VECTRA

BEST PRACTICES

5 Keys to Stopping Hybrid and Multicloud Cyberattacks on Critical Infrastructure

A playbook for defending Critical National Infrastructure (CNI) from cyberattacks and increasing SOC productivity by >2X.

Attack surface expansion continues to add complex security challenges for critical national infrastructure (CNI). This best practices document discusses the challenges facing CNI organizations and the necessary steps that security teams can take to successfully detect, prioritize, investigate and respond to the most urgent threats.

Chemical I Commercial I Communications I Critical Manufacturing I Dams I Defense Industry I Emergency Services I Energy I Financial Services I Food & Agriculture I Government Facilities I Healthcare & Health Services I Information Technology I Nuclear Power I Transportation I Water & Wastewater Systems

Key Challenges

- **Accelerating CNI organizations' capabilities** to identify, protect, detect, respond and recover from the attackers that successfully penetrate their systems. Manual analysis and detection lacks the scale and speed needed to efficiently detect and respond to today's attacks.
- **Slowing attackers' ability to compromise** valid credentials and launch attacks. Attackers avoid signature and anomaly-based detection by adopting user behaviors to mimic normal activity.
- **Detecting threats** in expanding, target-rich environments early enough to stop breaches due to a lack of security monitoring and controls for IoT and OT devices.
- **Successfully defending** against a near-infinite supply of tools that help persistent attackers spy, spread and steal inside the network.
- **Achieving continuous security visibility** and network monitoring to rapidly identify and respond to signs of active threats, recover from breaches and prevent new ones.

Security teams face unprecedented levels of threats and evasive attacks by a wide range of well-resourced, highly-skilled and motivated attackers. These sophisticated attempts target critical infrastructure to steal from, disrupt, damage or deny their digital-driven operations. In fact, the number of attacks launched on critical infrastructure by nation state groups doubled in the past year.[1] Security teams using AI/ML to correlate and prioritize the most critical and urgent threats specific to their environments will be best prepared to stay ahead of today's attacks. Vectra empowers security teams to do this with the Vectra platform, harnessing **Security AI-driven Attack Signal Intelligence™** to go beyond signatures and anomalies to understand attacker behavior and zero in on attacker TTPs across the entire cyber kill chain.

Five keys to success: Detect, prioritize, investigate, respond and hunt

Key #1 – Detection: Think like an attacker

To stop breaches, CNI security teams must think like an attacker. Vectra AI-driven detections go beyond signatures and anomalies to understand attacker behavior and zero in on TTPs across 4 of 5 attack surfaces — cloud, saaS, identity and networks. Vectra spots threats early by combining research, data science, ML algorithms, and behavioral analytics to detect malicious behaviors even when traffic is encrypted.

Key #2 – Prioritization: Know what is malicious, focus on the urgent

SOC teams deal with a high volume of daily alerts — knowing what is malicious is key. With AI-driven triage, Vectra quickly analyzes patterns unique to your environment to reduce alert noise and surface relevant and positive events. AI-driven prioritization provides analysts with unmatched signal clarity so they can focus on urgent threats instead of being overwhelmed by benign noise.

Key #3 – Investigations: Consolidate and integrate

Armed with a prioritized view of threats, SOC analysts can perform in-depth investigations from a single interface while providing a workbench for proactive threat hunting activities. With the Advanced Investigations feature, Vectra delivers a trail of threat context and forensic evidence for faster, more conclusive incident investigations and targeted containment actions.

Key #4 – Response: Integrated, targeted, flexible

SOC and CSIRT teams face increasingly longer threat response times (9 to 10 months on average) to identify and contain a breach[2] due to over reliance on manual tasks and a lack of workflow orchestration and process automation. The Vectra platform features native integrations for EDR, SIEM, SOAR and ITSM technologies, for fast, highly coordinated and targeted threat responses, with the flexibility of either manual or automated containment controls.

Key #5 – Hunting: Proactive and programmatic

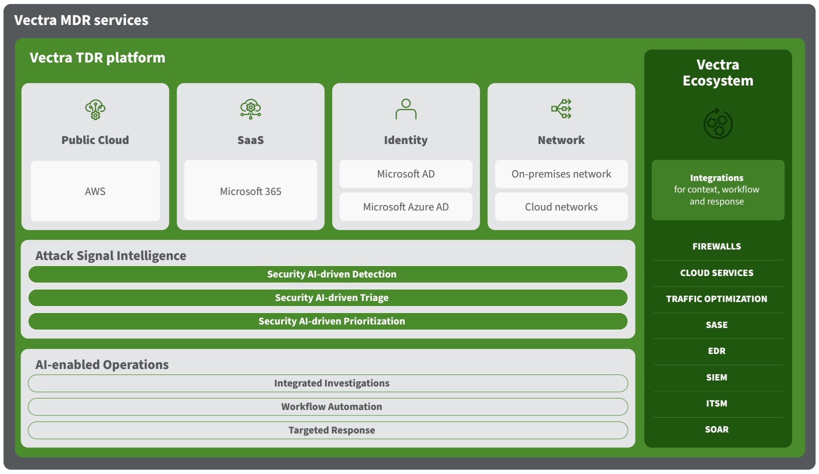
Armed with AI-driven detections that think like an attacker, advanced investigations, context-rich forensics and metadata ingested from networks, public cloud, SaaS, identity and endpoints, CNI red teams can deploy a proactive and programmatic practice to effectively detect and respond to threats.

Keys to success:

1. As your threat surface continues to expand, ensure that your security vendor will deliver coverage across all surfaces.
2. Work with a vendor that prioritizes signal accuracy so your team can focus on threats that pose the biggest risk.
3. Your solution should arm your human intelligence with tools needed to effectively detect, respond and investigate.

A more productive SOC

AI-driven threat detection and response solutions enable CNI SOC Leaders, CIOs and CISOs to get ahead of the steepening hybrid and multicloud threat curve — stopping attacks from becoming breaches. With continuous threat visibility across public cloud, SaaS, identity and networks, teams are enabled to detect signs of active threats to critical infrastructure. By deploying AI-driven threat detection and response, organizations will be more resilient to attacks with the capabilities to automatically detect, triage and prioritize threats — enable quick investigations and have the ability contain attackers that successfully penetrate the environment, raising SOC analyst productivity and throughput by >2X.



For more information, or to schedule a demo, visit https://www.vectra.ai/products/platform

About Vectra

Vectra® is the leader in hybrid cloud threat detection and response. Vectra's patented Attack Signal Intelligence detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

[1] 2022 Microsoft Digital Defense Report

[2] IBM Security Cost of a Data Breach Report 2022