LogicHub

Case Study

How Cobalt supercharges internal security with MDR+

Introduction

Cobalt was founded in 2013, and in 2016 began focusing on transforming the pentesting industry by rethinking application security and delivering an integrated security platform to connect modern organizations with top security talent. Their vision is to "become the world's interface to the security workforce." As a rapidly growing security startup, Cobalt's internal security operations are critically important, but like many early-stage companies, finding the resources to execute was a challenge.

The Challenge

For any company, particularly a rapidly growing startup, delivering 24/7 security on a limited budget can be both a logistical and financial challenge. Ray Espinoza, Cobalt's Chief Information Security Officer and a longtime industry veteran, was tasked with not only securing the company's existing infrastructure but building a program that could adapt and scale to meet future growth.

Ray had multiple challenges to overcome. As a global organization, Cobalt required 24/7 protection, but lacked the resources to fully staff an around the clock security operation. And despite having strong in-house expertise and an enterprise-ready security stack, the sheer volume of alert data his team was monitoring left them with a prohibitive amount of data to analyze, slowing down detection and response. What Ray and his team really needed was a way to streamline and accelerate first line triage of all of their alert data to quickly identify which threats were actionable. This would enable them to quickly mitigate attacks and free up time for more strategic security work.

Cobalt

Cobalt needed a solution that could deliver:

- 24/7 advanced detection and response
- Improved visibility into cloud, endpoint, network and user threats
- Strong integration with Cobalt's SIEM platform (SumoLogic)
- L1/L2 alert investigation and triage at scale to reduce false positives

The Solution

Ray and his team were considering a couple of potential solutions that each had their own strengths and drawbacks. A security orchestration, automation and response (SOAR) solution would deliver automated playbooks to analyze and respond to threats quickly. But the time and overhead necessary to build out the library of playbooks they would need was too high, so SOAR quickly became an unfeasible option.

The alternative was to outsource L1/L2 activities to a managed detection and response (MDR) provider. Engaging with an MDR provider would deliver the first line triage and 24/7 coverage Ray was looking for, as well as the false positive reduction they needed. However, the options that would deliver the level of broad-based visibility and protection Cobalt needed that would integrate with their existing security stack were well outside of their available budget. And that's where LogicHub came in.

Automation-driven MDR +

LogicHub presented Cobalt with a solution that offered the best of both worlds. Automation-driven MDR+ not only delivered the 24/7 detection and response that Cobalt was looking for, it was built on a SOAR platform that would integrate with their existing security solutions and deliver consistent threat protection at machine speeds. And the inherent efficiency gains of an automation-driven solution meant that LogicHub was able to offer 24/7 detection and response that covered cloud, endpoint, network, and user-based threats at a cost that fit within Cobalt's budget.

Problems Being Solved

Cobalt had numerous high priority items that they needed to address. The early tactical use cases they wanted to address included:

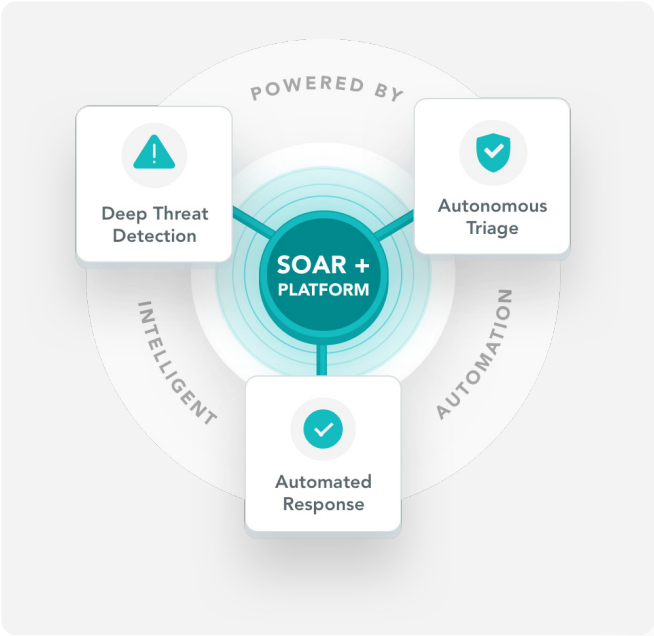
- Investigating and triaging Crowdstrike alerts to quickly identify exploits that needed remediation
- Detecting potential account abuse in G-suite by quickly identifying suspicious activity like duplicate logins from impossible geolocations
- Investigating attacks and other issues against their cloud platform infrastructure that could potentially cause downtime to their core application

The challenge was being able to do so in a way that delivered accurate and fast detection and response while also adapting to Cobalt's operating requirements. That included being able to analyze data from Cobalt's entire security stack, but doing so primarily using their SIEM, Sumologic, as the central collection point for alert data to initiate detection and response processes.

And with LogicHub being a newer entrant into the MDR field, Cobalt also needed assurances that the company would be willing and able to adapt quickly to address any service delivery issues that came up during implementation and in production. This included demonstrating the ability to rapidly integrate with Cobalt's existing security stack, showing the responsiveness necessary to adapt to their specific operating requirements, and a willingness to respond quickly to any issues as they came up.

Quantifiable Value Delivered

LogicHub was able to address Cobalt's concerns during a lengthy proof of concept and continued throughout the implementation process. This included the rapid turnaround of new integrations and a willingness to quickly escalate and implement changes in operating procedures to eliminate any gaps in service. Regular status updates, executive-level customer success advocacy and strong cooperation with Cobalt's security operations team has allowed LogicHub to deliver exceptional service with built-in processes for continuous improvement.



Cobalt's engagement with LogicHub empowers their existing team to detect and respond to threats faster and around the clock, without requiring an extensive amount of additional overhead or operating costs. The partnership allows Cobalt to:

- Better leverage their existing security stack through automation-driven threat detection, alert triage and incident response
- Extend the reach and capabilities of a skilled but small security team
- Eliminate the need for 1-2 FTEs who would have been dedicated to just performing event triage
- Benefit from the herd immunity from detection and response activities delivered across LogicHub's diverse customer base

Future Initiatives

While Cobalt has seen immediate value from LogicHub's managed detection and response services, the relationship continues to evolve as additional use cases are added and both automated and SOC-driven processes evolve. A few potential areas for expansion include:

- Add use cases to their MDR service to offload additional time consuming and manual processes and allow their team to focus even more on strategic security initiatives
- Incorporate more fully automated and one-click incident response actions to lower mean time to response (MTTR) and expedite remediation for a greater number of use cases
- Train Cobalt security staff to build their own automated playbooks in the dedicated SOAR+ instance included with the LogicHub MDR service

Salesforce Exfiltration Detection

The Challenge

Cobalt is an extensive Salesforce user, with a large amount of proprietary and sensitive customer data stored on the SaaS platform. They need to monitor activity on the platform to detect and prevent critical data from being stolen, but lack the in-house resources to monitor and investigate the necessary volume of data to do so effectively.

LogicHub MDR Solution:

- LogicHub's SOAR+ ingests copy, delete, read and write activity on Salesforce data
- Automated playbooks use machine learning to establish baselines of normal activity to detect suspicious or unusual Salesforce activity
- Suspicious activity is automatically enriched with information about who is performing the action and relevant context about that user's permissions
- LogicHub's MDR+ SOC analysts investigate suspicious activity to confirm any true threats and add additional relevant event context
- LogicHub escalates confirmed case with recommendations to Cobalt's security team for remediation

Customer Benefit

- Cobalt is able to secure their Salesforce data 24x7 without requiring an extensive amount of time or overhead to investigate potential exfiltration
- Misuse or malicious behavior within Salesforce is rapidly detected so that Cobalt can immediately initiate incident response to prevent data theft
- Cobalt's security team receives only confirmed cases with all relevant event context so that they can take action immediately to prevent data exfiltration

Unauthorised Access of G-Suite Accounts

The Challenge

As a globally distributed organization using G-Suite's cloud-based applications for productivity, detecting suspicious or unauthorized access of G-Suite accounts was particularly challenging for Cobalt. Identifying abnormal logins required an extra layer of research to see who was supposed to be logging in from where and when.

LogicHub MDR Solution:

- LogicHub uses alerts from Sumologic to monitor for suspicious logins based on authentication activity in G-Suite
- Automated playbooks use machine learning to baseline typical user authentication behavior in GSuite
- Alerts on suspicious authentication or access in GSuite are automatically analyzed to validate activity like new access methods, logins from never before seen countries, and impossible travel using integrations with: **Geo-mind, Abuse IPDB, OSINT scraping, runSearch**
- Alerts are automatically triaged and likely malicious/unauthorized authentication events are escalated to the LogicHub SOC for additional analysis and confirmation
- A LogicHub analyst forwards any confirmed case with all relevant event detail and mitigation recommendations to Cobalt for execution

Customer Benefit

- Cobalt is able to continuously monitor global authentication activity with minimal overhead on their security staff
- Any suspicious or malicious activity is rapidly detected, investigated and escalated to prevent unauthorized access from resulting in potentially damaging malicious behavior
- Global identity and access management is simplified and misuse of credentials is minimized

Cloud Data Exfiltration Detection and Response

The Challenge

Like a majority of distributed organizations, cobalt stores a lot of data on cloud resources like Google Drive. This creates additional challenges for securing confidential data because monitoring and investigating suspicious access of cloud resources on a 24x7 basis is a time consuming process. And that's assuming that potentially anomalous activity is identified in the first place. Cobalt needed a way to quickly detect and investigate any behavior tied to cloud storage that might lead to data exfiltration.

LogicHub MDR Solution:

- LogicHub uses alerts from Sumologic to monitor for anomalous or suspicious access to Google Drive
- Automated playbooks use machine learning to baseline typical user access and data usage on Google Drive
- Alerts on suspicious authentication or access in GSuite are automatically analyzed to validate activity like anomalous amounts of files accessed, new file paths accessed, access being sourced from new locations and new IPs using integrations with: **WhoIs, Abuse IPDB, OSINT scraping**
- runSearch (for G-Suite access logs)
- Alerts are automatically triaged and likely malicious/unauthorized authentication events are escalated to the LogicHub SOC for additional analysis and confirmation
- A LogicHub analyst forwards any confirmed case with all relevant event detail and mitigation recommendations to Cobalt for execution

Customer Benefit

- LogicHub's automation-driven investigation processes have lowered the mean time to detect (MTTR) per incident from 20 minutes down to less than three minutes
- Cobalt is able to continuously monitor cloud data access on a 24x7 basis with overhead on their security staff
- Any suspicious or malicious activity is rapidly detected, investigated and escalated to prevent exfiltration of confidential company and customer data