KEYPOINT INTELLIGENCE

CYBERSECURITY INTEGRITY AUDIT

Mitigating Risk through Comprehensive Assessments

KEYPOINT INTELLIGENCE
80 Little Falls Road
Fairfield, NJ 07004
TEL: +1 973 797 2100
keypointintelligence.com

YOU CAN'T PROTECT AGAINST WHAT YOU CAN'T SEE

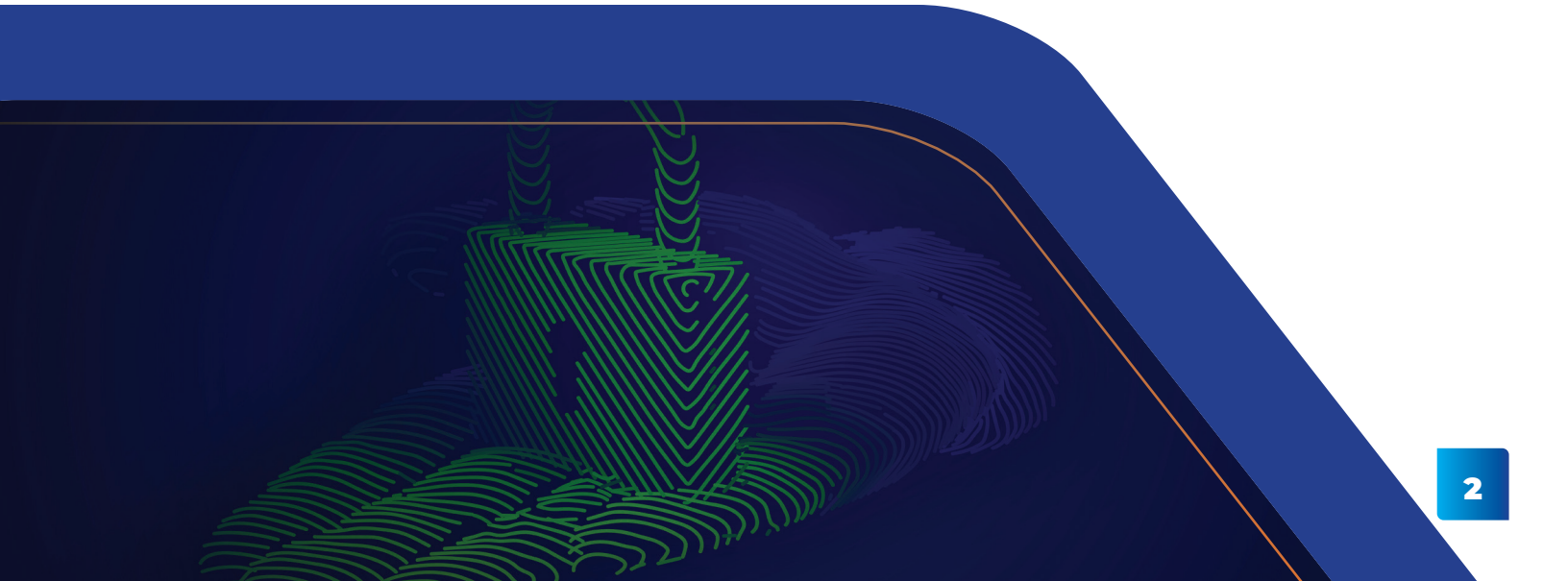
The Cybersecurity Integrity Audit can help to expose vulnerabilities, thus enabling organizations to more effectively manage risk.

Executive Summary

The Cybersecurity Integrity Audit (CIA) is an integral component of any IT security plan. 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 and Level 2, plus a penetration test to demonstrate how an adversary could exploit vulnerability findings.

This would also include a detailed report of findings.

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
- Keypoint Intelligence 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 Keypoint Intelligence partners have 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

Keypoint Intelligence will validate the target list provided. This is a safety measure and will ensure the accuracy of subsequent findings. Keypoint Intelligence 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, Keypoint Intelligence 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

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.

Web applications are characteristically the most vulnerable applications, and Keypoint Intelligence 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 Keypoint Intelligence 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:

The types of vulnerabilities typically detected by this testing 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
- Keypoint Intelligence source IP address ranges, tools, and techniques

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. Keypoint Intelligence 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

Keypoint Intelligence will validate the target list provided. This is a safety measure and will ensure the accuracy of subsequent findings. Keypoint Intelligence 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, Keypoint Intelligence 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.


KEYPOINT
INTELLIGENCE
keypointintelligence.com