HALOCK®

RISK-BASED THREAT ASSESSMENT

Before the risk becomes an attack.

A ransomware attack takes place every 14 seconds. Nearly one-fourth of data breaches can be attributed to web application attacks. There is a notable increase globally across attack vectors and it is your team's responsibility to manage the potential risks. How do you verify your resiliency in the event of a cyber attack?

Identifying the likely threats to your organization is the best approach to prepare and protect. Regular reviews establish a baseline of your controls and performance, and a method to improve your security posture and fix any vulnerabilities.

Informed Risk Management

As cyberthreats continue to evolve and become more sophisticated, you require a comprehensive look at how to enhance your protection against the five MITRE ATT&CK Types listed in Center for Internet Security's Community Defense Model. The **HALOCK Risk-Based Threat Assessment**, using HALOCK's ***Duty of Care Risk Analysis (DoCRA) methodology***, combines security guidance from Center for Internet Security, Inc. (CIS®), MITRE, The National Institute of Standards and Technology (NIST), and the VERIS Community Database (VCDB) to provide this unique offering.

With the Risk-Based Threat Assessment, organizations can prioritize security controls to enhance or implement using the best threat data the cybersecurity community offers. This results in budget and resource efficiencies by addressing the security areas of highest concern and in order of importance, to increase your resilience to cyber attacks.

Improve protection against the five MITRE ATT&CK Types:

- Ransomware attack
- Malware attack
- Insider Abuse attack
- Web App attack
- Persistent External attack

Why Choose HALOCK?

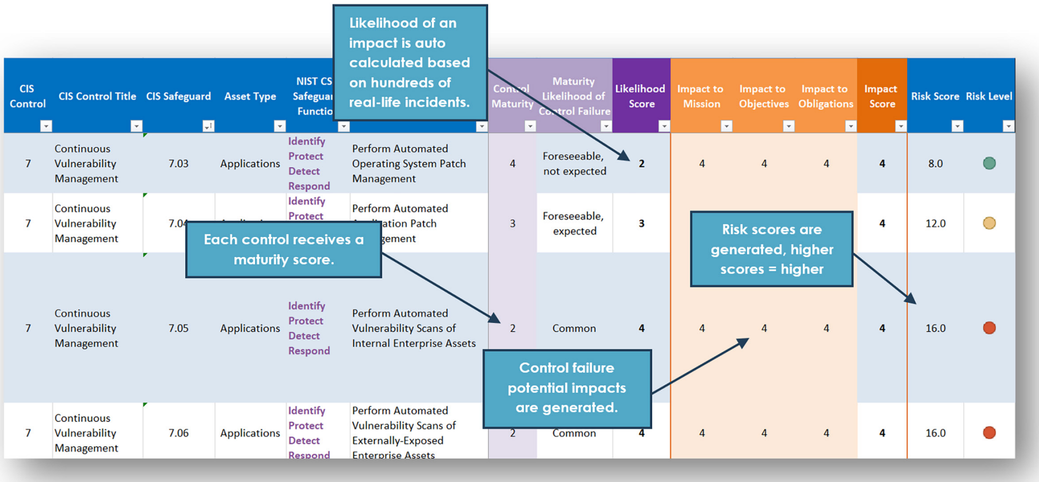
As authors of the DoCRA Standard and developers of CIS RAM, HALOCK has specialized insight to guide you through a risk method to establish reasonable and appropriate security.

Risk expertise like no other.

The Methodology and Deliverables

This DoCRA based threat assessment includes interviews with your organization's personnel using the CIS Critical Security Controls (CIS Controls) to understand how your security is currently deployed.

A **risk register** will be created and each applicable CIS control scored.



CIS Control	CIS Control Title	CIS Safeguard	Asset Type	NIST CS Safeguard Functio		Control Maturity	Maturity Likelihood of Control Failure	Likelihood Score	Impact to Mission	Impact to Objectives	Impact to Obligations	Impact Score	Risk Score	Risk Level
7	Continuous Vulnerability Management	7.03	Applications	Identify Protect Detect Respond	Perform Automated Operating System Patch Management	4	Foreseeable, not expected	**2**	4	4	4	**4**	8.0	●
7	Continuous Vulnerability Management	7.04	Applications	Identify Protect	Perform Automated Application Patch Management	3	Foreseeable, expected	**3**				**4**	12.0	●
7	Continuous Vulnerability Management	7.05	Applications	Identify Protect Detect Respond	Perform Automated Vulnerability Scans of Internal Enterprise Assets	2	Common	**4**	4	4	4	**4**	16.0	●
7	Continuous Vulnerability Management	7.06	Applications	Identify Protect Detect Respond	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	2	Common	**4**	4	4	4	**4**	16.0	●

Likelihood of an impact is auto calculated based on hundreds of real-life incidents.

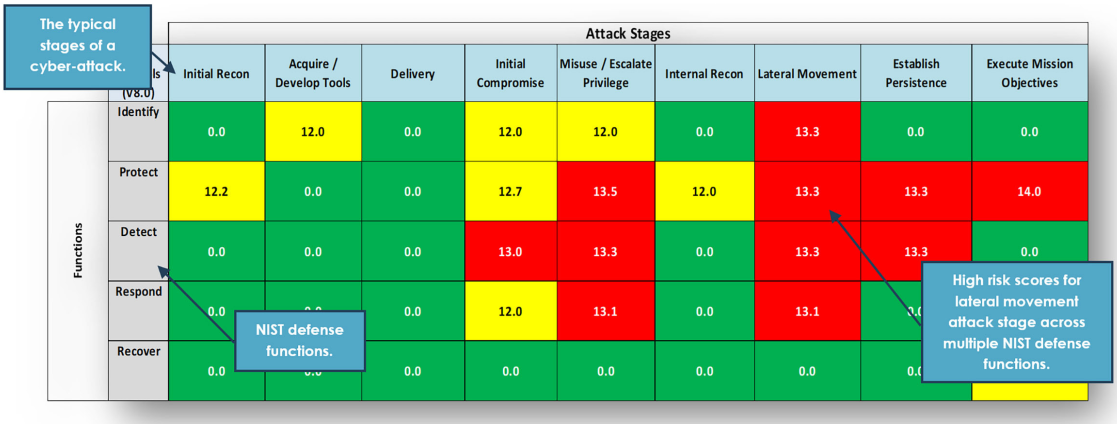
Each control receives a maturity score.

Risk scores are generated, higher scores = higher

Control failure potential impacts are generated.

Risk Register

Using the scores generated from the risk register, a **heat map** will be created for each attack type identifying the vulnerabilities that impose the greatest threat to your organization.



		Attack Stages								
	ls (V8.0)	Initial Recon	Acquire / Develop Tools	Delivery	Initial Compromise	Misuse / Escalate Privilege	Internal Recon	Lateral Movement	Establish Persistence	Execute Mission Objectives
Functions	Identify	0.0	12.0	0.0	12.0	12.0	0.0	13.3	0.0	0.0
	Protect	12.2	0.0	0.0	12.7	13.5	12.0	13.3	13.3	14.0
	Detect	0.0	0.0	0.0	13.0	13.3	0.0	13.3	13.3	0.0
	Respond	0.0	0.0	0.0	12.0	13.1	0.0	13.1	0.0	[illegible]
	Recover	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	[illegible]

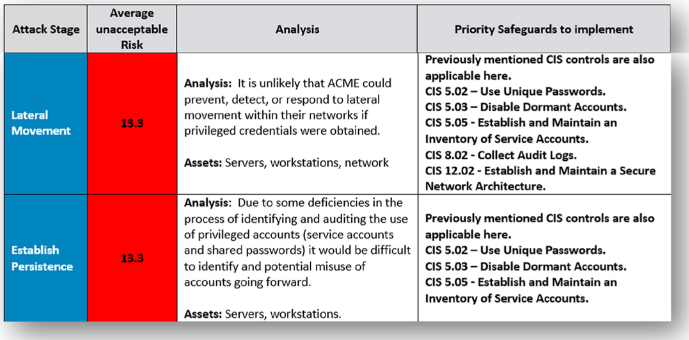
The typical stages of a cyber-attack.

NIST defense functions.

High risk scores for lateral movement attack stage across multiple NIST defense functions.

Heat Map/Attack Path Average Unacceptable Risk Scores

Analysis and recommendations are provided at each stage to give you the priority road map to improve your risk posture.



Attack Stage	Average unacceptable Risk	Analysis	Priority Safeguards to implement
Lateral Movement	13.3	**Analysis:** It is unlikely that ACME could prevent, detect, or respond to lateral movement within their networks if privileged credentials were obtained. **Assets:** Servers, workstations, network	**Previously mentioned CIS controls are also applicable here.** **CIS 5.02 – Use Unique Passwords.** **CIS 5.03 – Disable Dormant Accounts.** **CIS 5.05 - Establish and Maintain an Inventory of Service Accounts.** **CIS 8.02 - Collect Audit Logs.** **CIS 12.02 - Establish and Maintain a Secure Network Architecture.**
Establish Persistence	13.3	**Analysis:** Due to some deficiencies in the process of identifying and auditing the use of privileged accounts (service accounts and shared passwords) it would be difficult to identify and potential misuse of accounts going forward. **Assets:** Servers, workstations.	**Previously mentioned CIS controls are also applicable here.** **CIS 5.02 – Use Unique Passwords.** **CIS 5.03 – Disable Dormant Accounts.** **CIS 5.05 - Establish and Maintain an Inventory of Service Accounts.**

Report Analysis

The Risk-Based Threat Assessment

can be a one-time project or an annual program to continually model threats.

You can choose 1 or up to all 5 attack types for the assessment. Clients can use a previously completed risk register or initiate a new one.

Prioritize Remediation Using What Matters Most To You:

Maturity of security controls and NIST CSF Security Functions

Risks associated with security controls

MITRE ATT&CK Types

Your roadmap from current risks to 'reasonable' controls