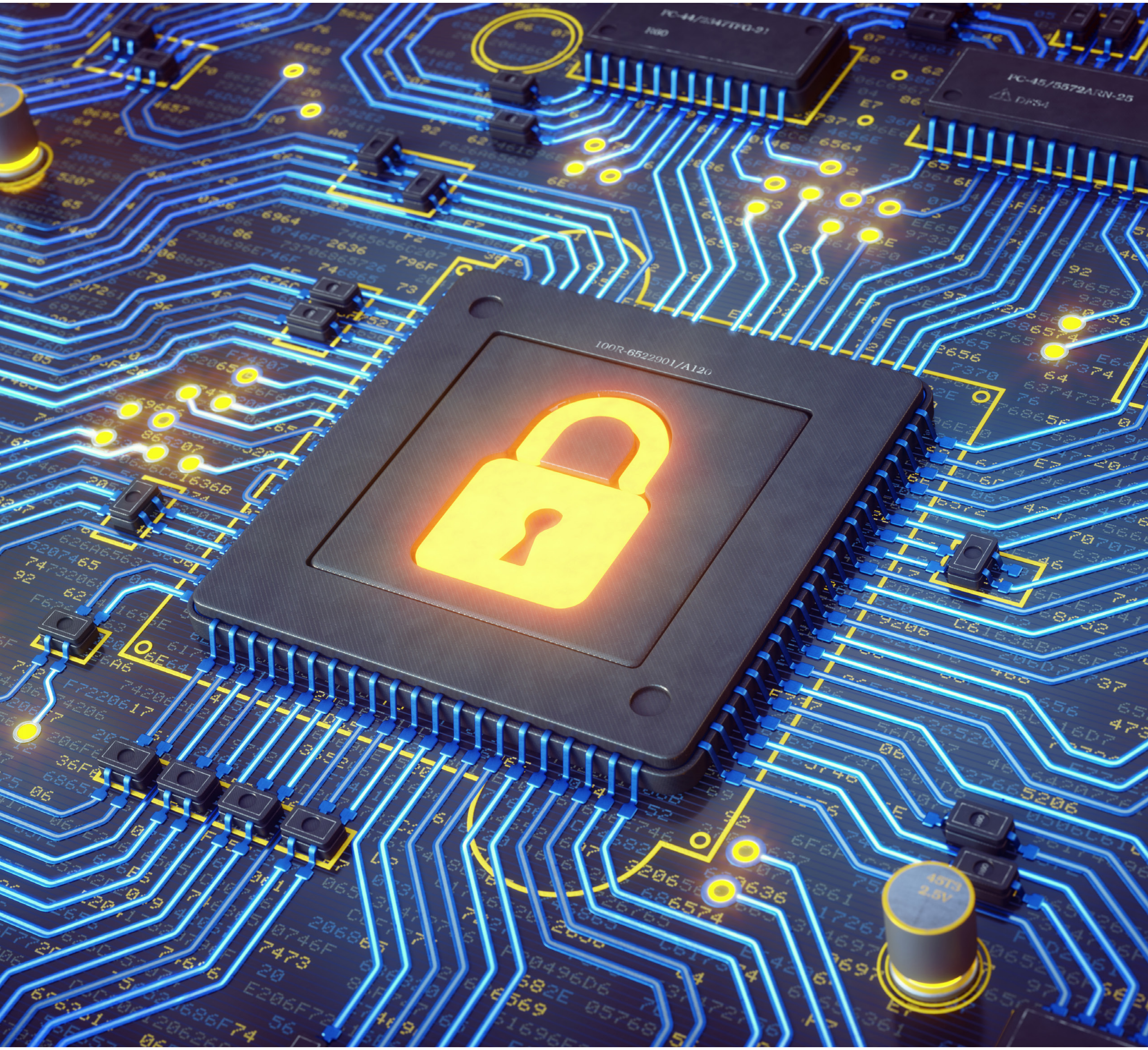
CANON SOLUTIONS AMERICA

ACS
agile cybersecurity solutions



CYBERSECURITY INTEGRITY AUDIT

Mitigating Risk Through Comprehensive Assessments

SMART CHANGE STARTS HERE.

CANON SEE IMPOSSIBLE

YOU CAN'T PROTECT WHAT YOU CAN'T SEE

The Cybersecurity Integrity Audit can help to expose vulnerabilities, thus enabling organizations to more effectively manage risk.

EXECUTIVE SUMMARY

The Cybersecurity Integrity Audit is an integral component of our 5 Pillar Security Strategy. Through comprehensive vulnerability assessments and penetration testing services, your organization can manage risk more effectively by uncovering areas in your technology infrastructure that could represent a threat toward your business health.

By uncovering potentially damaging attack vectors, your IT and security teams can develop a comprehensive mitigation strategy that can bring peace of mind for all stakeholders who are accountable for the sustainability of your security posture.

It is not enough to just examine the perimeter. Your business processes rely on a secure network and secure on-premises and web applications. Do you store content in an on-site repository or in the cloud? Do you have key business processes that leverage SaaS solutions? Public and private cloud services providers utilize proprietary data centers as well as co-locating on proven platforms such as Amazon Web Services and Microsoft® Azure. They often insist that these platforms are secure through routine and in-depth vulnerability assessments and penetration testing and go even further to boast certifications such as ISO/IEC 27001 and SOC 2 audits. But what about the applications that sit on top of these platforms?

The Cybersecurity Integrity Audit can help deliver peace of mind in an uncertain and dangerous cyber landscape. It has assessment levels to fit any organization.

LEVEL 1

Includes an automated scan with a detailed report of findings.

LEVEL 2

Includes an automated scan and also some manual activities with a detailed report.

This option will also include a one-hour debrief via teleconference to explain findings and address any questions.

LEVEL 3

Includes an extensive, all inclusive vulnerability assessment, combination of level 1 & 2 plus a penetration test to demonstrate how an adversary could exploit vulnerability findings.

This would also include a detailed report of findings.

THE CYBERSECURITY INTEGRITY AUDIT VOUCHER* PROGRAM

The Cybersecurity Integrity Audit is funded through a special voucher program in conjunction with our cybersecurity services provider, Agile Cybersecurity Solutions (ACS). During an initial needs assessment consultation, ACS will scope the project at the appropriate level and then furnish a comprehensive Statement of Work (SOW).

ABOUT ACS

Established in 2012, ACS has become a trusted leader in cybersecurity. Their unique combination of proven methodologies and multi-disciplined cyber expertise forms a proactive, end-to-end cybersecurity solution. ACS consists of a team of expert cybersecurity practitioners that can help to build a strong defense against the cyber threat, and also to keep you one step ahead of it.

***Note:** The Cybersecurity Integrity Audit Voucher does not constitute a legal contract; it is merely a method of funding the SOW. Vouchers will expire if not used in 5 years. If after the needs assessment consultation the SOW exceeds the value of the voucher, it will require supplemental funding to proceed with the audit.*

CYBERSECURITY INTEGRITY AUDIT IN DETAIL

VULNERABILITY ASSESSMENT

The objective of a vulnerability assessment is to validate host configurations and produce a list of known vulnerabilities existing on in-scope systems. The testing includes manual validation of vulnerabilities to reduce false positives.

Pre-Engagement

During the initial scheduling and kickoff sessions, the rules of engagement for the testing are established. Topics to be covered include:

- Goals and objectives for the testing.
- Definition of scope and validation of targets.
- Testing timelines and schedules.
- Rules of engagement, levels of effort, and risk acceptance.
- Reporting requirements and deliverables, timelines, and milestones.
- Key personnel, roles and responsibilities, escalation rules, and emergency planning.
- ACS source IP address ranges, tools, and techniques.

The consultant will send a confirmation email following project kickoff to ensure agreement on these topics.

Execution

A technical network security assessment is designed to identify critical flaws in your network that an attacker could exploit. Testing may include any networked device, including firewalls, routers, or other network infrastructure devices; intrusion detection and prevention systems; web servers; email systems; virtual private networking (VPN) systems; etc. We may use a combination of automated and manual scanning with commercial and publicly available tools, as well as custom scripts and applications that ACS has developed.

The types of vulnerabilities typically detected by this testing include:

- Microsoft® Windows, Linux® operating systems, and Unix® operating system vulnerabilities and patches.
- Known and published host application and service vulnerabilities, such as Apache®, Microsoft Internet Information Services (IIS), IBM® WebSphere®, etc.
- Simple Mail Transfer Protocol (SMTP) email servers.
- Remote access services, such as SSH, Telnet, RDP.
- Other servers, such as NTP, FTP, SSL wrappers, etc.
- Network device vulnerabilities, such as firewalls, VPNs, routers.
- Thousands of other vulnerabilities.

Automated tools can greatly assist in reducing work effort and costs associated with repetitive and time-consuming tasks, but manual techniques and analysis are also performed in each step to have the greatest understanding of your environment. Manual validation of findings reduces false positives; manual vulnerability testing reduces false negatives. False positives on a report lead to wasted effort in remediation. False negatives can expose an organization to risk of intrusion.

Vulnerability Assessment Step 1 – Scope Validation

ACS will validate the target list provided. This is a safety measure and will ensure the accuracy of subsequent findings. ACS may perform such activities as:

- Ping sweeps, port scans, and route tracing.
- Footprinting of networks and systems.
- Internet domain name registration searches.
- Internet registry number searches.
- Domain name system (DNS) lookups.

Vulnerability Assessment Step 2 – Enumeration and Vulnerability Mapping

Enumeration involves actively trying to identify running services, used applications, version numbers, service banners, etc. Testing in this phase is at a more noticeable level of activity, which might reveal that we are performing reconnaissance activities that typically precede an attack.

In vulnerability mapping, ACS will take what has been learned about the environment and attempt to determine vulnerabilities that are present. Some vulnerabilities will be apparent using only the information learned from the first two steps. However, many vulnerabilities can only be investigated with probe-and-response testing. In this test, we send data to a service or application and look for a certain response that indicates a possible vulnerability.

Automated scanning tools occasionally fail to report some vulnerabilities, so we conduct additional manual testing, which does not rely on automated scanning. A testing methodology that solely relies on automated scan results can give a false sense of security.

Vulnerability Assessment Step 3 – Manual Verification

Automated scanning tools often report false positives, which are reported vulnerabilities that are not actually present. For vulnerabilities discovered through automated scanning, we take steps to ensure that report findings are an accurate representation of your environment. Without this often-overlooked step, time may be wasted attempting to remediate vulnerabilities that don't exist.

A Note on Web Applications

Web applications are characteristically the most vulnerable applications, and ACS has services designed to thoroughly test and assess web application security. If we find web applications in IP address range within scope for this project, we will perform testing on the web application server, not on the application itself. This testing should not be considered a comprehensive or focused test of your web application.

PENETRATION TESTING

Penetration testing is included at Level 3

Very similar to a vulnerability assessment, the objective of a penetration test is to validate host and network configurations and produce a list of known vulnerabilities existing on in-scope systems. A penetration test goes an additional step by exploiting those vulnerabilities to gain access to your email systems, firewalls, routers, VPN tunnels, web servers, and other devices. The testing and exploitation of vulnerabilities reduces false positives and mimics real world attacks.

Key Benefits:

- Identify security risks: our security experts identify the information assets at risk.
- Identify test readiness: depending on your maturity, these testing services help address your security.
- Meet compliance: experienced testers understand compliance requirements.
- Improve security: obtain a prioritized list of actionable items to address.

Pre-Engagement

A critical component of an ACS engagement is to clearly establish and agree to the rules of engagement. During the initial scheduling and kickoff sessions, the rules of engagement for the testing are established. Topics to be covered include:

- Goals and objectives for the testing.
- Definition of scope and validation of targets.
- Testing timelines and schedules.
- Rules of engagement, levels of effort, and risk acceptance.
- Reporting requirements and deliverables, timelines, and milestones.
- Key personnel, roles and responsibilities, escalation rules, and emergency planning.
- ACS source IP address ranges, tools, and techniques.

The consultant will send a confirmation email following project kickoff to ensure agreement on these topics.

Execution

A technical network security assessment is designed to identify critical flaws in your network that an attacker could exploit. Testing may include any networked device, including firewalls, routers, or other network infrastructure devices; intrusion detection and prevention systems; web servers; email systems; virtual private networking (VPN) systems; etc. ACS will use a combination of automated and manual scanning with commercial and publicly available tools, as well as custom scripts and applications that we has developed.

The types of vulnerabilities typically detected by this testing include:

- Microsoft Windows, Linux, and Unix operating system vulnerabilities and patches.
- Known and published host application and service vulnerabilities, such as Apache, Microsoft Internet Information Services (IIS), IBM WebSphere, etc.
- Simple Mail Transfer Protocol (SMTP) email servers.
- Remote access services, such as SSH, Telnet, RDP.
- Other servers, such as NTP, FTP, SSL wrappers, etc.
- Network device vulnerabilities, such as firewalls, VPNs, routers.
- Thousands of other vulnerabilities.

Automated tools can greatly assist in reducing work effort and costs associated with repetitive and time-consuming tasks, but manual techniques and analysis are also performed in each step to have the greatest understanding of your environment. Manual validation of findings reduces false positives; manual vulnerability testing reduces false negatives. False positives on a report lead to wasted effort in remediation. False negatives can expose an organization to risk of intrusion.

Penetration Testing Step I: Scope Validation

ACS will validate the target list provided. This is a safety measure and will ensure the accuracy of subsequent findings. ACS may perform such activities as:

- Ping sweeps, port scans, and route tracing.
- Footprinting of networks and systems.
- Internet domain name registration searches.
- Internet registry number searches.
- Domain name system (DNS) lookups.

Penetration Testing Step II: Enumeration and Vulnerability Mapping

Enumeration involves actively trying to identify running services, used applications, version numbers, service banners, etc. Testing in this phase is at a more noticeable level of activity, which might reveal that we are performing reconnaissance activities that typically precede an attack.

In vulnerability mapping, ACS will take what has been learned about the environment and attempt to determine vulnerabilities that are present. Some vulnerabilities will be apparent using only the information learned from the first two steps. However, many vulnerabilities can only be investigated with probe-and-response testing. In this test, we send data to a service or application and look for a certain response that indicates a possible vulnerability.

Automated scanning tools occasionally fail to report some vulnerabilities, so we conduct additional manual testing, which does not rely on automated scanning. A testing methodology that solely relies on automated scan results can give a false sense of security.

Penetration Testing Step III: Vulnerability Validation and Exploitation

Automated scanning tools often report false positives, which are reported vulnerabilities that are not actually present. For vulnerabilities discovered through automated scanning, we take steps to ensure that report findings are an accurate representation of your environment. Without this often-overlooked step, time may be wasted attempting to remediate vulnerabilities that don't exist.

The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions. The goal is to further validate vulnerabilities by executing known exploits and observing the results. ACS will devise and develop possible attacks and testing methods. We will give more emphasis to attacks that cannot or typically have not been carried out by automated means, as well as those that would expose you to the highest risk (reputation, direct loss, liability, compliance) if compromised by a malicious attacker.

As appropriate, testing will include various attacks, such as buffer overflows, format string attacks, arbitrary code execution, and default credentials. We may also attempt customized attacks, which may be unique to your systems or configurations. However, we will not perform Denial of Service (DoS) attacks, brute forcing passwords, complex password guessing, or other high-impact/low-value testing without specific written approval.

Canon

CANON SOLUTIONS AMERICA

1-800-815-4000 CSA.CANON.COM/SECURITY

Canon Solutions America does not provide legal counsel or regulatory compliance consultancy, including without limitation, Sarbanes-Oxley, HIPAA, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Some security features may impact functionality/performance; you may want to test these settings in your environment.

Canon Solutions America, Inc. ("CSA"), is compensated to refer prospective customers to our cybersecurity providers ("Provider"). Customer acknowledges and agrees that: (i) Provider will provide products and services to you pursuant to an agreement between you and Provider; (ii) CSA shall have no obligation or liability therefore; (iii) you shall look solely to Provider as to any claim or cause of action arising from such products and services, or your agreement with Provider; and (iv) you waive your rights to bring any such claim or cause of action against CSA.

Neither Canon Inc., nor Canon U.S.A., Inc., nor Canon Solutions America represents or warrants any third-party product or feature referenced hereunder. Canon is a registered trademark of Canon Inc. in the United States and may also be a registered trademark or trademark in other countries. All other referenced product names and marks are trademarks of their respective owners. Specifications and availability subject to change without notice. Not responsible for typographical errors.