Integrating Cognito with IBM QRadar

The IBM® QRadar® Device Support Modules (DSMs) for Cognito

CHALLENGE

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

With attackers sidestepping the automated protections of firewalls and signature-based defenses, security teams have been forced to rely on time-consuming manual investigations and post-mortem analysis after damage has been done to the network.

SOLUTION

The integration brings Cognito real-time, precorrelated threat detections and host scores into the QRadar platform and automatically maps Cognito events to the appropriate QRadar categories.

This mapping via a dedicated DSM configuration for Cognito allows QRadar to use Cognito cutting edge threat detections and behavioral traffic analysis to easily build custom rules within QRadar to enrich the context of real-time threat investigations.

BENEFITS

The Cognito-QRadar integration saves time, effort, and enables security teams to take action before a network intrusion leads to data loss.

This enables fast, real-time investigations by showing the devices that pose the most risk to the network based on Cognito analysis, and automatically correlates those investigations with logs generated by other devices.

Together, the Cognito™ automated threat detection and response platform from Vectra® and IBM QRadar deliver a practical solution to the persistent problems facing enterprise security – finding and stopping active cyber attacks, while getting more out of an IT security team's limited time and manpower.

The need for a new approach to security

Attackers have repeatedly shown the ability to penetrate traditional perimeter defenses, which security practitioners have historically relied upon to keep networks safe. These breaches have resulted in massive losses, front-page news, and ever-declining job security for CISOs.

Unable to rely entirely on perimeter defenses, security teams have been left to investigate threats manually, resulting in overworked analysts digging through vast amounts of noise in search of a weak signal.

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

A new model of threat detection

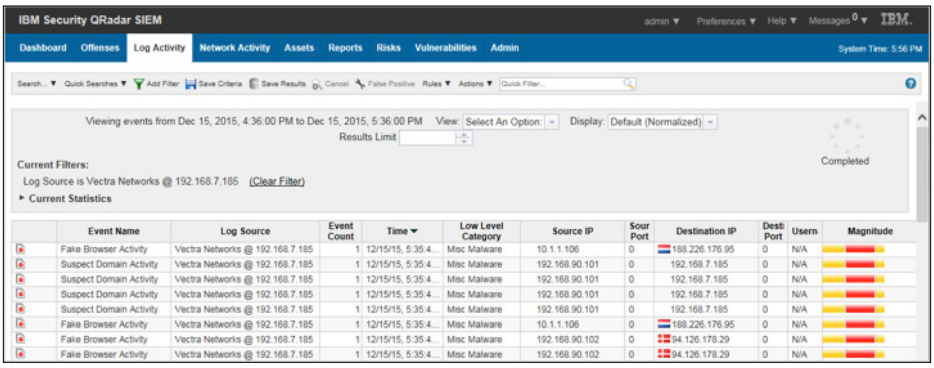
Using artificial intelligence, Cognito automatically detect threats in real time by analyzing the underlying behavior of attackers viewed from the objective viewpoint of the network.

This behavioral analysis of the network detects threats without signatures or reputation lists, and empowers security teams to detect new, custom or unknown threats, as well as attacks that do not rely on malware, such as malicious insiders or compromised users.

Cognito applies this intelligence to all phases of an attack, ranging from command-and-control traffic, internal reconnaissance, lateral movement, and data exfiltration.

The Cognito-QRadar integration brings all Cognito detections and host scores directly into the QRadar dashboard, allowing them to be easily added to existing security operational workflows.

Additionally, the integration allows IT security teams to use precorrelated Cognito detections to build fast and efficient custom rules within QRadar.



Key features

- **Automated mapping of Cognito detections to QRadar QIDs** – The integration between Cognito and QRadar leverages syslog protocol configuration and dedicated DSM technology to map Cognito detections to their corresponding QRadar QIDs.

  The Cognito DSM allows QRadar to automatically detect the log source and complete mapping, permitting users to automatically see Cognito events within QRadar along with the appropriate QRadar category and magnitude. This ensures that security teams can properly correlate and track all Vectra events and leverage them in the QRadar workflow.

- **Pinpoint hosts with the highest risk to the network** – Cognito automatically associates all malicious behaviors to the physical network host – even if the IP address or user role changes – and scores the host in terms of its overall risk.

  The Cognito-QRadar integration brings this information into the QRadar platform and improves response time by eliminating the need to manually investigate events. These precorrelated threat scores provide powerful ways to quickly build fast and efficient custom rules within QRadar.

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

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

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 168X. 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, firewall security to automate containment, and provides a clear starting point for searches within SIEM and forensic tools.

About IBM QRadar

IBM QRadar SIEM consolidates log events and network flow data from thousands of devices, endpoints and applications distributed throughout a network. It normalizes and correlates raw data to identify security offenses, and uses an advanced Sense Analytics engine to baseline normal behavior, detect anomalies, uncover advanced threats, and remove false positives.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai