VECTRA® SECURITY THAT THINKS® | MICRO FOCUS®

SOLUTION BRIEF

Integrating Cognito with ArcSight

MICRO FOCUS ArcSight Tested

The integration of the Cognito® cybersecurity platform with the Micro Focus ArcSight SIEM empowers fast, context-driven investigations into active cyber attacks.

Together, Cognito from Vectra® and Micro Focus ArcSight deliver a practical solution to the most persistent problems facing enterprise security–finding and stopping active cyber attacks, while getting the most out of the organization's limited time and manpower.

The need for a new approach to security

Modern cyber attackers easily penetrate traditional perimeter defenses that IT security teams have historically relied upon to keep networks safe.

The adoption of BYOD and mobile technologies have weakened these defenses and increased the network attack surface. Many network intrusions have resulted in massive financial losses, front-page news, brand damage, and tenuous job security for CISOs.

Unable to rely entirely on perimeter defenses, security teams are left to manually investigate threats, giving attackers an advantage as analysts are overworked as they dig through vast amounts of noise in search of a weak signal.

CHALLENGE

As attackers become more advanced, they are increasingly adept at penetrating the network perimeter and evading security controls to spy, spread, and steal inside the network.

These attacks evade firewalls and signature-based protections. As a result, today's security teams must perform manual, time-consuming investigations that fail to stay ahead of attackers, requiring a post-mortem analysis after key assets have been stolen or destroyed.

SOLUTION

The Micro Focus ArcSight Resource Package from Vectra provides bidirectional integration that ensures ArcSight users receive precorrelated threat detections that enable them to pinpoint and mitigate active intrusions.

The integration brings real-time detections as well as host threat and certainty scores from Cognito into the ArcSight platform, enabling further correlation with information and events within ArcSight, such as user names from Microsoft domain controllers.

Analysts can quickly search on any details from the ArcSight Management Console by pivoting back into the Cognito user interface or accessing packet captures of threats on demand.

BENEFITS

This integration saves time and manpower, reduces attacker dwell time, and speeds incident response before data is stolen or destroyed. It also enables real-time investigations by showing the infected hosts that pose the highest threat risk based on Vectra analysis, and automatically correlates those investigations with logs generated by other devices.

In practice, this means that breaches are first discovered after the fact and are reported by an external third party, turning the investigation into a forensic effort rather than a preventive exercise.

A new model of threat detection

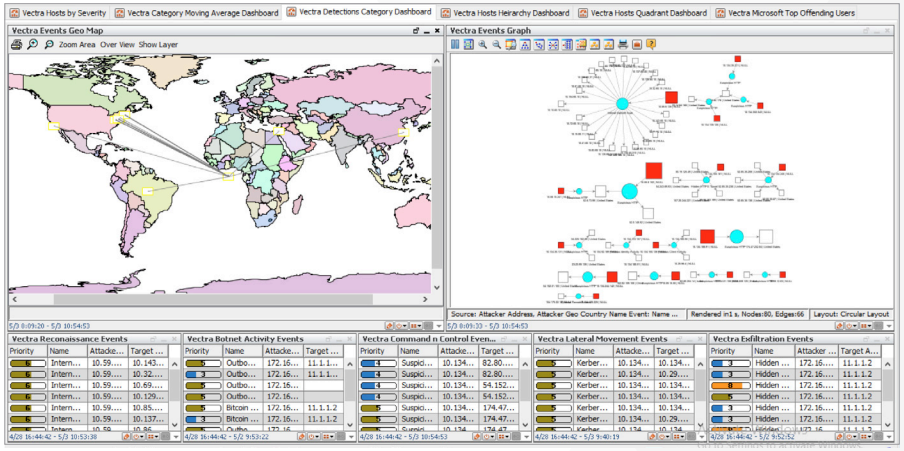
The Cognito automated threat detection and response platform detects threats in real time by analyzing the underlying behaviors of cyber attackers from the objective viewpoint of the network. This behavioral analysis of the network detects threats without signatures or reputation lists.

In addition, Cognito empowers security teams to detect new and unknown threats as well as attacks that do not rely on malware, such as malicious insider threats and compromised users machines.

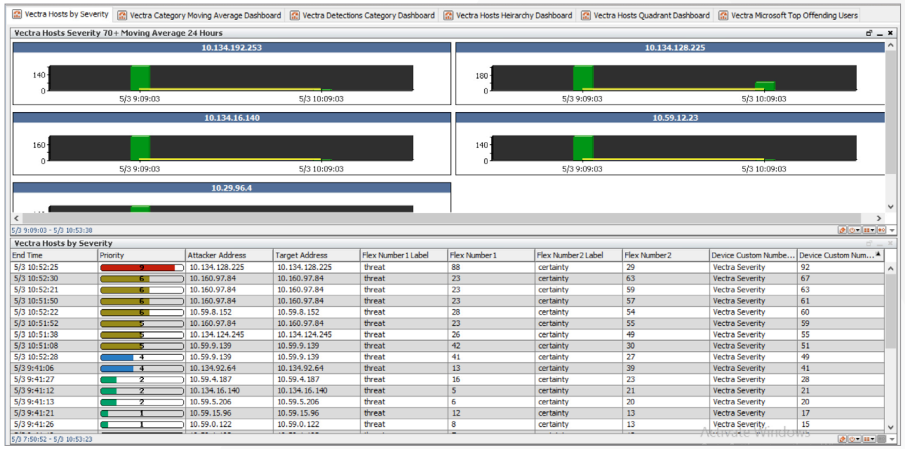
This unique intelligence is applied to all phases of an active cyber attack, ranging from command-and-control (C&C) server traffic, internal reconnaissance behaviors, lateral movement, and data exfiltration.

The Cognito and ArcSight integration brings all Cognito detections and host scores directly into the ArcSight dashboard, enabling them to be easily integrated into existing security operational center workflows.

The highly flexible Micro Focus ArcSight Resource Package from Vectra ensures that analysts have complete visibility into cybersecurity events and can pivot to any level of detail needed by security analysts.



A geographical map showing Cognito detection events



Cognito host detections over a 24-hour period ranked by severity

Key features

- **Automated correlation and integrated workflow** – The integration ties Cognito data to more than 240 ArcSight resource elements. This enables security teams to easily correlate Vectra data with any other data housed within.

  Security teams can easily correlate a Cognito event to user names in Microsoft domain controller events. Security teams can also feed Cognito data into ArcSight dashboards, build custom rules and integrations, and update active lists and filters.

- **Pinpoint hosts with the highest risk to the network** – Cognito automatically associates all malicious behaviors to physical network hosts – even if IP addresses or user roles change – and scores hosts in terms of their overall risk.

  Cognito integrates this information into the ArcSight platform, and accelerates incident response by eliminating the need for security analysts to manually investigate events. Precorrelated threat scores enable security teams to quickly build custom rules within ArcSight.

- **Visibility into threats across the kill chain** – The Cognito and ArcSight integration provides critical insight into specific threats as well as the progression of attacks across the kill chain.

  This unique visibility allows security teams to quickly distinguish opportunistic botnet behavior from more serious targeted threats and take action before data is stolen or damaged.

- **Deep investigation, on demand** – In addition to bringing Cognito information into ArcSight, integration allows security teams to pull additional forensics on demand or pivot into the Vectra user interface for additional investigation.

  While investigating an event, ArcSight users can leverage integration commands to quickly access a packet capture of the event in question in one click. This ensures that security analysts have everything they need to complete fast, conclusive investigations.About Vectra

About Vectra

As a leader in network detection and response (NDR), Vectra® AI protects your data, systems and infrastructure. Vectra AI enables your SOC team to quickly discover and respond to would-be attackers —before they act.

Vectra AI rapidly identifies suspicious behavior and activity on your extended network, whether on-premises or in the cloud. Vectra will find it, flag it, and alert security personnel so they can respond immediately.

Vectra AI is Security that thinks®. It uses artificial intelligence to improve detection and response over time, eliminating false positives so you can focus on real threats.

About Micro Focus

Micro Focus is a leading global enterprise software company uniquely positioned to help customers extend existing investments while embracing new technologies in a world of Hybrid IT. Providing customers with a world-class portfolio of enterprisegrade scalable solutions with analytics built-in, Micro Focus delivers customer-centered innovation across DevOps, Hybrid IT, Security and Risk Management, and Predictive Analytics. For more information visit www.microfocus.com.

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai