RADICL™

How SMBs Can Implement Cyber-HDR for Increased Protection and Reduced Risk

RADICL POV

INTRODUCTION

Companies seeking true protection from advanced cyber threats must adopt a cybersecurity Harden-Detect-Respond (cyber-HDR) operation. Nation-State sponsored cyber espionage units are actively targeting American companies driving innovation (i.e., AI, biotech) and supporting the defense industry. Companies are also increasingly feeling the impact of cybercrime with 46% of SMBs experiencing $100K+ in costs associated with cybersecurity incidents[1].

The adoption of a cyber-HDR operation materially reduces the risk of experiencing intellectual property (IP) theft, ransomware, financial fraud, and other cyber-related incident risks. For years, large enterprises have been maturing their cyber-HDR operation, investing in the layers of defense backed by modern technology and well-staffed teams. SMBs have been left out in the cold due to the cost of achieving cyber-HDR. That is, until now.

RADICL was born with the mission to deliver cyber-HDR operations to SMBs at an affordable price. We care about protecting SMBs driving American innovation and defense. We know how critical cyber-HDR is to defending these businesses. We have intentionally designed our platform to enable us to quickly and seamlessly become your security operations team, to deliver cyber-HDR as a managed offering, powered by our Xtended Threat Protection (XTP) platform and Virtual Security Operations Center (vSOC).

The remainder of this paper describes in more detail what a cyber-HDR operation entails and requires. The RADICL offering has been designed to deliver high-grade HDR to SMBs at a price they can afford. We have achieved this through the development of a proprietary technology platform that leverages analytics and automation to amplify and accelerate the efforts of our vSOC team.

This paper also describes what it takes to build out and staff a modern and capable cyber-HDR operation, equivalent to what large enterprises have established for themselves, or that RADICL can provide as a managed offering. The practical reality is that most SMBs cannot afford to build out such an operation and will instead rely on a third-party Managed Service Provider (MSP). This paper should provide helpful guidance in evaluating the efficacy of third-party providers by better understanding what a high-quality cyber-HDR operation should look like.

1. DIB Cybersecurity Maturitey Report | 2024

HARDEN CRITICAL CAPABILITIES DEFINED

Hardening consists of shrinking your attack surface, making it harder for an adversary to penetrate the environment and expand their footprint. There are three principal operational capabilities critical to making your business harder to attack.

SERVER AND WORKSTATION PROTECTION

User workstations are at the edge of your IT perimeter. They are often mobile and find themselves in untrusted environments like homes, cafés, and hotels. Depending on the business, server infrastructure, whether physical or cloud, may also be directly exposed to the internet. Servers also house the data threat actors are often after, or keys to that data. Servers and workstations must be protected by modern and advanced technology able to block known and emerging avenues of attack.

PRINCIPAL OPERATIONS

1. Deploying protection and monitoring technology agents on end-user systems.
2. Deploying protection and monitoring technology physical, virtual, and cloud server infrastructure.
3. Managing threat detection policies and custom detection content.

SECURITY AWARENESS TRAINING

People and their credentials have access to workstations, IT infrastructure, and data. Poor cybersecurity hygiene can open them up to personal or professional attack that can ultimately lead to system or data compromise. Social engineering attacks like phishing can cause them to make mistakes that result in systems or account compromise. Employees need to be continuously trained on modern cybersecurity practices and tested to ensure they can stand up to targeted and creative AI-augmented social engineering attacks.

PRINCIPAL OPERATIONS

1. Training new and existing employees on fundamental concepts.
2. Providing ongoing training exercises to introduce new and reinforce existing concepts.
3. Provide simulated social engineering attacks to test training effectiveness and employee resiliency.

VULNERABILITY MANAGEMENT

Vulnerabilities, whether they be out-of-date software or a system misconfiguration, are constantly being introduced. On an ongoing basis, vulnerabilities need to be identified and cataloged. Vulnerabilities presenting the highest risk of exploitation need to be prioritized for remediation. Remediation efforts need to be tracked and managed across time to ensure work is being done as expected and required.

PRINCIPAL OPERATIONS

1. Identifying IT vulnerabilities and weaknesses through continuous monitoring and scanning techniques.
2. Cataloging, prioritizing, and reporting on vulnerabilities based on business risk.
3. Coordinating and facilitating vulnerability remediation efforts with IT.

DETECT CRITICAL CAPABILITIES DEFINED

VISIBILITY

The only way to detect the myriad of Tactics, Techniques, and Procedures (TTPs) threat actors will leverage is by increasing visibility into the IT and cloud environment. Log, event, and alert data needs to be centrally collected, processed, and enriched to support effective security analytics. Foundational visibility includes: endpoint activity, authentication activity, data access activity, and data movement.

PRINCIPAL OPERATIONS

1. Integrating data sources for centralized visibility.
2. Developing and maintaining data enrichment policies.
3. Monitoring the health of data sources and rapidly responding to visibility disruption.

DETECTION ANALYTICS

The first priority for detection analytics is ensuring already deployed endpoint and network security solutions are properly configured to detect the type of TTPs they have visibility into. Next up is developing and deploying advanced detection rules that sit on top of your visibility layer. The final layer of detection defense is the deployment of anomaly detection that can identify shifts in user or IT behavior that might indicate an embedded threat is persistent within the environment. The ultimate objective for detection analytics is to achieve comprehensive TTP coverage as measured against frameworks like MITRE ATT&CK.

PRINCIPAL OPERATIONS

1. Tuning detection policies on existing endpoint, network, and infrastructure security systems.
2. Tuning vendor-supplied detection analytics content per business and IT environment uniqueness.
3. Monitoring threat intelligence sources and developing bespoke analytics content as appropriate.

THREAT HUNTING

The unfortunate reality is that many companies are currently compromised and don't realize it. If you are a company doing interesting and valuable work to nation-state spies, backdoors may already be in place. The surest way to find and kill embedded threats before data is stolen or operations are disrupted is to proactively hunt for them. Threat hunting leverages the experience and intuition of human "threat hunters." These threat hunters will leverage the visibility layer along with threat intelligence channels to search deeply within the IT environment and hunt for any indicator of compromise.

PRINCIPAL OPERATIONS

1. Monitoring threat intelligence channels and TTP sources to identify threats most likely to target the business.
2. Developing and executing hunt campaigns to look for indicators of compromise within the IT environment.
3. Translating observations and lessons learned into automated detection analytics - when technologically feasible.

RESPOND CRITICAL CAPABILITIES DEFINED

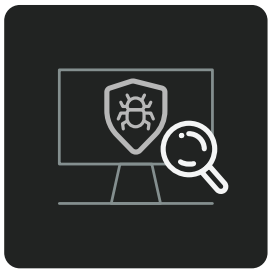
24X7 MONITORING

Threat actors don't take weekends and holidays off. High risk indicators of intrusion and compromise must be evaluated within minutes, whatever time of day or day of the week they occur. According to the recent 2024 CrowdStrike Global Threat Report, the average 'breakout' time for a threat actor to begin moving laterally after gaining initial access to a network was 62 minutes in 2023. The fastest observed breakout time was only 2 minutes and 7 seconds. 24x7 monitoring requires infrastructure and staff to be in place to ensure someone is at the ready to quickly triage and investigate alarms, regardless the day and time they occur. Investing in advanced endpoint, network, and cloud security products only takes you so far if nobody is ready to respond in the event of an alarm.

PRINCIPAL OPERATIONS

1	Managing and tuning 24x7 response orchestration and notification technology (e.g., Pager Duty).
2	Managing 24x7 staff rotation and adjusting as necessary for sickness and retention risk.
3	Responding to and triaging alarms within a timeframe appropriate to the prioritized risk.

THREAT INVESTIGATION



When potential incidents are identified, whether through detection analytics or threat hunting, they must be thoroughly and completely investigated. A compromised endpoint can quickly lead to compromised accounts that are then used to quickly compromise other systems and accounts. Attackers will also seek to quickly plant back doors. Threat investigation leverages the visibility layer to understand what happened when and by whom, and assess whether an actual incident has occurred. If so, investigation continues until the full scope of impact has been determined.

PRINCIPAL OPERATIONS

1	Forensic analysis of endpoint activity pertaining to the (potential) incident.
2	Log analysis across other systems involved in the (potential) incident.
3	Recording investigation activity and capturing evidence.

INCIDENT RESPONSE

When an incident has occurred, time is of the essence. The longer a threat is allowed to exist within the environment, the more expensive they become to dislodge. Operational and business risk quickly accelerate as well. Threat actor access to the IT environment must be quickly severed. Once this has been achieved, clean-up efforts can begin. It will also be important to determine whether data containing personal identification information (PII) has been compromised and if so, whether legal implications exist. Based on the scale of compromise, this may take hours or weeks. In some situations (e.g., ransomware, PII compromise), a third-party incident response (IR) firm may need to be engaged. A coordinated and complete response plan must be developed and executed. Clear and consistent communications to the executive team and other stakeholders must occur throughout.

PRINCIPAL OPERATIONS

1	Coordinating, guiding, and collaborating with IT in support of incident response operations.
2	Engaging with a third-party IR firm when appropriate, often in concert with the insurer.
3	Communicating with the executive team, legal, and HR as necessary and appropriate.

CYBER HDR AND NIST 800-171/CMMC COMPLIANCE

Compliance regulations like NIST 800-171 require cyber-HDR capabilities. How well these capabilities are operationally achieved makes the difference between being truly protected versus just being compliant. RADICL's cyber-HDR capabilities provide true protection and immediately reduce a company's compliance burden. RADICL reduces the compliance adherence load across 41 of the 110 NIST 800-171 requirements. RADICL's COMPLY module provides managed and guided adherence across the remaining requirements.

Alternatively, customers seeking to achieve compliance might invest in a Governance Risk and Compliance (GRC) platform to help manage and track their compliance journey. They might alternatively or in addition to also engage consulting and advisory services.

BUILDING AND OPERATING A CYBER HDR CAPABILITY

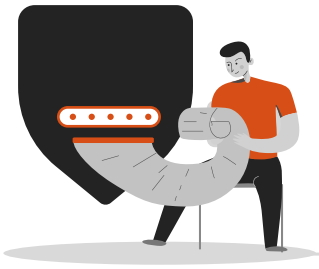
CYBER-HDR ESSENTIAL STAFF

Realizing a cyber-HDR operation requires investment in specialized talent and expertise. The following are the key roles that would need to be filled for effective operations.

SECURITY ENGINEER

SALARY RANGE: $100K – $150K

Security Engineers focus on the integration, operation, and maintenance of the cyber-HDR technology stack. They will deploy and manage agents, onboard data sources, run vulnerability scans, oversee training exercises, configure and tune automation, and much more. The cyber-HDR is a complex and ever evolving technology stack that requires ongoing maintenance and tuning to ensure high efficiency operations and maximally reduce cyber incident risk.



SECURITY ANALYST

SALARY RANGE: $70K – $110K

Security Analysts focus on initial triage and investigation of alerts. Their primary function is to quickly evaluate any indicator of compromise and determine whether further investigation operations are required. Based on experience, they may perform the investigations themself or involve more senior members of the team. On a small team, they often have primary 24x7 on-call duties for around the clock monitoring. Security Analysts are often the most junior member of the team.

THREAT HUNTER

SALARY RANGE: $130K – $200K

Threat Hunters are highly experienced security personnel able to proactively hunt for indicators of threats in the environment. They have deep knowledge of the MITRE ATT&CK framework and the Tactics, Techniques, and Procedures (TTPs) of threat adversaries. This knowledge is transferred into targeted, manual hunts that utilize deep endpoint visibility (via EDR) and log data visibility (via SIEM). Their experience is also translated into threat detection content that may be deployed into EDR/SIEM technology to facilitate automated threat detection.

INCIDENT RESPONDER

SALARY RANGE: $130K – $200K

Incident Responders are highly experienced security personnel who understand how to perform in-depth incident investigations and can manage the incident response process. They are able to perform file system and log analysis across endpoint (via EDR) and enterprise visibility (via SIEM). They also translate their experience into automated routines to expedite future response operations. They also help develop and tune detection content based on knowledge gained via incident investigation and response operations.

STAFF TO OPERATIONAL CAPABILITY MATRIX

The following table identifies the type and amount of staff required to support cyber-HDR operations for a 25 to 250 employee organization.

	CRITICAL CAPABILITY	SECURITY ENGINEER	SECURITY ANALYST	THREAT HUNTER	INCIDENT RESPONDER
HARDEN	ENDPOINT PROTECTION	.1-.5			
	VULNERABILITY MANAGEMENT	.3-.5			
	SECURITY AWARENESS TRAINING	.1			
DETECT	LOG VISIBILITY	.2-.5		.25	
	DETECTION ANALYTICS	.3-.5		.25	
	THREAT HUNTING		.5-.2		
RESPOND	24x7 MONITORING			.25	.5
	INVESTIGATION OPERATIONS			.25	.5
	INCIDENT RESPONSE				
	COMPLIANCE MANAGEMENT	1-2 FTE	.5-2 FTE	1 FTE	1 FTE
		TOTAL FULL TIME EMPLOYEES: 4-7			

CYBER-HDR ESSENTIAL TECHNOLOGIES

Realizing a cyber-HDR operation requires a significant investment in technology and staff. The following is a breakdown of the required investments to build a cyber-HDR operation versus partnering with a company like RADICL who can deliver it all as a turn-key managed offering.

ENDPOINT PROTECTION PLATFORMS (EPP)/ENDPOINT DETECTION AND RESPONSE (EDR)

EPP/EDR can be thought of as the successor to Anti-Virus (AV). Like AV, these platforms deploy agents to endpoints and servers and prevent known malware from being successfully installed. Unlike legacy AV, these platforms leverage AI and threat intelligence to detect novel and emerging threats. They also provide deep forensic visibility into endpoint activity in support of threat hunting and incident response operations.

Example Vendors Include: CROWDSTRIKE SentinelOne TREND MICRO

VULNERABILITY MANAGEMENT (VM) PLATFORMS AND TECHNOLOGIES

EPP/EDR can be thought of as the successor to Anti-Virus (AV). Like AV, these platforms deploy agents to endpoints and servers and prevent known malware from being successfully installed. Unlike legacy AV, these platforms leverage AI and threat intelligence to detect novel and emerging threats. They also provide deep forensic visibility into endpoint activity in support of threat hunting and incident response operations.

Example Vendors Include: tenable RAPID7 Qualys

SECURITY AWARENESS TRAINING (SAT) PLATFORMS

Provide education and awareness to help employees improve their personal cybersecurity "hygiene" and avoid being fooled by social engineering attacks such as phishing. These platforms provide a mix of online courses and continuous exercises to reinforce learnings and simulate attacks.

Example Vendors Include: KnowBe4 NINJIO phishing box

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Provide flexible and powerful collection and enrichment of audit and log data. They have powerful search tools for use in threat hunting, investigation, and incident response. They also include automated detection analytics capabilities for identifying threats requiring cross-data source visibility. Some SIEMS also include capabilities for orchestrating and automating security operations.

Example Vendors Include: splunk> LogRhythm exabeam

SECURITY ORCHESTRATION AUTOMATION AND RESPONSE (SOAR)

Serve to manage and orchestrate threat investigation and incident response. They include case management facilities for tracking and coordinating cross-team activities and capturing forensic evidence. These technologies also include extensive workflow automation capabilities that enable small or large teams to operate more efficiently.

Example Vendors Include: SWIMLANE tines DEVO

	CRITICAL CAPABILITY	EPP/ EDR	VM	SAT	SIEM	SOAR	HDR
HARDEN	ENDPOINT PROTECTION	●	◑				✓
	VULNERABILITY MANAGEMENT		●				✓
	SECURITY AWARENESS TRAINING			●			✓
DETECT	LOG VISIBILITY	◔			●		✓
	DETECTION ANALYTICS	◑			●		✓
	THREAT HUNTING	◑			◑		✓
RESPOND	24x7 MONITORING				◑	●	✓
	INVESTIGATION OPERATIONS	◑			◑	●	✓
	INCIDENT RESPONSE	◑			◑	●	✓

CONCLUSION

Companies that seek to materially reduce their cyber incident risk must invest in mature and ever evolving Cyber-HDR operations. Doing so can be especially daunting for SMBs lacking large cybersecurity budgets and staff.

Most SMBs will have no choice but to outsource these capabilities. When outsourcing, leverage the information shared in this paper to deeply scrutinize the capabilities of any managed service providers. Too often, capabilities can be oversold or under-shared. Dig in! Your cybersecurity posture will only be as strong as your outsourced provider.

Make sure they have the chops.Make sure they are transparent and provide visibility into the actions and operations being performed on your behalf. RADICL wants to see all SMBs serving American defense and prosperity realize a strong cyber-HDR capability.

Whether you work with us, or someone else, demand excellence – protection of your brand and business should require no less.

RADICL™

How SMBs Can Implement Cyber-HDR for Increased Protection and Reduced Risk

RADICL POV