VECTRA

Vectra AI Response Capabilities

Dive into all threat response capabilities available natively on the Vectra AI Platform, through technology integrations, and with Vectra MXDR (Managed Extended Detection and Response)

The Vectra AI Platform ensures end-to-end threat detection, investigation, and response for any hybrid environment. Understanding that threat investigation and response is not as simple as a single action on one platform, Vectra AI offers not only native response actions on the Vectra AI Platform, but also seamless, single-click pivot to response through technology integrations or reliance on the Vectra MXDR team for managed investigation, response, and remediation.

Native Vectra AI Response Capabilities

- Active Directory Lockdown
- Entra ID Lockdown
- EDR Lockdown

Vectra Automated Response Framework

The Vectra Automated Response Framework rapidly targets hosts and accounts that are observed behaving in ways above a user-defined security priority threshold on the Vectra AI Platform and sends immediate notification of such behavior via email and/or syslog, while issuing entity isolation actions to the configured third-party tools. Third party tools include but are not limited to:

- Bitdefender
- Call an external program
- Cisco AMP
- Cisco FMC
- Cisco ISE
- Cisco Meraki
- Cisco PxGrid
- ClearPass
- Endgame
- Fortinet Firewalls (FortiIOS)
- Harmony
- McAfee EPO
- Palo Alto Networks Firewalls (Panorama or not)
- PAN Cortex
- Pulse Secure NAC
- Sophos Firewall
- Static destination IP blocking
- Trendmicro ApexOne
- Trendmicro CloudOne
- Trendmicro VisionOne
- VMWare vSphere
- WatchGuard
- Windows (direct PowerShell commands to shutdown host)
- WithSecure Elements

Learn more about Vectra Automated Response Framework

Technology Integrations

CheckPoint

- Contain malware
- Quarantine and inspect files
- Block

CrowdStrike

- Lockdown account
- Kill process
- Run commands and scripts
- Automatic sandbox
- Containment

Cybereason

- Threat hunting
- Lockdown host
- Remediation
- Quarantine files
- Prevent file execution
- Isolate host

FireEye Endpoint Security

- Isolate host
- Collect and analyze data
- Remediation

Fortinet NAC

- Quarantine endpoint
- Remediation
- Trigger security configuration changes

Juniper Networks

- Isolate host
- Stop communication with C&C server
- Enable firewall policies

Microsoft Defender for Endpoint

- Block lateral movement and remote encryption
- Disperse deception techniques
- Stop communication with C&C server
- Containment
- Patch vulnerabilities

Nozomi Networks

- Trigger system backups and spares
- Enact incident response plan

Palo Alto Networks

- Quarantine hosts
- Extend blocking to PAN firewall
- Block

Palo Alto Networks Cortex XSOAR

- Trigger automated playbooks
- Analyze malware
- Cloud-aware incident response
- Threat hunting

SentinelOne

- Quarantine network
- Deploy agents on unprotected workstations
- Remove files
- Kill process
- Patch vulnerabilities
- Trigger security configuration changes
- Trigger automated playbooks
- Trigger policy enforcement
- Run forensics

ServiceNow

- Fetch detections
- Manage tags
- Download PCAP file
- Create security incident ticket

Splunk SOAR

- Block
- Lookup URL reputation
- Trigger automated playbooks
- Triage malware
- Disable hosts

Swimlane

- Trigger automated playbooks
- Stop communication with C&C server
- Stop data exfiltration
- Quarantine host

VMWare Carbon Black

- Block (operations, malware, malicious scripts, access)
- Restrict apps
- Delay execute for cloud scan
- Disperse deception techniques
- Prevent signature

Learn more about Response Integrations

Managed Response Capabilities

CrowdStrike

- Fetch detections
- Kill process
- Remove files
- Lockdown

Microsoft Defender

- Fetch detections
- Investigations
- Restrict app
- Quarantine file
- List exposed devices

SentinelOne

- Fetch detections
- Trigger security configuration changes
- Trigger policy enforcement
- Run forensics

Learn more about Vectra MXDR

Learn more about Vectra AI

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.

VECTRA®

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