CASE STUDY

Bridging the Gap: How a Leading Insurer Operationalized API Security within CrowdStrike

Executive Summary

A premier Workers' Compensation Insurance provider struggled with a common enterprise challenge: API security was siloed. While their SecOps team had deep visibility into endpoints and workloads via CrowdStrike, their API layer was a blind spot, managed primarily by engineering with limited visibility from a WAF. By integrating Salt Security directly with CrowdStrike Falcon, the organization unified its defense, turning abstract API threats into actionable security signals within its existing operations.

The Challenge: The "WAF + SIEM" Blind Spot

Despite having a mature security stack, the Security Engineering & Architecture Team faced a critical visibility gap.

- **The Visibility Void:** The team lacked a continuous, living inventory of their API fabric. They relied on manual investigations through their API Gateway, leaving them blind to "shadow" API endpoints and drift.
- **The Detection Gap:** Their existing stack (WAF + Logs + SIEM) monitored for volumetric attacks but failed to detect **authenticated business logic abuse**. These attacks appear to be legitimate traffic but manipulate process logic.
- **The Operational Silo:** API security was treated as an "engineering function" disconnected from the core Security Operations Center (SOC). This meant API threats were not being prioritized or triaged with the same rigor as endpoint threats.

The Salt + CrowdStrike Solution

The customer chose Salt Security not just for its detection capabilities but for its seamless integration with their existing ecosystem.

- **Unified Visibility:** Salt discovered the full API attack surface and fed that inventory and risk data directly into the CrowdStrike Falcon console.
- **Behavioral Detection:** Salt moved beyond simple signature matching to identify "low-and-slow" logic abuse patterns that the WAF missed.
- **Operational Efficiency**: Instead of adding "yet another standalone tool" to the analyst's dashboard, Salt signals were ingested into existing workflows. This allowed the team to triage API attacks alongside endpoint alerts.

"Before Salt, APIs lived outside our core security operations and were a primary engineering function. After integrating with CrowdStrike Falcon, we are operationalizing API threats to become immediately actionable alongside endpoint and workload signals. That shift alone fundamentally improves our ability to detect, prioritize, and respond to modern application-layer attacks."

— Senior Manager of Security Engineering, Premier Insurance Provider

Key Takeaway for Security Teams

Stop treating API security as a separate island. By integrating **Salt Security** with **CrowdStrike**, you can maximize your existing investment, simplify operations, and gain the behavioral context needed to stop attacks that your traditional security stack, such as WAF and API Gateways miss. Whether they come from humans or AI agents, Salt provides the coverage you need.