CYBORG SECURITY

THREAT HUNTING ENABLEMENT CASE STUDY

UNITED STATES FINANCIAL SERVICES COMPANY EVOLVES THEIR THREAT HUNTING FROM REACTIVE TO PROACTIVE

This financial services company is a US-based Fortune 500 financial services institution operating consumer and commercial banking operations nationwide, offering its clients a wealth of financial services products including asset management, mortgage, insurance, and securities. It has a highly mature 600-strong cybersecurity function complete with a CTI capability, established blue and red teams, and dedicated teams covering CERT, IT GRC, third-partymanagement, and more.

The organization anticipated that as cyber-attacks grew in complexity, traditional security technologieswould be insufficient to defend their environment.Therefore, they established a threat hunting team thatwould proactively hunt within their networks to discover undetected threats. In order to ensure this team was able to proactively hunt for these threats, the company sought a solution that would feed their team with timely, relevant, and actionable threat hunting and detection content. Cyborg Security, through its HUNTER Platform, was able to provide behavioral hunting and detection content that allowed their teamsto defend their organization from advanced threats that had evaded detection by traditional security controls.

BENEFITS

- Cyborg Security puts real security first. With all of our content based exclusively on suspicious and malicious behaviors, and not fragile or stale indicators of compromise, Cyborg Security's hunt and detection packages will work even when the actor adapts and evolves.
- Not all threats are equal. Cyborg Security's threat detection content is fed by comprehensive threat intelligence. This allows you to find hunt and detection content that applies to you; whether by tactic, technique, procedure, actor, malware, or geography.
- Show don't tell. Cyborg Security's hunt and detection packages include cyber threat emulation (CTE) allowing security teams to emulate advanced adversaries and malware to ensure proper and ongoing detection.
- Your time is valuable. Cyborg Security's licensing doesn't use credits, tokens, or other microtransactions. We give you unlimited access to the best behavioral detection content, period. This means you'll be able to focus on security and not accounting!

CYBORG SECURITY

THE CHALLENGE

In 2020, the organization launched a threat hunting capability. The goal was to 'deepen' proactive security capabilities and move beyond basic indicator-fuelled monitoring and alerts. Starting with two FTEs, the company planned to expand to five FTEs over 24 months.

Initially, the threat hunting team faced three challenges:

1. Limited time to develop effective threat hunts—the team needed 2-3 weeks to plan and build each hunt.
2. Mapping hunts to gaps using models like MITRE ATT&CK.
3. Difficulty growing the team and bridging knowledge gaps due to lack of available education and high-quality content.

The organization needed a supplemental product to provide specialized threat hunting content and education geared to the financial services industry.

THE SOLUTION

Acme assessed several open source and paid threat hunting content platforms. In most cases, the company was concerned about the lack of transparency provided into relevant intelligence and context for each hunt. This information was internally housed and not shared with the customer.

Another concern was that some platforms required a locally installed agent, which would further complicate the organization's tool stack.

The company agreed to a trial with Cyborg Security for specific hunting packages. In particular, Acme was impressed by Cyborg Security's:

- Continuous validation and improvement of threat hunts.
- Decay modeling to remove outdated hunts from the portal.
- Automated customization of queries to fit Acme's environment.
- Full access to relevant context, CTI, and analyst runbooks.

CYBORG SECURITY

THE RESULT

> **"PERHAPS THE NUMBER ONE BENEFIT WE'VE SEEN FROM WORKING WITH CYBORG IS OUR THREAT HUNTERS ARE EXCITED TO WORK WITH THEIR CONTENT. IT INSPIRES THEM TO DO A GREAT JOB, AND IT'S ALSO GREAT FROM A HIRING PERSPECTIVE BECAUSE IT HELPS NEW HUNTERS GET UP AND RUNNING FAST IN OUR INDUSTRY."**
>
> **– THREAT HUNTING TEAM LEAD, US FORTUNE 500 FINANCIAL ORGANIZATION**

The organization Formalized the partnership and began using Cyborg Security's content platformfor up to 80% of its hunting operations. Benefits included:

- Huge time savings—from ~3 weeks per hunt to ~1 day.
- Content transparency gives confidence that each hunt is effective.
- Helps current and prospective threat hunters build their skillset
- Developing hunts for new threats takes days, not weeks.
- Maps to MITRE ATT&CK, Cyber Kill Chain, and Diamond Model.
- Helps Acme identify logging and data deficiencies.
- Validation and emulation tools aid in 'sense checking' content.

CYBORG SECURITY

ABOUT CYBORG SECURITY

Cyborg Security is pioneering threat hunt and detection content with its HUNTER platform. HUNTER enables security teams to deploy advanced behavioural content in their environment with no extra tools, appliances, or resources. The HUNTER platform delivers threat hunt and detection packages for security platforms like SIEM, data lake, and EDR.

Our packages feature an analyst-first approach that guides analysts through the investigation. Every package includes platform content, analyst-focused run books, and threat emulation. The packages detect the latest techniques, attacks, and exploits observed from threat intelligence. And each package is also tagged and enriched with MITRE ATT&CK, Kill Chain, Diamond Model, and more.

During an investigation, the focus should be on security, and not accounting. Cyborg Security uses a straightforward “all-you-can-eat” model, without the complexity of micro-transactions. This ensures organizations have the content when they need it.

Begin Your Hunt with Cyborg Security.

EVOLVE YOUR THREAT HUNTING WITH HUNTER