LEGION

CASE STUDY

How the University of Tulsa Cut Investigation Time by 83% with Legion

THE UNIVERSITY OF TULSA

Sector:
Education

Size of SOC:
11 analysts

Employees:
5,000

Use Cases:
Automating Tier 1 Investigations

> “Legion cut our average investigation time by 83%, allowing our small team to keep up with the considerable workload.”
>
> **Tyler Burroughs**, Security Analyst at The University of Tulsa

Problem Statement

At the University of Tulsa SOC, students train as real-world analysts by investigating threats, making decisions, and learning the workflows they'll use in enterprise environments. But like most SOC teams, they struggled with alert overload, repetitive manual tasks, and inconsistent investigations. Maintaining continuity is tough for any SOC, especially when your analysts graduate every year.

This busywork not only slowed investigations but also left students with less time for high-value analysis and skill development. The SOC needed a solution that didn't just automate tasks but also think like an analyst, reinforce consistent processes, and support hands-on learning.

The Solution

The University of Tulsa SOC integrated Legion to help standardize and automate its investigations, without needing any new infrastructure. They recorded their daily investigations, following established procedures, and Legion created an investigation standard based on these analyses.

This quickly revealed gaps and inconsistencies among student analysts, even with the same alert types. Legion made these differences visible, enabling instructors to correct mistakes and train students to follow best practices.

By combining automation with analyst oversight, the SOC maintained its focus on education and procedural discipline while reclaiming time from repetitive work.

The Result

With Legion, the University of Tulsa's SOC reduced the average MTTI by 83%, without needing to add headcount or extra tools. Analysts spent less time on repetitive intel gathering and more time sharpening real-world skills.

The result? Fewer false positives draining valuable time, better continuity despite annual student turnover, and students graduating with practical experience in the workflows they'll use as professional security analysts.

MTTI (Human)
29m:7s
Mean Time To Investigate manually

MTTI (Legion)
4m:42s
Mean Time To Investigate with Legion

MTTI (Improvement)
83%
Efficiency gain post-Legion implementation