FINANCIAL SERVICES · PAYMENTS

A LIVE ATTACK ON A CORE PAYMENT SYSTEM, STOPPED THREE DAYS BEFORE PEAK.

How a major payments and communications provider gained in-house SOC depth, consolidated its tooling onto Splunk, and turned its security program into a reason customers choose it.

OUTCOME 01

A DAY AHEAD IN A LIVE INCIDENT

Ahead of the outside IR firm, because Alchemy knew the environment.

OUTCOME 02

TOOL CONSOLIDATION

Custom Splunk reporting replaced overlapping tools.

OUTCOME 03

SECURITY AS A DIFFERENTIATOR

A reason B2B customers and partners choose the client.

KEY RESULTS

- Found and contained a major attack three days before the client's biggest day of the year
- Stayed a full day ahead of the outside IR provider
- Consolidated overlapping tools onto custom Splunk reporting
- Turned security into a differentiator with B2B customers and partners
- Met investor requirements and launched a multi-year maturity roadmap
- Renewed the partnership for three more years

BACKGROUND

The client is a major payments and communications provider with a large in-house security team. As a financial services company handling sensitive customer data and payment processing, it answers to strict internal security requirements, PCI compliance, cyber insurance mandates, and contractual obligations to business partners.

What it needed was in-house SOC capability: people who know its systems, its crown jewels, and its adversaries, on shift around the clock. It chose a partner to provide exactly that.

THE CHALLENGE

THREE PRESSURES AT ONCE

01

IN-HOUSE DEPTH, 24×7

The client wanted analysts who know its environment as well as its own staff do, on shift around the clock. Hiring, training, and keeping that team was a multi-year effort in a tight market.

02

INVESTOR PRESSURE

Investors wanted a stronger security posture to protect the company's value, and business partners wanted proof of it.

03

CONTINUITY AMID TURNOVER

A shortage of trained practitioners drove high turnover. The client needed to keep maturing its defenses while threats kept changing.

WHY THEY CHOSE ALCHEMY SECURITY

FOCUSED, AND BUILT TO SCALE

After vetting larger firms, the client chose Alchemy Security to operate as an extension of its own SOC, tuned to its environment. Six capabilities decided it:

01 Scale to match rapid organizational growth

02 Faster time-to-value: detections prioritized by the adversaries most likely to target payment processors

03 Advanced log collection, search, and preservation on Splunk

04 Threat reporting and intelligence from Athanor, ranking what matters first for payment processors

05 A unified threat monitoring program, including deception technology

06 Transparent method built on the Unified Kill Chain and MITRE ATT&CK

THE SOLUTION

ADVERSARY-LED, BUILT IN PHASES

Alchemy started with the adversaries. Athanor showed which groups target payment processors and the techniques they use. Working sessions then mapped those techniques to the client's critical systems, high-risk assets, and privileged identities, and set the order of the work.

PHASE 1

DETECT THE LIKELIEST ATTACKS FIRST

Phase 1 mapped those adversaries' techniques to MITRE ATT&CK, onboarded the data sources each priority technique needs, deployed those detections first, and established escalation workflows with defined stakeholders.

Alchemy also placed honeypots (decoys that trap attackers) on the paths those adversaries would take, and around high-value assets that remained vulnerable.

PHASE 2

WIDEN COVERAGE, KEEP RE-PRIORITIZING

Phase 2 extended telemetry to the company's crown jewels, compliance-scoped assets, and other systems in scope for log collection and preservation.

As Athanor tracked changes in the threat landscape, detections and hardening recommendations continued to evolve with it, so coverage kept pace with the adversaries targeting their industry.

BEYOND DETECTION

REPORTING

REPORTING LEADERSHIP CAN ACT ON

Athanor threat reporting showed executives which adversaries were active against payment processors, what the environment was seeing, and what to close next.

CONSOLIDATION

FEWER TOOLS, ONE SPLUNK VIEW

Custom Splunk reporting covered work several standalone tools had been doing. The client consolidated that tooling onto one platform.

BUSINESS VALUE

SECURITY AS A DIFFERENTIATOR

For a B2B provider moving its customers' payments, security is part of what it sells. A mature program became a reason customers choose it.

PHASE 3 · THE INCIDENT

THREE DAYS BEFORE PEAK

About 18 months into the partnership, Alchemy detected suspicious activity on one of the client's most critical systems: an outdated, highly vulnerable application behind core payment processing, one that would have cost millions to upgrade properly.

It happened three days before the client's biggest operational day of the year. When the client's own containment and recovery attempts failed, it became an all-hands incident, and the client turned to Alchemy for emergency response.

While the client's outside IR provider was still getting up to speed, Alchemy's analysts had already found the source of the attack and were advising on containment. Together they removed the attacker and added monitoring on the vulnerable system. The client ran at full capacity through its peak period.

> **WHEN THE POSTMORTEM EXERCISE WAS COMPLETED FOR THE INCIDENT, THE CLIENT OBSERVED THAT WE WERE CONSISTENTLY A DAY AHEAD OF ANALYSIS AND FINDINGS COMPARED TO THEIR OUTSIDE IR PROVIDER, LARGELY BECAUSE WE WERE SO INTIMATELY TUNED IN TO THEIR ENVIRONMENT.**
>
> — JOE BONNELL · FOUNDER & CEO, ALCHEMY SECURITY

PHASE 4 · THE AFTERMATH

Alchemy ran a full review and recommended how to harden the legacy application until it could be modernized, including additional monitoring sensors and tighter firewall policies. Alchemy also matured the client's Splunk SOAR investment to orchestrate automated response.

PHASE 5 · RENEWED FOR THREE MORE YEARS

On the strength of those results, the client renewed its MDR partnership for three more years. Alchemy continues to protect the client's critical infrastructure and mature its program.

KNOW THE ADVERSARY. PRIORITIZE YOUR DEFENSE.

See who is most likely to target you and what to do first.

REQUEST A CYBER RESILIENCE ASSESSMENT

alchemysecurity.com/request-assessment