Hunters / vmware Carbon Black Solution Brief

Connect Threat Detection and Response Across the Entire Attack Surface

SOC teams today are facing an unprecedented challenge at sifting through the enormous amount of security data generated by the variety of tools living in silos and the lack of automation of repetitive tasks, preventing them to scale and focus on remediating threats in time.

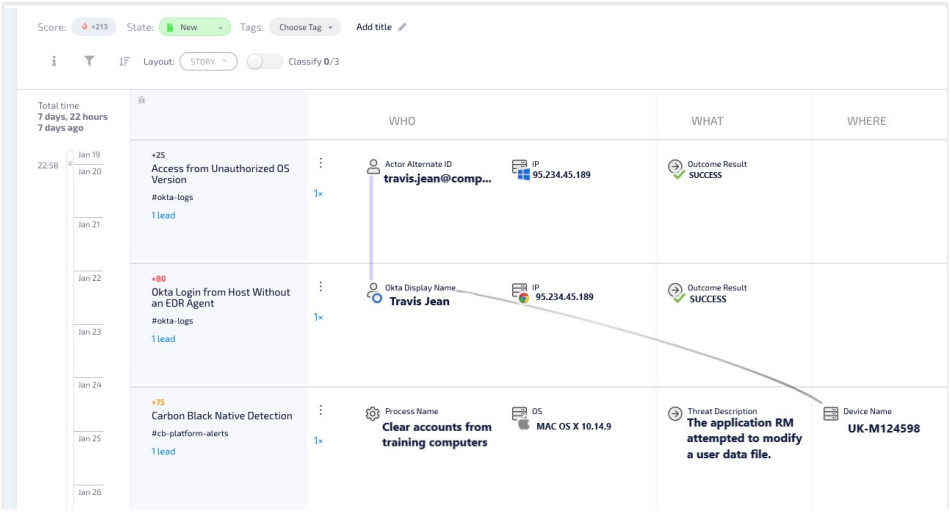
Market-leading solutions like VMware Carbon Black have enabled organizations to monitor and respond to threats thanks to the rich endpoint telemetry generated by the EDR. Using Hunters' open XDR, customers can now scale their security operations with high-fidelity Attack Stories across surfaces and automate repetitive tasks like cross-product investigations and having one single interface that connects data from EDR with other existing security and organizational tools, eventually making it safer to navigate the threat landscape and close the gaps with the attackers.

Your security team has invested in the right tools and talent over the years. Now it's time to take those to the next stage of threat detection and response.

THE SOLUTION

Hunters is an open, agile XDR solution that harnesses adversary expertise and machine learning to proactively detect and respond to threats across the entire attack surface - on endpoint, cloud, network, identity, and email. SaaS-delivered, Hunters seamlessly ingests petabytes of organizational data and security telemetry to search for threat signals, and automatically analyze, score and correlate them with existing alerts from Carbon Black. Using a proprietary Knowledge Graph, Hunters XDR provides analysts with detailed attack stories and context for effective investigation and rapid response. It provides rich insights for containment, and streamlines response by integrating with SOAR and workflow tools.

With Hunters, organizations can easily go from EDR to XDR, achieving higher detection efficacy with their existing IT stack while significantly reducing SOC triage and MTTR.



An Attack Story showing a successful Okta login to an employee account and later a detection on his personal device. A week later there is an endpoint alert as seen by the Carbon Black detection. After a series of automatic investigations by Hunters, the Okta logs and the Carbon Black alert are connected, indicating a credential theft and an attempt to compromise the endpoint a week later.

BENEFITS

Seamlessly transform your existing VMware Carbon Black endpoint telemetry into an XDR

Expedite MTTD and MTTR with data-proof Attack Stories across all surfaces

Understand Incidents in seconds rather than minutes or hours with Hunters' autonomous investigations and Entity Search

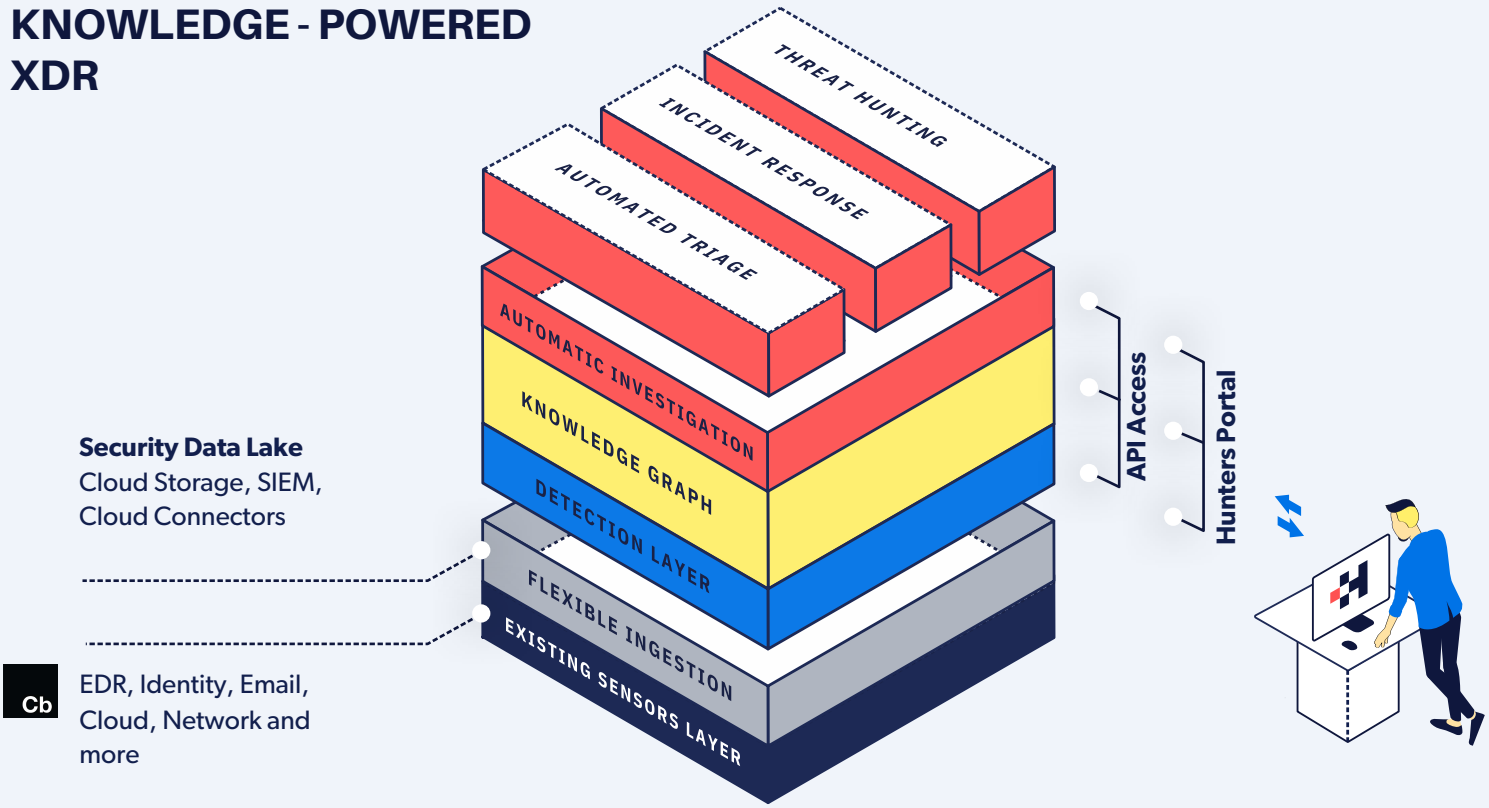
Use Hunters alignment with the MITRE ATT&CK framework to identify your coverage and address blind spots

Deploy Hunters XDR in minutes with just a few clicks, no agents or pre-configuration required

HOW IT WORKS

1. **Seamless, Flexible Ingestion:** Using cloud connectors to pipe into existing security tools, or directly connecting to SIEM, Hunters XDR collects logs, events and telemetry from Carbon Black as well as other dozens of data sources on premises and in the cloud, including NDRs, cloud service providers, firewalls, Identity and Access management tools, and more.
2. **Detection Engine:** Hunters XDR extracts threat signals and alerts from petabytes of existing security data using a stream processing analytics technology. It enables near real-time processing and complex analytics. Threat signal extraction is guided by Hunters' TTP-based attack intel which is also mapped onto a MITRE ATT&CK technique.
3. **Data Representation on a Multi-Dimensional Graph:** The telemetry collected from various IT and security tools is effectively connected together on a proprietary Knowledge Graph, a structured representation of all the suspicious behaviours, all the entities in the network, and the relationships between them.
4. **Automatic Investigation:** In order to understand weak threat signals and alerts, Hunters runs automatic investigations. It fetches all relevant information associated with those, including features and entities that were involved in a specific suspicious activity, and automatically enriches them with further context.
5. **Scoring and Prioritization:** Once there is enough context around threat signals and alerts, Hunters XDR leverages ML to score them from 0 to 100, allowing for an easy prioritization and quick triage.
6. **Cross-Surface Correlation:** Hunters uses unsupervised learning to correlate signals and alerts across disparate areas of suspicious activity in the Graph (e.g., suspected phishing email followed by malware downloads on gateway and EDR), and surface actionable Attack Stories which include full attack summary and outline.
7. **Response and Remediation:** Streamline detection and response by escalating Attack Stories into SOAR tools and other existing workflows, enabling response automation and reducing attackers' dwell time.

KNOWLEDGE - POWERED XDR



Watch a Hunters XDR demo

Hunters