See Every Threat, Secure Every API

CROWDSTRIKE Falcon® Next Gen SIEM + SALT Security

Elevate API Security with Salt Security and CrowdStrike NG-SIEM

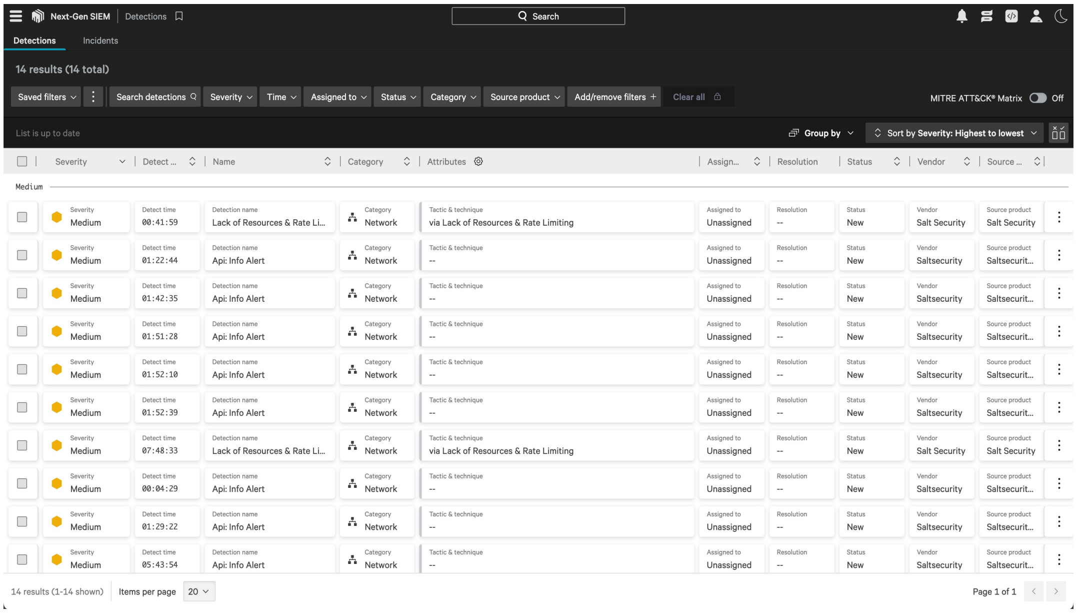
Introduction

APIs are essential to modern business operations, but they also create a growing attack surface. To effectively secure APIs, organizations require comprehensive solutions that offer deep visibility, advanced threat detection, and rapid response capabilities. The integration of Salt Security with CrowdStrike's next-generation SIEM (NG-SIEM) provides these critical security features, enabling businesses to identify, understand, and respond to API-targeted threats in real time.

Key Benefits of the Integration

Unified Threat Detection and Response:

- **Enhanced Monitoring:** Salt Security's advanced API inspection capabilities, which include the discovery of shadow and zombie APIs, combined with CrowdStrike's superior threat intelligence, create a powerful synergy for identifying malicious behavior and potential vulnerabilities across your entire API landscape.



14 results (14 total)

List is up to date

Medium

Severity	Detect time	Detection name	Category	Tactic & technique	Assigned to	Resolution	Status	Vendor	Source product
Medium	00:41:59	Lack of Resources & Rate Li...	Network	via Lack of Resources & Rate Limiting	Unassigned	--	New	Salt Security	Salt Security
Medium	01:22:44	Api: Info Alert	Network	--	Unassigned	--	New	Saltsecurity	Saltsecurit...
Medium	01:42:35	Api: Info Alert	Network	--	Unassigned	--	New	Saltsecurity	Saltsecurit...
Medium	01:51:28	Api: Info Alert	Network	--	Unassigned	--	New	Saltsecurity	Saltsecurit...
Medium	01:52:10	Api: Info Alert	Network	--	Unassigned	--	New	Saltsecurity	Saltsecurit...
Medium	01:52:39	Api: Info Alert	Network	--	Unassigned	--	New	Saltsecurity	Saltsecurit...
Medium	07:48:33	Lack of Resources & Rate Li...	Network	via Lack of Resources & Rate Limiting	Unassigned	--	New	Salt Security	Salt Security
Medium	00:04:29	Api: Info Alert	Network	--	Unassigned	--	New	Saltsecurity	Saltsecurit...
Medium	01:29:22	Api: Info Alert	Network	--	Unassigned	--	New	Saltsecurity	Saltsecurit...
Medium	05:43:54	Api: Info Alert	Network	--	Unassigned	--	New	Saltsecurity	Saltsecurit...

14 results (1-14 shown) Items per page 20

Page 1 of 1

- **Rapid Threat Response:** Alerts and threat information from Salt Security integrate seamlessly into CrowdStrike's NG-SIEM dashboard. This integration enables security teams to respond quickly to API-specific threats within the cotext of broader security events.

Comprehensive API Visibility and Analytics:

- **Complete API Lifecycle Coverage:** Salt Security offers exceptional visibility into the API lifecycle by identifying all APIs and analyzing their behaviors. This information is integrated into CrowdStrike's Next-Generation Security Information and Event Management (NG-SIEM) for comprehensive threat analysis and vulnerability management.
- **Behavioral Analysis:** CrowdStrike's NG-SIEM utilizes the in-depth data provided by Salt Security on API traffic patterns. This enables advanced anomaly detection and event correlation, helping to reveal potential API-based attacks that might otherwise go unnoticed.

Streamlined Incident Response Workflows:

Automated Workflows: This integration enables automatic incident generation within the NG-SIEM whenever specific API threat thresholds are reached, making investigations more efficient and speeding up the remediation process.

Contextual Intelligence: Security analysts gain valuable contextual intelligence from Salt Security, enhancing CrowdStrike's NG-SIEM 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. Respond in real-time by utilizing combined insights from Salt Security and CrowdStrike's Next-Generation Security Information and Event Management (NG-SIEM).
- **Proactive API Risk Management:** Prioritize and address potential risks within the API ecosystem before they escalate into critical issues. Leverage Salt Security's API discovery and vulnerability assessment capabilities, integrated with CrowdStrike's NG-SIEM.
- **Enhanced Compliance Reporting:** Simplify regulatory compliance by utilizing robust API monitoring and detailed logging from Salt Security, seamlessly integrated with CrowdStrike's NG-SIEM reporting features.

Technical Highlights

- **Seamless Data Flow:** Salt Security integrates with CrowdStrike's NG-SIEM platform through a secure data exchange, ensuring that Crowdstrikes NG-SIEM is up-to-date with the latest threat information.

- **Customizable Alerts and Dashboards:** Users can customize their dashboards within the CrowdStrike NG-SIEM to include data from the Salt Security API, allowing them to tailor alert systems to meet their organization's specific needs.
- **API Anomaly Correlation:** CrowdStrike's NG-SIEM enhances detection capabilities by correlating API-specific data from Salt Security with broader system activities, providing a comprehensive view of potential threats.

Conclusion

The integration of Salt Security with CrowdStrike's NG-SIEM marks a major advancement in securing APIs against contemporary threats. By merging in-depth API insights with robust threat intelligence and a unified security platform, organizations can strengthen their security posture, ensure a swift response to incidents, and confidently protect their critical assets.