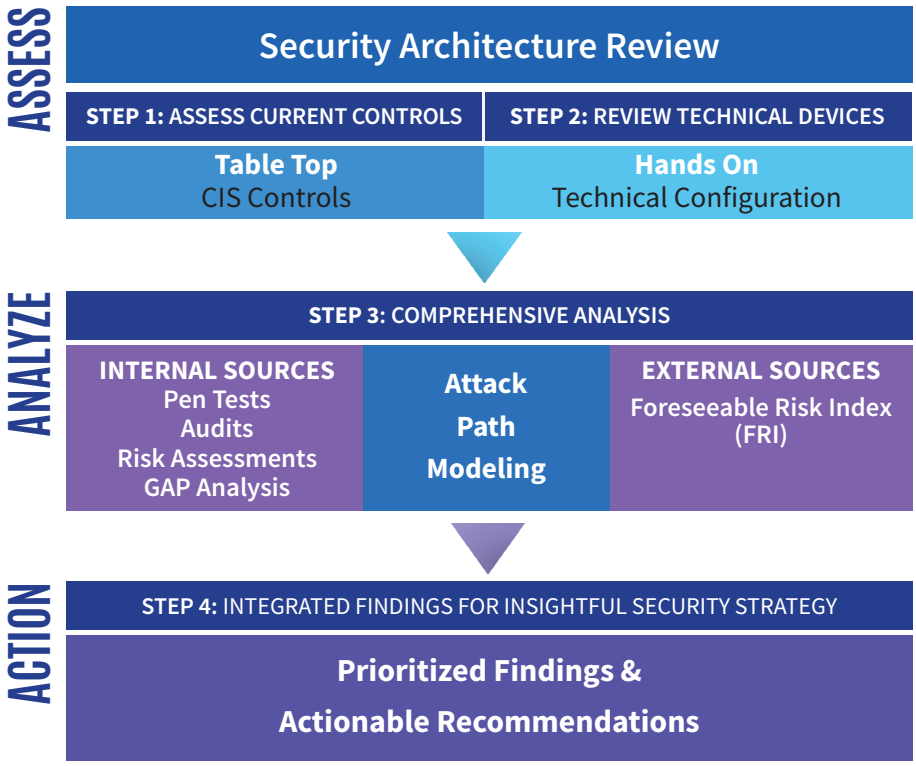
THREAT-BASED SECURITY ARCHITECTURE ANALYSIS

How are your controls performing against the threats that are affecting your peers?

Identifying priorities and justifying improvements is made easier with **HALOCK's Threat-based Security Architecture Analysis**. Understanding maturity of your controls is not enough. Leveraging the Foreseeable Risk Index ("FRI"), HALOCK reviews your controls in the context of industry specific threats. HALOCK also incorporates previous diagnostics made available including; gap assessments, penetration tests, risk assessments, incident reports and compliance audits.

Combining all this data offers a comprehensive look at how best to refine your specific security strategy.

BUILD YOUR DIAGNOSTIC



Simplify the complex. Consolidate the process.

HALOCK streamlines your security architecture review workflow. We collect information on your current security processes and analyze your posture against our **Foreseeable Risk Index (FRI)** data to gauge your risks, to develop security recommendations based on your specific environment.

THREAT-BASED SECURITY ARCHITECTURE ANALYSIS

Critical Security Controls Evaluated

BASIC

1 Inventory and Control of Hardware Assets
2 Inventory and Control of Software Assets
3 Continuous Vulnerability Management
4 Controlled Use of Administrative Privileges
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6 Maintenance, Monitoring and Analysis of Audit Log

FOUNDATIONAL

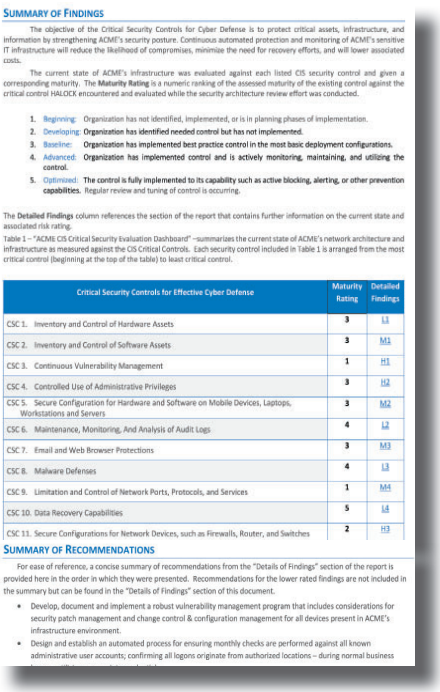
7 Email and Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports, Protocols and Services
10 Data Recovery Capabilities
11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring and Control

ORGANIZATIONAL

17 Implement a Security Awareness and Training Program
18 Application Software Security
19 Incident Response and Management
20 Penetration Tests and Red Team Exercises

Security Architecture & Attack Path Report

Understand your security landscape easily with a full report on findings of your current environment and how to make it better. Your report offers an Executive Summary, Details of Findings, and Attack Path Modeling to give you the full picture.



SUMMARY OF FINDINGS

The objective of the Critical Security Controls for Cyber Defense is to protect critical assets, infrastructure, and information by strengthening ACME's security posture. Continuous automated protection and monitoring of ACME's sensitive IT infrastructure will reduce the likelihood of compromises, minimize the need for recovery efforts, and will lower associated costs.

The current state of ACME's infrastructure was evaluated against each listed CIS security control and given a corresponding maturity. The **Maturity Rating** is a numeric ranking of the assessed maturity of the existing control against the critical control HALOCK encountered and evaluated while the security architecture review effort was conducted.

1. Beginning: Organization has not identified, implemented, or is in planning phases of implementation.
2. Developing: **Organization has identified needed control but has not implemented.**
3. Baseline: **Organization has implemented best practice control in the most basic deployment configurations.**
4. Advanced: **Organization has implemented control and is actively monitoring, maintaining, and utilizing the control.**
5. Optimized: **The control is fully implemented to its capability such as active blocking, alerting, or other prevention capabilities.** Regular review and tuning of control is occurring.

The **Detailed Findings** column references the section of the report that contains further information on the current state and associated risk rating.

Table 1 – "ACME CIS Critical Security Evaluation Dashboard" –summarizes the current state of ACME's network architecture and infrastructure as measured against the CIS Critical Controls. Each security control included in Table 1 is arranged from the most critical control (beginning at the top of the table) to least critical control.

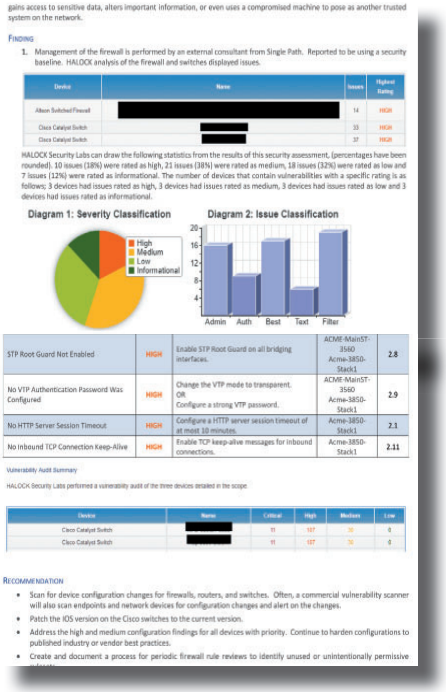
Critical Security Controls for Effective Cyber Defense	Maturity Rating	Detailed Findings
CSC 1. Inventory and Control of Hardware Assets	3	I1
CSC 2. Inventory and Control of Software Assets	3	M1
CSC 3. Continuous Vulnerability Management	1	H1
CSC 4. Controlled Use of Administrative Privileges	3	H2
CSC 5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	3	M2
CSC 6. Maintenance, Monitoring, And Analysis of Audit Logs	4	L2
CSC 7. Email and Web Browser Protections	3	M3
CSC 8. Malware Defenses	4	L3
CSC 9. Limitation and Control of Network Ports, Protocols, and Services	1	M4
CSC 10. Data Recovery Capabilities	5	L4
CSC 11. Secure Configurations for Network Devices, such as Firewalls, Router, and Switches	2	H3

SUMMARY OF RECOMMENDATIONS

For ease of reference, a concise summary of recommendations from the "Details of Findings" section of the report is provided here in the order in which they were presented. Recommendations for the lower rated findings are not included in the summary but can be found in the "Details of Findings" section of this document.

- Develop, document and implement a robust vulnerability management program that includes considerations for security patch management and change control & configuration management for all devices present in ACME's infrastructure environment.
- Design and establish an automated process for ensuring monthly checks are performed against all known administrative user accounts; confirming all logons originate from authorized locations – during normal business

Executive Summary



gains access to sensitive data, alters important information, or even uses a compromised machine to pose as another trusted system on the network.

FINDING

1. Management of the firewall is performed by an external consultant from Single Path. Reported to be using a security baseline. HALOCK analysis of the firewall and switches displayed issues.

Device	Name	Issues	Highest Rating
Alison Switched Firewall	[redacted]	14	HIGH
Cisco Catalyst Switch	[redacted]	33	HIGH
Cisco Catalyst Switch	[redacted]	37	HIGH

HALOCK Security Labs can draw the following statistics from the results of this security assessment, (percentages have been rounded). 10 issues (18%) were rated as high, 21 issues (38%) were rated as medium, 18 issues (32%) were rated as low and 7 issues (12%) were rated as informational. The number of devices that contain vulnerabilities with a specific rating is as follows; 3 devices had issues rated as high, 3 devices had issues rated as medium, 3 devices had issues rated as low and 3 devices had issues rated as informational.

Diagram 1: Severity Classification

Diagram 2: Issue Classification

STP Root Guard Not Enabled	HIGH	Enable STP Root Guard on all bridging interfaces.	ACME-MainST-3560 Acme-3850-Stack1 2.8
No VTP Authentication Password Was Configured	HIGH	Change the VTP mode to transparent. OR Configure a strong VTP password.	ACME-MainST-3560 Acme-3850-Stack1 2.9
No HTTP Server Session Timeout	HIGH	Configure a HTTP server session timeout of at most 10 minutes.	Acme-3850-Stack1 2.1
No Inbound TCP Connection Keep-Alive	HIGH	Enable TCP keep-alive messages for inbound connections.	Acme-3850-Stack1 2.11

Vulnerability Audit Summary

HALOCK Security Labs performed a vulnerability audit of the three devices detailed in the scope.

Device	Name	Critical	High	Medium	Low
Cisco Catalyst Switch	[redacted]	11	127	70	6
Cisco Catalyst Switch	[redacted]	11	127	70	6

RECOMMENDATION

- Scan for device configuration changes for firewalls, routers, and switches. Often, a commercial vulnerability scanner will also scan endpoints and network devices for configuration changes and alert on the changes.
- Patch the IOS version on the Cisco switches to the current version.
- Address the high and medium configuration findings for all devices with priority. Continue to harden configurations to published industry or vendor best practices.
- Create and document a process for periodic firewall rule reviews to identify unused or unintentionally permissive

Details of Findings

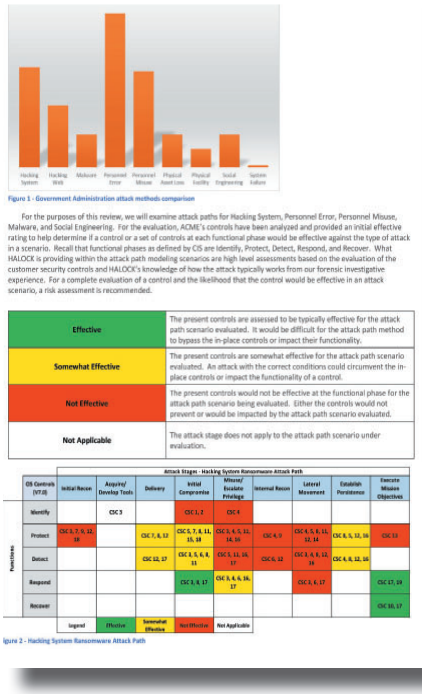


Figure 1 - Government Administration attack methods comparison

For the purposes of this review, we will examine attack paths for Hacking System, Personnel Error, Personnel Misuse, Malware, and Social Engineering. For the evaluation, ACME's controls have been analyzed and provided an initial effective rating to help determine if a control or a set of controls at each functional phase would be effective against the type of attack in a scenario. Recall that functional phases as defined by CIS are Identify, Protect, Detect, Respond, and Recover. What HALOCK is providing within the attack path modeling scenarios are high level assessments based on the evaluation of the customer security controls and HALOCK's knowledge of how the attack typically works from our forensic investigative experience. For a complete evaluation of a control and the likelihood that the control would be effective in an attack scenario, a risk assessment is recommended.

Effective	The present controls are assessed to be typically effective for the attack path scenario evaluated. It would be difficult for the attack path method to bypass the in-place controls or impact their functionality.
Somewhat Effective	The present controls are somewhat effective for the attack path scenario evaluated. An attack with the correct conditions could circumvent the in-place controls or impact the functionality of a control.
Not Effective	The present controls would not be effective at the functional phase for the attack path scenario being evaluated. Either the controls would not prevent or would be impacted by the attack path scenario evaluated.
Not Applicable	The attack stage does not apply to the attack path scenario under evaluation.

Figure 2 - Hacking System Ransomware Attack Path

Attack Path Modeling

HALOCK INDUSTRY THREAT (HIT) INDEX

HALOCK Security Labs' HIT analyzes breach data from the public domain, and from HALOCK's incident response findings. The FRI provides an evidence-based approach for modeling threats and estimating their likelihood within individual industries.

FRI can be used for risk analysis for any information security framework, including ISO 27000, NIST Special Publications and Cybersecurity Framework, PCI DSS, and CIS Controls.