LEGION

CASE STUDY

Saving 9 FTEs Worth of Investigative Hours with Legion

THE CUSTOMER

Sector:	Size of SOC:	Employees:
Insurance	10 analysts	31,000

Use Cases:

Automating Tier 1 Investigations

> "Legion massively cuts down the noise. We're drowning in over 10,000 false positives. Without it, we'd need a whole extra team to get through it all."
>
> Manager, Network Security

Problem Statement

A large multinational insurance provider needed to scale its SOC without expanding headcount. They currently have an MDR vendor that helps manage investigations, but has struggled to help scale their SOC. Their analysts were spending excessive time manually triaging high-volume, repetitive Tier 1 alerts, primarily signature violations for web-based attacks and phishing attempts. Investigations were time-consuming and inconsistent.

The Solution

They deployed Legion's autonomous mode to handle Tier 1 investigations end-to-end, without human intervention. Legion ingests alerts from LogRhythm and:

- Investigates signature violations by analyzing log patterns associated with web attack vectors
- Responds to phishing alerts triggered by network firewall blocks

It enriches these alerts using a blend of external threat intelligence tools and internal telemetry from firewall logs.

The Result: First 30 Days Using Legion

Legion transformed its Tier 1 investigation process from manual and reactive to automated and highly efficient. By eliminating ~90% of the human effort involved, they effectively saved the work of nine full-time analysts without compromising accuracy.

Autonomous Investigations **24.1K** Total automated security investigations	Suspicious Investigations **1.9K (7%)** 7% of total flagged as suspicious	MTTI (Human) **3m:51s** Mean Time To Investigate manually
MTTI (Automation) **1m:09s** Mean Time To Investigate with Legion	Time Saved **1546 hours** Equivalent to ~9 FTEs	Success Rate **99.998%** Accuracy or effectiveness of automation
MTTR (pre-Legion) **19.1 min** Mean Time To Resolve before Legion	MTTR (post-Legion) **2.07 min** MTTR after deploying Legion	MTTR Improvement **89.15%** Efficiency gain post-Legion implementation