

# CORE IMPACT AND THE CONSENSUS AUDIT GUIDELINES (CAG)

Extending automated penetration testing to develop an intelligent and cost-efficient security strategy for enterprise-scale information systems

## CAG BACKGROUND

In 2009, a consortium of United States federal agencies and their private-sector partners released the Consensus Audit Guidelines (CAG), a set of twenty IT security controls that the group has recommended for adoption across all U.S. government agencies to improve protection of federal information systems and encourage organizations to implement methods for continuous compliance with the Federal Information Security Management Act (FISMA).

Authored by constituents including the Department of Defense (DoD), Department of Homeland Security (DHS) and National Security Agency (NSA), along with government agency CIOs, the National Institute of Standards and Technology (NIST) and private IT consulting, training and solutions providers, the CAG controls were written to dovetail with the latest version of the NIST 800-53 security mandate, which was comprehensively updated in February 2009. These NIST-issued guidelines are recognized as the de facto operational requirements for government agencies preparing for government IT security audits dictated by FISMA.

## CAG OVERVIEW

The introduction to the CAG guidelines, first published by training specialists at The SANS Institute in Feb. 2009, specifically cites the need for federal cyber-security controls that are tacitly proactive and can “inform defense” of actual attacks that have compromised systems, or those that could transpire to do so.

This endorsement of more proactive security controls and ongoing self-assessment is also a primary element of the U.S. Information and Communications Enhancement (ICE) Act of 2009 which the Senate Homeland Security and Government Affairs Committee have proposed as a replacement for the existing FISMA legislation, and is currently awaiting review by Congress.

The ICE Act expressly calls on federal agencies to:

*“Monitor, detect, analyze, protect, report, and respond against known vulnerabilities, attacks, and exploitations” and “continuously test and evaluate information security controls and techniques to ensure that they are effectively implemented.”*

The CAG document also submits that the controls it recommends should be “automated where possible, and periodically or continuously measured using automated measurement techniques where feasible.”

## WHERE CORE IMPACT PENETRATION TESTING FITS IN

Among the listed CAG controls is one, Critical Control 17, which specifically calls for agencies to adopt proactive penetration testing and Red Team assessment exercises which can be addressed using CORE IMPACT Pro.

Another, Critical Control 10, demands continuous vulnerability assessment and remediation, a process to which IMPACT Pro and penetration testing can lend tremendous benefits in validating and filtering results.

There are also a handful of other CAG controls that involve security programs to which penetration is relevant both as a functional process and in embracing the underlying spirit and intended goals of the measures.

The following is a listing of individual CAG controls that can either be achieved or optimized via the use of the CORE IMPACT Pro automated penetration testing solution, as well as those wherein use of the solution can help meet individual elements of the guidelines.

### Directly Applicable CAG Controls

#### **Critical Control 17: Penetration Tests and Red Team Exercises (Excerpt)**

“Organizations should conduct regular penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.”

**CORE IMPACT Pro** provides organizations with the ability to perform ongoing penetration testing of Web applications, network systems, endpoints and email users, and to simulate both external and internal attacks, including the ability to carry out testing over wireless networks. Using the solution’s library of safe, commercial-grade exploits, agencies can isolate, validate and prioritize exploitable vulnerabilities across their IT assets and gain an acute understanding of how flaws or mis-configurations can be used by attackers to gain access to critical programs and backend databases.

IMPACT Pro automates many of the time-consuming tasks involved in manual pen testing and reporting functions, and allows testers to add, expand and/or customize onboard exploit code via an extensible Python interface. In addition, discovering vulnerabilities and attack vectors using IMPACT Pro proves weaknesses, possible violations and potential improvements required in many of the other Critical Control areas.

### **Critical Control 10: Continuous Vulnerability Assessment and Remediation (Summary Excerpt)**

“Organizations should run automated vulnerability scanning tools against all systems on their networks on a weekly or more frequent basis... Security personnel should chart the numbers of unmitigated, critical vulnerabilities, for each department/division [and] share vulnerability reports indicating critical issues with senior management to provide effective incentives for mitigation... Organizations should measure the delay in patching new vulnerabilities and ensure the delay is equal to or less than the benchmarks set forth by the organization.”

**CORE IMPACT Pro:** Vulnerability Assessment, specifically scanning, provides organizations with an initial list of possible vulnerabilities for remediation through signature based checks. IMPACT Pro offers fully-supported integration with multiple top-tier vulnerability scanners, giving organizations the ability to import results to initiate the penetration testing process and filter scanner output to prioritize risks, eliminate false positives and understand how multiple issues across different IT systems can be used in concert during multi-staged attacks.

Using IMPACT Pro to run automated penetration testing on a regular basis across network systems, endpoints and applications, provides security staffers with detailed information about which vulnerabilities can be most easily utilized by attackers to gain access to their systems and data – including which databases and what types of information may be exposed. Automated penetration testing empowers organizations with the actionable data they need to foster more efficient patch management and remediation programs, and to ensure that patching and other operational security projects are meeting required goals and schedules.

IMPACT Pro produces detailed reports of vulnerabilities and the specific risks they pose in language tailored to different audiences with varied levels of technical acumen, giving IT security departments the ability to calibrate and benchmark risks to measure changes and improvements over time, and demonstrate the efficacy of ongoing mitigation efforts to management officials.

## **Contextually Applicable CAG Controls**

### **Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers (Summary Excerpt)**

System images must have documented security settings that are tested before deployment [and] should be validated and refreshed on a regular basis (such as every six months) to update their security configuration in light of recent vulnerabilities and attack vectors... run assessment programs on a varying sample of systems to measure the number that are and are not configured according to the secure configuration guidelines... provide senior executives with charts showing the number of systems that match configuration guidelines versus those that do not match, illustrating the change of such numbers month by month for each organizational unit.

**CORE IMPACT Pro** allows organizations to test device security mechanisms before deployment and on an ongoing basis to ensure that they prevent specific types of threats, including many cutting-edge hacking and malware techniques. IMPACT Pro gives organizations a comprehensive, automated

manner of running periodic assessments to track which devices are or are not properly defended from real-world threats, and generates detailed reports that can be shared with management to highlight overall status and establish benchmarks that can be referenced over time to measure and demonstrate the efficacy of ongoing mitigation efforts.

#### **Critical Control 4: Secure Configurations of Network Devices Such as Firewalls and Routers (Summary Excerpt)**

“Organizations should compare firewall, router, and switch configurations against standard secure configurations... test (firewalls, network IPS and routers) that filter unneeded services or block attacks against traffic including a mixture of legitimate, allowed traffic with attacks at line speeds... attempt to launch packets through the device, measuring all TCP and UDP ports allowed through... such measurement should be conducted at least every quarter, and also when significant changes are made to firewall rule sets and router access control lists.”

**CORE IMPACT Pro** gives organizations the ability to test the efficacy of firewalls, IPS/IDS and other network security tools on an ongoing basis to ensure that they react properly to specific types of threats. Conducting regular penetration testing of network assets protected by these types of security systems also gives organizations the ability to establish benchmarks and create tangible metrics that can be used to measure the performance of the security systems over time, and highlight the effect that modifications made to their rules and settings have on their ability to stop various methods of attack. Testing can be carried out safely on live production systems to highlight network security performance under real-world operating conditions.

#### **Critical Control 5: Boundary Defense (Summary Excerpt)**

“Organizations should deploy IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic... All devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels... Organizations should periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.”

**CORE IMPACT Pro:** Provides organizations with the ability to proactively test their networks to determine how required security systems are performing in preventing specific types of threats, and to ensure that undesired traffic cannot circumvent security control mechanisms, or authentication systems. With an extensive, regularly updated library of exploit code that emulates the same types of malicious traffic (both incoming and outgoing) produced by hackers and malware programs, including Trojan attacks and botnets, IMPACT Pro allows organization to understand precisely how real-world threats and hacking campaigns will target perimeter security controls.

### **Critical Control 7: Applications Software Security (Summary Excerpt)**

“Organizations should... test Web application for common attacks, including but not limited to Cross-Site Scripting, SQL injection, command injection, and directory traversal attacks. Organizations should test in-house developed and third-party procured Web and other application software for coding errors and malware insertion, including backdoors prior to deployment using automated static code analysis software. Organizations should test in-house developed and third-party procured Web applications for common security weaknesses using automated remote Web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis, such as weekly.”

**CORE IMPACT Pro** allows organizations to proactively assess Web applications for available vulnerabilities and attempt to exploit any issues discovered to understand precisely how real-world attackers can use the weaknesses to target applications, either to affect performance (including via DoS type attacks) or move through them into other IT assets to carry out subsequent attacks or data theft (including Cross-Site Scripting, SQL injection, buffer overflow and PHP file inclusion). Bringing IMPACT Pro in-house not only allows organizations to test applications for potential vulnerabilities throughout the development process and while in production, giving them the ability to create benchmarks for applications security status over time, but also allows them to compare results with traditional vulnerability scanners to eliminate false positives and target costly remediation efforts on their most significant exposures.

### **Critical Control 8: Controlled Use of Administrative Privileges (Summary Excerpt)**

“Organizations should change all default passwords for applications, operating systems, routers, firewalls and other systems to a difficult-to-guess value... configure all administrative-level accounts to require regular password changes on a 30-, 60-, or 90-day interval... implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.”

**CORE IMPACT Pro:** Gives organizations the ability to test the ability of IT systems and applications authentication mechanisms in the face of specific methods of circumventing such controls. Having gained entry to an authenticated asset, IMPACT Pro also allows testers to leverage established user and network relationships to escalate attacks and scope the ability of real-world attackers to gradually advance their capabilities via the use of available administrative controls.

### **Critical Control 12: Malware Defenses (Summary Excerpt)**

“Organizations should monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, and host-based Intrusion Prevention System functionality... verify that anti-malware solutions are running [and] periodically introduce a benign, non-spreading test case onto a system in the environment to ensure that it is detected by the anti-malware system, and that the detection is reported to the enterprise anti-malware management

system... deploy honeypots or tarpits as detection mechanisms that can also slow down an attacker's progress inside a network.”

**CORE IMPACT Pro** offers organizations the ability to test the efficacy of their anti-malware defenses in preventing specific types of real-world hacking and malware threats, including the capability to pivot from vulnerable systems to other devices to which they are connected to further test the ability of those assets to detect suspicious activities and determine if the events are properly recognized by relevant security management tools. Using IMPACT Pro to assess the effectiveness of anti-malware solutions can also help illustrate whether other internal defensive techniques, such as honeypots and tarpits, have the desired effect of impeding various breeds of attacks.

### **Critical Control 13: Limitation and Control of Network Ports, Protocols, and Services (Summary Excerpt)**

“Host-based firewalls or port filtering tools should be applied on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. Periodically, a secure version of an authorized service should be activated on a relatively unimportant system to verify that the change is flagged by the configuration and vulnerability testing tools in the environment.”

**CORE IMPACT Pro:** Allows organizations to test the ability of firewalls and port filters to detect and block specific types of real-world hacking and malware threats, including Trojan and botnet attacks and their ability to use inbound and outbound data encryption techniques to circumvent security controls and remain hidden from filters while attempting to summon additional payloads and infections. IMPACT Pro also gives organizations the opportunity to conduct penetration tests on specific services to determine whether or not they trigger applicable management or vulnerability systems.

### **Critical Control 15: Data Leakage Prevention (Summary Excerpt)**

“Organizations should conduct periodic scans of server machines using automated tools to determine whether PII (personally identifiable information) data is present on the system in clear text. These tools, which search for patterns that indicate the presence of PII, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information in data at rest. Periodically, such as once per quarter, information security personnel should run a script that purposely tries to trigger the data loss prevention functionality deployed at network perimeters.”

**CORE IMPACT Pro:** Gives organizations the ability to prove the ability of hackers and malware programs to exploit vulnerabilities that can allow them to gain access to protected data, including the opportunity to understand which databases may be exposed and what types of information they contain. IMPACT Pro also allows IT security departments to test their perimeter defenses to see if they can detect a potential data breach incident by simulating stealthy malware and data theft techniques including Trojans and botnets, including the use of outbound data encryption, highlighting the ability of attempted data theft attacks to sneak information past existing controls.

## **Critical Control 20: Security Skills Assessment and Appropriate Training to Fill Gaps (Summary Excerpt)**

“Organizations should devise periodic security awareness assessment quizzes, to be given to employees and contractors on at least an annual basis, determining whether they understand the information security policies and procedures for the organization, as well as their role in those procedures... should conduct periodic exercises to verify that employees and contractors are fulfilling their information security duties, by conducting tests to see whether employees will click on a link from suspicious e-mail or provide sensitive information.”

**CORE IMPACT Pro:** Allows organizations to test employees' adherence to security training programs on a regular basis, including the ability to craft social engineering attempts such as targeted e-mail phishing campaigns that attempt to lure individuals into clicking on unverified website links or handing over sensitive information including customer records or IT systems log-on credentials. IMPACT Pro can also mine the Web for publicly available e-mail account information to spoof addresses within a specific organization and/or target those individuals whose data can be collected, just as real-world attackers do.

### **LEARN MORE**

For additional information on the specifics of NIST 800-53, specifically 800-53a “Appendix G” – which directly addresses the need for penetration testing and spells out the standards group’s requirements for such assessments – refer to the Core Security Web site (<http://www.coresecurity.com/content/nist-sp>) and the white paper “CORE IMPACT Pro and FISMA/NIST Compliance.”



For additional information on the CORE IMPACT family of comprehensive security testing products, please contact us at 617-399-6980 or via email at [info@coresecurity.com](mailto:info@coresecurity.com). You can also visit our web site at [www.coresecurity.com](http://www.coresecurity.com).