See Every Threat, Secure Every API

CROWDSTRIKE + SALT Security

Elevate API Security with Salt Security and CrowdStrike

Introduction

APIs are crucial to modern business operations but also increase the attack surface for potential security threats. Organizations need comprehensive solutions that provide deep visibility, advanced threat detection, and rapid response capabilities to secure APIs effectively. Integrating Salt Security with CrowdStrike's NG-SIEM and Falcon Firewall delivers these essential security features, allowing businesses to identify, understand, and respond to API-targeted threats in real-time.

Key Benefits of the Integrations

- **Unified Threat Detection and Response:** Salt Security’s advanced API inspection capabilities—such as discovering shadow and zombie APIs—combined with CrowdStrike’s superior threat intelligence create a powerful synergy for identifying malicious behaviors and potential vulnerabilities across your entire API landscape.
- **Rapid Threat Response:** Alerts and threat information from Salt Security seamlessly integrate into CrowdStrike's NG-SIEM dashboard and Falcon Firewall. This integration enables security teams to quickly address API-specific threats within the broader context of overall security events.
- **Comprehensive API Visibility and Analytics:** Salt Security offers exceptional visibility into the API lifecycle by identifying all APIs and analyzing their behaviors. This data is integrated into CrowdStrike's NG-SIEM and Falcon Firewall for thorough threat analysis and effective vulnerability management.
- **Behavioral Analysis:** CrowdStrike's NG-SIEM utilizes Salt Security's detailed data on API traffic patterns. This facilitates advanced anomaly detection and event correlation, helping

uncover potential API-based attacks that might go unnoticed.

- **Streamlined Incident Response Workflows:** These integrations enable automatic incident generation within the NG-SIEM and Falcon Firewall whenever specific API threat thresholds are met. This makes investigations more efficient and accelerates the remediation process. Salt Security provides security analysts with valuable contextual intelligence, enriching CrowdStrike's NG-SIEM and Falcon Firewall with actionable data related to API-specific attack vectors and vulnerabilities.

Key Use Cases

- **Detecting and Mitigating Advanced API Threats:** Identify sophisticated attacks—such as data exfiltration, injection, or DDoS attacks targeting APIs—and respond in real time by leveraging combined insights from Salt Security and CrowdStrike's NG-SIEM and Falcon Firewall.
- **Proactive API Risk Management:** Prioritize and address potential risks within the API ecosystem before they escalate into critical issues. Utilize Salt Security's API discovery and vulnerability assessment capabilities, integrated with CrowdStrike's NG-SIEM and Falcon Firewall.
- **Enhanced Compliance Reporting:** Simplify regulatory compliance by using robust API monitoring and detailed logging from Salt Security, which is seamlessly integrated with CrowdStrike's NG-SIEM and Falcon Firewall reporting features.

Technical Highlights

- **Seamless Data Flow:** Salt Security integrates with CrowdStrike's NG-SIEM and Falcon Firewall platforms through a secure, uni-directional data exchange, ensuring that both platforms are continuously updated with the latest threat information from Salt Security.
- **Customizable Alerts and Dashboards:** Users can customize their dashboards within the CrowdStrike NG-SIEM and Falcon Firewall to include data from the Salt Security API, allowing them to tailor alert systems to suit their organization's specific needs.
- **API Anomaly Correlation:** CrowdStrike's NG-SIEM and Falcon Firewall enhance detection capabilities by correlating API-specific data from Salt Security with broader system activities, providing a comprehensive view of potential threats.

Conclusion

Integrating Salt Security with CrowdStrike's NG-SIEM and Falcon Firewall represents a significant advancement in securing APIs against contemporary threats. By combining in-depth API insights with robust threat intelligence and a unified security platform, organizations can strengthen their security posture, swiftly respond to incidents, and confidently protect their critical assets.