SOLUTION BRIEF

CYBEREASON + VECTRA: END-TO-END DETECTION AND REMEDIATION

The Cybereason Defense Platform integrates with the Vectra Cognito platform to prevent, detect, and respond to advanced cyberattacks. Vectra's cloud-native network detection capabilities, combined with Cybereason complete endpoint protection, allows security teams to easily correlate data for end-to-end visibility from the endpoint across the network. Together, the two solutions accelerate security investigations and enable rapid response to incidents.

Complete Network and Endpoint Visibility and Context

Vectra Cognito and Cybereason integrate via an API to share network and endpoint data. This means security practitioners get visibility into extended attributes directly from the Cognito platform. Teams can easily correlate attacks that span the cloud, enterprise environments, enduser machines, and IoT devices.

The joint solution also provides additional context with corresponding information from the Cybereason Malicious Operation - Malop™, so investigators can get context into the specific Mitre ATT&CKR techniques detected, identify root cause, view an attack timeline, see all affected users and machines, and discover any malicious incoming or outgoing communication. Users can also pivot easily from Vectra Cognito into affected hosts for additional investigation and automated remediation. Full network and endpoint visibility, plus proactive threat hunting capabilities mean attackers have nowhere to hide.

Accelerate Investigations and Response

With additional attributes and context at their fingertips, the Cybereason and Vectra integration greatly reduces security operation workload and enables faster response times.

CHALLENGE

Security teams are often bombarded with alerts. What's worse, unprioritized alerts makes triaging them even more time consuming. Even for fully staffed teams, the lack of visibility, correlation, and context between network and endpoint data for incidents results in time-consuming investigations and delayed responses.

SOLUTION

Cybereason's Cyber Defense Platform with its complete endpoint protection offering have partnered with Vectra Cognito to help security teams combine network and endpoint data for full visibility and accelerated response to cyberattacks.

BENEFITS

The Cybereason and Vectra integration saves time and security resources by providing end-to-end endpoint and network visibility. With prioritized alerts, automatically correlated data, and full attack context, security teams can investigate and remediate incidents quickly and efficiently.

Combining data science, modern machine learning techniques and behavioral analysis, Vectra Cognito performs continuous, automated threat hunting. Incidents are automatically prioritized with packaged forensics, making investigations as easy as possible. In fact, Vectra Cognito has been shown to reduce time spent on threat investigations by up to 90%. Incident responders can then trigger appropriate actions based on the type of threat, risk level, and certainty.

Integration with Cybereason further allows for built-in endpoint prevention, detection and remediation across the broadest range of endpoints, from mobile to fixed and virtual endpoints running Windows, MacOS, Linux, iOS & Android devices. Security staff can kill processes, quarantine files, prevent file execution, or isolate machines to effectively stop cyberattacks and prevent lateral movement across the enterprise.

Enterprise-Ready and Scalable

The joint Cybereason and Vectra integration provides visibility into all enterprise environments to support hybrid, multi-cloud, or on-premises deployments with ease. Vectra's cloud-native platform combined with Cybereason's lightweight agent forms a effective solution to combat against today's modern cyberattacks.

Built with 'Privacy by Design', the Cybereason and Vectra solutions start protecting enterprises from day one. Vectra's advanced machine learning techniques and always-learning behavioral models means accurate detection and high fidelity results from day one. Unlike other network detection tools, Vectra Cognito does not require a learning period. This combined with Cybereason's unique Malop™ approach and built-in threat hunting means security teams don't need to perform intricate configurations or waste time tuning complex and static rules.

Spanning network and endpoints to protect against the broadest spectrum of threats, security teams can leverage the joint Vectra and Cybereason solution to gain complete threat visibility and respond faster to cyberattacks.

ABOUT CYBEREASON

Cybereason is the champion for today's cyber defenders providing future-ready attack protection that unifies security from the endpoint, to the enterprise, to everywhere the battle moves. The Cybereason Defense Platform combines the industry's top-rated detection and response (EDR and XDR), next-gen anti-virus (NGAV), and proactive threat hunting to deliver context-rich analysis of every element of a Malop (malicious operation). The result: defenders can end cyber attacks from endpoints to everywhere. Cybereason is a privately held, international company headquartered in Boston with customers in more than 30 countries.

Learn more:
https://www.cybereason.com/

ABOUT VECTRA

Vectra® is an artificial intelligence company that is transforming cybersecurity. Its Cognito™ platform is the fastest, most efficient way to detect and respond to cyberattacks, reducing security operations workload by 34X.

Cognito performs real-time attack hunting by analyzing rich metadata from network traffic, relevant logs and cloud events to detect attacker behaviors within all cloud and data center workloads, and user and IoT devices. Cognito correlates threats, prioritizes hosts based on risk and provides rich context to empower response.

Cognito integrates with endpoint, NAC, and firewall security to automate containment, and provides a clear starting point for searches within SIEM and forensic tools.