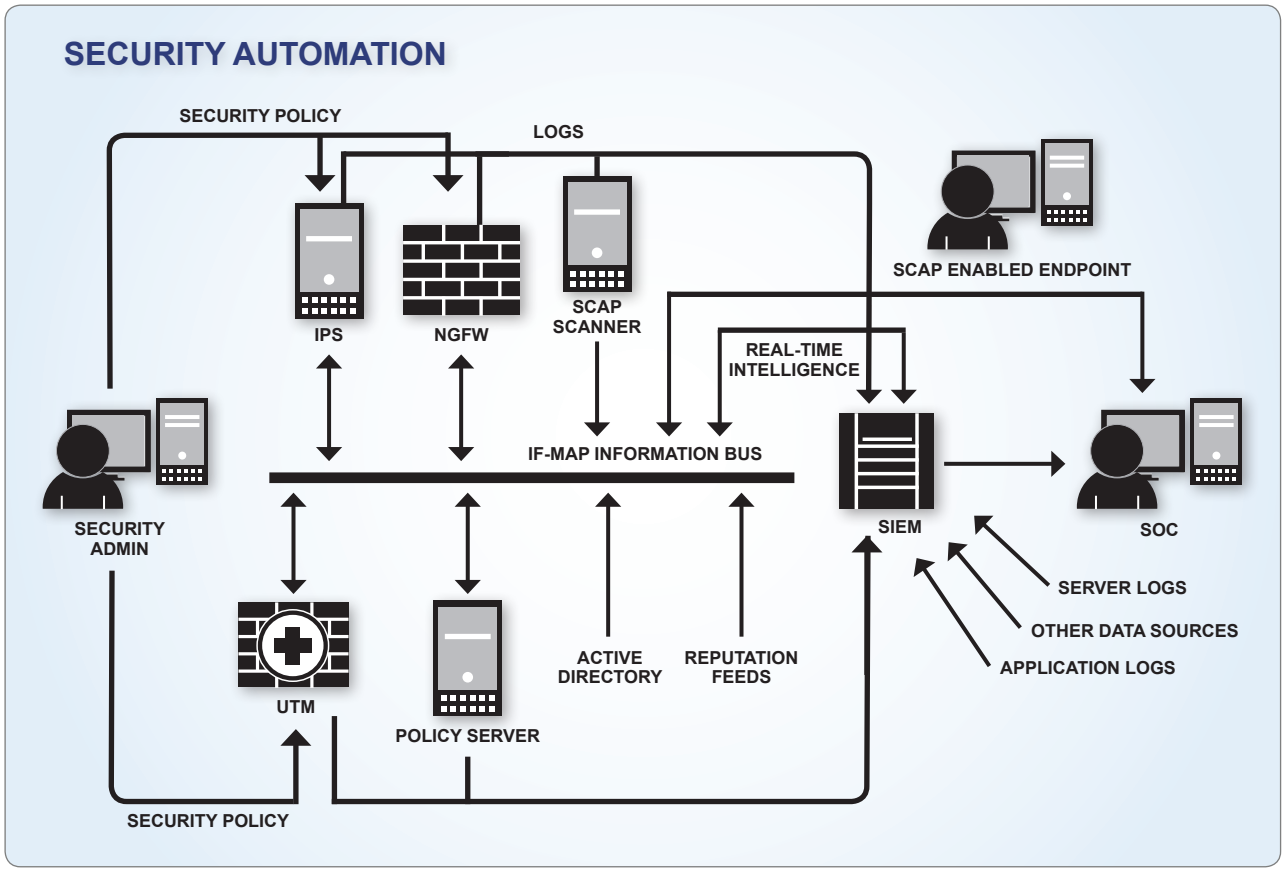

Figure 4: The big picture of security automation.

The elements in *Figure 4* can be interconnected using off-the-shelf components, providing interoperability, scalability, and reusability. With consistent conformance data provided by SCAP, highly protected and extremely reliable security automation results.

Copyright © 2013 Trusted Computing Group All rights reserved. www.trustedcomputinggroup.org

Future

IF-MAP and SCAP are used extensively in real-world applications today for commercial and government applications, including critical infrastructure protection. The developers of these security standards are looking at ways that they can be expanded to apply to new use cases in the future.

Possible future applications of IF-MAP include:

- An analysis system determines that there's an attack underway; in addition to triggering a response, it notifies security administrators of the attack taking place, populating a dashboard with information to create a "heat map" of the attack
- A content management database (CMDB) receives notification of a new device on the network – perhaps via notification that a DHCP server has assigned an IP address to a new MAC address — and scans the new endpoint, then updates its data store with endpoint identity, software inventory and configuration state information
- An IF-MAP enabled SDN controller makes packet-handling decisions based on information from other network components
- An analysis engine observes some behavior on the network and requires more information about the associated endpoint, so it requests an investigation by another component such as an endpoint profiler or vulnerability scanner
- A security administrator modifies an existing security policy, or adds a new policy, and various policy servers / sensors are notified, triggering a re-evaluation of the network's endpoints
- Network routers redirect traffic through deep packet inspection based on suspicious user activity
- An application server publishes a request for bandwidth for a particular user based on the service the user is accessing — and network infrastructure components change Quality of Service (QoS) settings for those traffic flows based on that request

NIST envisions further expansion of its security automation efforts in compliance, remediation, and network monitoring, and encourages contribution relative to these and additional disciplines. In addition to improving support for being able to assess servers and workstations for their security configuration compliance, NIST is investigating techniques to expand SCAP to support network devices and to address printers and mobile devices as well.

Conclusion

Security automation's goal is linking together information from all of the various infrastructure and security technologies in an enterprise's network and using that information to make dynamic, intelligent, automated decisions.

The benefits of security automation are improved efficiency, reduced operating costs, and dynamic protection against increasing threats, with a methodology that can evolve as the threat landscape evolves.

A network operating autonomously under normal conditions, where humans only have to get involved for exceptions, results in increased system efficiency and lower labor costs. Open standards keep costs low by reusing existing infrastructure resources rather than replacing them with single vendor products that use proprietary protocols.

One final benefit of security automation is better visibility. Security automation allows admins to see real-time information on endpoint compliance, user access, and network threats more thoroughly than was previously possible.

Call to Action

- Design security automation solutions customized for your unique environments
- Contact vendors and insist on acquiring TCG-certified security automation solutions based on the TNC and SCAP standards
- Deploy solutions in pilot first, observe and correct issues and then deploy into production
- For more information on TCG technologies and architects guides, please visit the Trusted Computing Group web site www.trustedcomputinggroup.org
- Additional information on security automation will be available over the next several months. Learn about the latest advances by following us on LinkedIn, Facebook and Twitter.

Contact TCG at admin@trustedcomputinggroup.org with any questions.

Copyright © 2013 Trusted Computing Group All rights reserved. www.trustedcomputinggroup.org