VECTRA | superna

Vectra AI and Superna: Safeguard your data with an integrated and automated approach to security

Key Challenges

Having a large portfolio of security technologies is the norm for today's cybersecurity space. With the adoption of more and more hybrid environments, maintaining a cohesive security program continues to be a challenge that many organizations face, especially when it comes to detecting threats and responding to them with confidence and speed. Vectra AI and Superna's technical integration seamlessly bridges the gap between detection and response with automation playbooks and critical AI technologies.

Solution Overview

Combining Network security and Cyber Storage security with automation allows customers to execute automated playbooks that provide SOC teams with the tools they need to protect corporate data. The combination of network and storage playbooks provides a host to storage automation solution that simplifies data protection.

SOC administrators that leverage a SOAR platform for automation will be able to combine the early detection capabilities of Vecta AI and the proactive data protection capabilities of Superna.

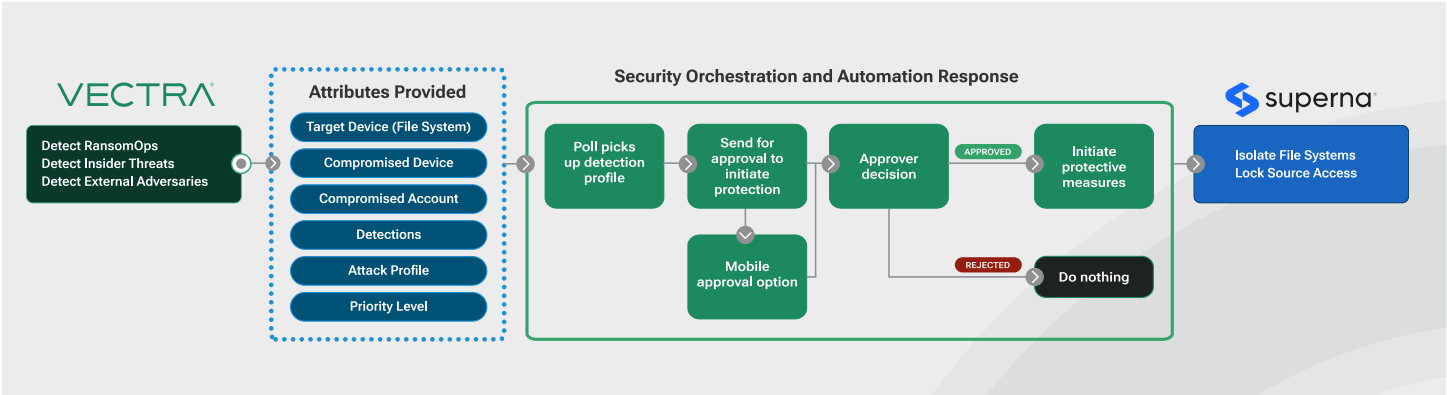
Solution Components:

- Automation playbooks
- Network and storage playbooks
- Real-time analytics
- Historic forensics
- Vectra AI Attack Signal Intelligence
- Superna Zero Trust

Key Benefits:

- Rapid, confident, and automatic response to threats
- AI-driven threat prioritization
- Mitigation before attack fully occurs, avoiding a costly recovery
- Real-time auditing and historical forensics for effective remediation

How it Works



Vectra AI uses advanced artificial intelligence to identify and prioritize suspicious activity early in the attack progression — before any damage is inflicted. When individual threats or attack profiles target data, Vectra AI notifies Superna through automation playbooks, so that critical data can be immediately placed into a protective, immutable state and lockout the compromised user account without impacting production data access for other users. Thus, securing the data and isolating the user's data access and preventing the need for costly recovery.

Additionally, Superna delivers its real-time analytics and historical forensics at the data layer, understanding when a nefarious activity timeline is critical to root cause and remediation. This advanced, real-time auditing and historical view of data activity helps secure and provide forensics to assist in root cause and impact radius of a compromised IT environment.

For samples playbooks to implement automation between Vectra AI and Superna Zero Trust, please visit Vectra AI's XSOAR GitHub repository.[1]

1. Vectra AI – Superna Critical Data Protection PlayBook
   a. You can run this playbook for any incident where data security is at risk and an immutable snapshot is needed to protect critical data. The snapshot can be used to recover data, and Cyber Storage analytics from Security Edition can detect malicious data activity and log file access. This is necessary to investigate the root cause of what data was affected by the malicious user or host.
2. User Request Storage Lockout Playbook
   a. Accepts an input question to accept the userID that should be locked out of storage. This playbook can be run by any SecOps workflow where the threat to data has increased and a proactive step to ensure no data can be destroyed.

About Vectra AI

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single XDR platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MXDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

About Superna

For more than a decade, Superna has provided innovation and leadership in data security and cyberstorage solutions for unstructured data, both on-premise and in the hybrid cloud. Superna solutions are utilized by thousands of organizations globally, helping them to close the data security gap by providing automated, next-generation cyber defense at the data layer. Superna is recognized by Gartner as a solution provider in the cyberstorage category. For more information, visit www.superna.io/superna-data-security-edition.

[1]These playbooks were originally developed using the Palo Alto Cortex XSOAR platform but can be easily translated to other automation tools.

For more information please contact us:
Email: info@vectra.ai | vectra.ai