Hunters / okta Solution Brief

Identity-Driven Data for Better Detection and Response

IDENTITY IS CENTRAL TO CYBER ATTACKS.

Effective detection and response of cyber attacks require close inspection of authentication telemetry, and correlation with user, endpoint, network and other indications of compromise.

Adding identity and user-based data to the detection and response picture gives the needed enhanced visibility to understanding attack stories across surfaces while achieving higher-fidelity findings.

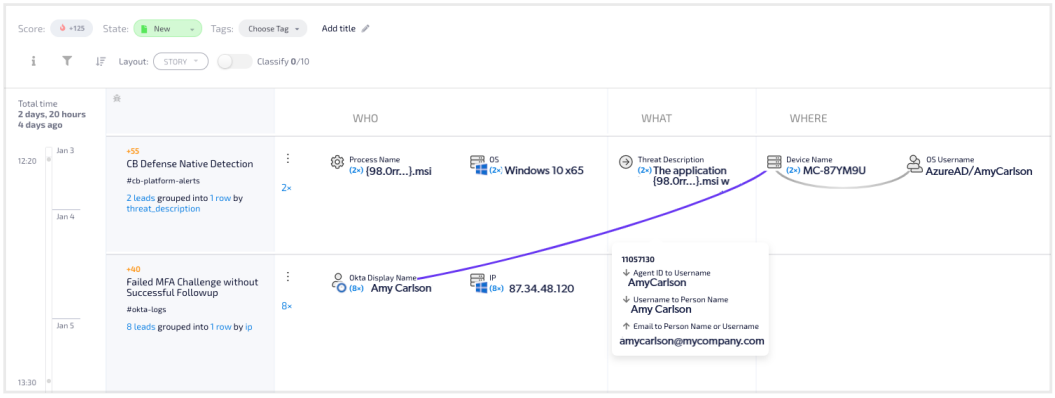
But effectively applying detection and response across multiple security solutions is not an easy task: these systems are siloed, generating a variety of telemetry that is hard to effectively correlate and require advanced expertise to separate benign from malicious alerts.

THE SOLUTION

Hunters XDR applies deep security knowledge to drive effective detection and response across all organizational environments. Using Okta's API, Hunters XDR seamlessly ingests Okta logs and telemetry as a key knowledge source for detecting suspicious behaviors, mapping sparse identities into actual users, and enriching and adding context to the automatic investigations performed by the solution.

Utilize existing Okta's logs and native alerts such as the ones from Okta ThreatInsight to achieve broader detection and response all across the enterprise with high-fidelity correlations.

- **Obtain meaningful Attack Stories** using Hunters' Knowledge Graph to correlate Okta's data with telemetry from other security products from endpoint, cloud or network.
- **Correlate users' SaaS activities** by tying them to their Okta identity to understand the full story and whether there has been an illegitimate access or use of corporate resources.
- **Leverage user-based data** like permissions sets, applications and employee's profile of a specific user to investigate and enrich security telemetry from other data sources.
- **Achieve wider visibility** and better understanding of security posture enterprise-wide.



Attack Story in Hunters' platform showing a credential compromise of a user from their endpoint, natively detected by Carbon Black, and logon attempts to their Okta account two days later. This correlation is powered by Hunters' unique "Person-Matcher" automatic investigation, which can correlate different identities from the same person.

BENEFITS

Seamlessly transform your existing telemetry into an XDR using Okta's identity-driven data

Detect attacks that bypass existing security controls, with cohesive threat detection across your entire IT environment (cloud, network, endpoint and identity)

Achieve higher fidelity correlations by connecting identity data to existing security telemetry with Hunters XDR

Expedite time-to-detect and time-to-respond with high-fidelity Attack Stories

Deploy Hunters in minutes with just a few clicks, no agents required

HOW IT WORKS

1. **Flexible Ingestion:** Hunters uses its cloud connectors to ingest logs and events from Okta as well dozens of additional data sources, including cloud services providers, SaaS applications and firewalls.

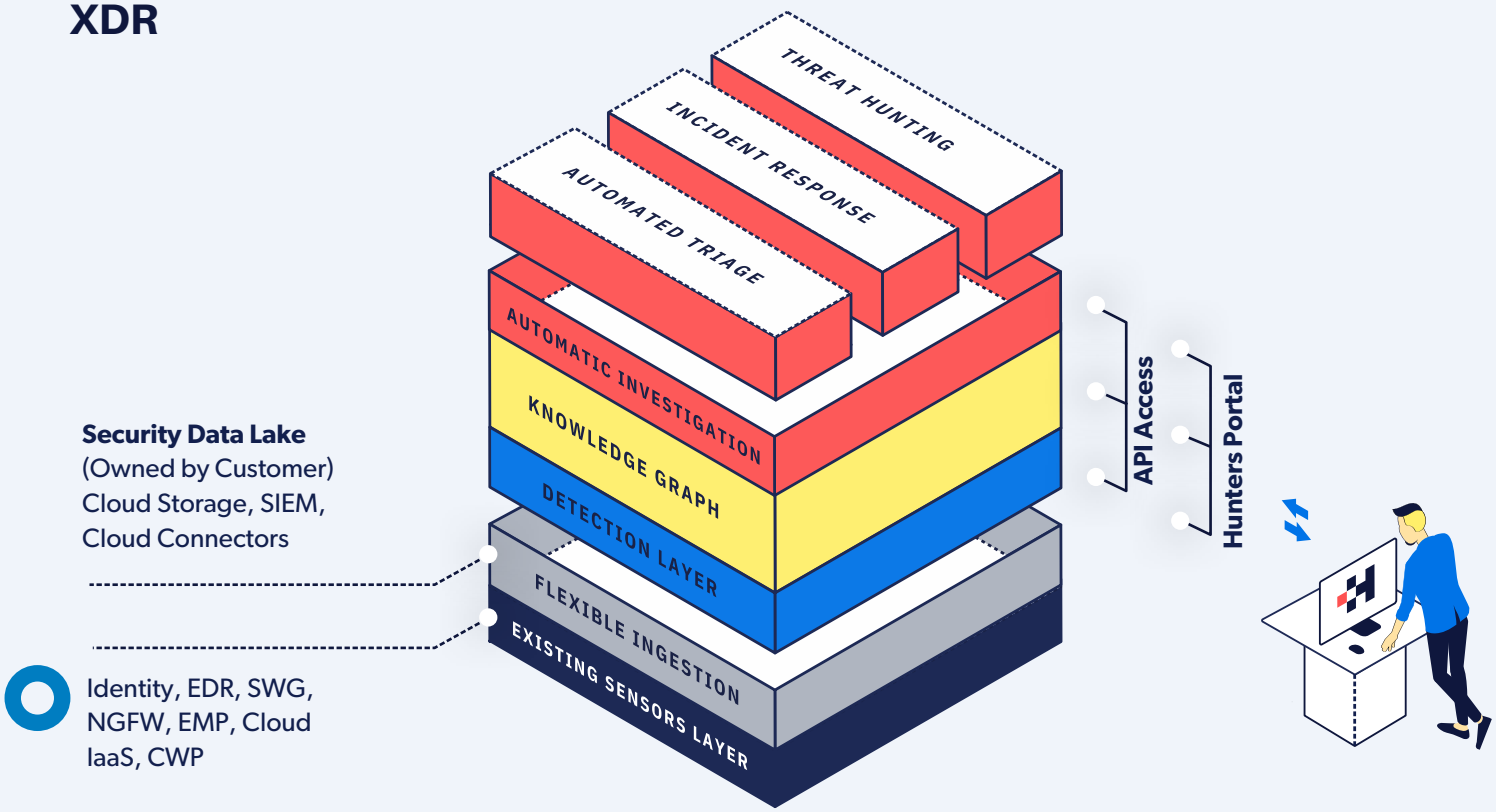
2. **Extraction Engine:** Hunters extracts threat signals as well as alerts from the petabytes of security data generated by the existing stack of security products. It leverages stream processing technology which enables both near real-time processing and unique complex analytical capabilities. This activity is guided by Hunters' TTP-based attack intel which is also mapped into a MITRE ATT&CK technique.

3. **Automatic Investigation and Scoring:** In order to contextualize and understand both weak and noisy threat signals and alerts, Hunters performs autonomous investigations. It automatically extracts features and entities that were involved in a specific suspicious activity, and leverages ML to score them.

4. **Cross-Surface Correlation:** Investigated threat signals and alerts are loaded into Hunters' proprietary Knowledge Graph of related entities and relationships. The solution then uses unsupervised learning to correlate them across disparate areas of suspicious activity to surface Attack Stories, all across the enterprise.

5. **Actionable Attack Stories:** Final investigation outputs from Hunters are delivered as Attack Stories, which include full attack summary and outline, with details such as context, path, target and potential impact.

KNOWLEDGE - POWERED XDR



Watch a Hunters XDR demo

Hunters