Network Detection and Response: Making the Impossible, Possible

How to Detect Known and Unknown Threats with NDR

LogRhythm

TABLE OF CONTENTS

NDR
Making the Impossible, Possible

How to Detect Known and Unknown Threats with NDR

At the start of any James Bond movie, the British spy is given an impossible mission. More importantly, however, he's presented with a new car and a set of cutting-edge technological gadgets. In the end, Bond always completes his missions, but he couldn't do it without the technically advanced tools that are designed specifically for the task at hand.

Like Bond, you are charged with a seemingly impossible mission: stop all threats, including network-borne threats that bypass traditional controls — and do so as quickly as possible. Unfortunately, you aren't escorted to an underground laboratory where you're shown shiny new tools that will give you an advantage over the adversary. Instead, you're expected to pull off the mission with the software and resources you have today — some of which are five to ten years behind those used by cyberattackers.

Nevertheless, the mission is critical. The ability to detect and respond to advanced, persistent, and internal threats is crucial for preventing data exfiltration and IT service disruption. But organizations can't rely on their signature-based security tools to do the job, and few have the resources to continuously monitor the network to detect these threats. Those that do quickly find themselves inundated by false positives.

Fortunately, stopping network-borne threats isn't a truly impossible mission if you have the right solution for the job. Like Bond, you need advanced technology to complete your mission. Centralized, machine-based analysis of network traffic can help you gain visibility into these threats, making the impossible, possible. Effective response solutions, including efficient workflows and automated responses, allow you to take quick, decisive action.

This white paper will show you how you can obtain full coverage against both known and unknown threats when, like James Bond, you have the right technology for the right job.

Understanding Network Detection and Response

The Problem with Existing Tools

To a cyberattacker, an enterprise network is a poorly lit, virtual playground. Existing security tools essentially serve as spotlights scattered throughout the network, lighting up spots here and there, with blind spots in between. Like schoolchildren hiding behind a slide or running from tree to tree when the teacher isn't looking, attackers can use these blind spots to move laterally across the network or abuse access rights without detection.

Full visibility of the network is critical to an effective network security strategy. It's the only way to rapidly and effectively detect and stop advanced, persistent threats. Without visibility, these threats can spread quickly, evade detection by existing security tools, and cause substantial damage. Lack of visibility also enables threats to originate inside an organization's security perimeter, instantiating themselves with broad access across the network. For example, a rogue privileged user can abuse their access, or an attacker with legitimate access credentials can move about the network without raising suspicion.

Legacy security tools like NetFlow analyzers, next-generation firewalls (NGFW), and intrusion-detection and prevention systems (IDS/IPS) don't provide the visibility or response capabilities organizations need for detecting advanced network security threats that require broader analysis. Instead, they only provide restricted Layer 7 visibility with limited or no packet capture for further analysis. IDS/IPS engines, for example, typically focus on a single data point within packet data to identify malicious payloads, and they tend to miss other anomalies. Network monitoring software, which is typically oriented around IT operations, also focus on a single data point at a time. NGFWs provide visibility at only one point in the enterprise, and lack retrospective and advanced analysis functionality.

The problem extends beyond the network perimeter as well. Organizations have insufficient visibility into network security threats that require monitoring beyond the perimeter, such as in the cloud. IDS/IPS and traditional network security monitoring solutions focus on monitoring a single aggregating link. This requires enterprises to choose to either forego visibility (because they are only monitoring a single link) or to maintain multiple complex instances independently.

Time is of the Essence

Time is crucial when it comes to detecting and responding to advanced, persistent, and internal threats. Network-borne threats must be detected as quickly as possible to limit or avoid damage. The longer it takes, the more time attackers have to move laterally across the network, gain privileged access, and compromise systems in their search for valuable data. Without real-time awareness of security-relevant network activities, you will always be a step behind adversaries, and detection is not always early enough to prevent damage.

Manual forensic analysis and response efforts burden understaffed security organizations. Traditional network forensics solutions require extensive storage and skilled personnel, prohibiting a deeper level of network understanding beyond the few organizations that can justify the large investment.

You need advanced solutions that incorporate automation and integrated workflows to quickly identify and respond to network-borne threats.

This is key because many routine actions your team may take to respond to these threats can be automated, allowing you to focus on other matters. Most importantly, the response itself to these threats can be automated, reducing dwell time. For example, an account can automatically be disabled, or an IP address blocked in response to an attack, without requiring manual intervention.

The Network Doesn't Lie!

Network data often provides the earliest indicators of reconnaissance or compromise, but organizations must have the right data to see the threat and the right solutions to remediate it. Advances in centralized, machine-based analytics make it possible to more effectively detect network-borne threats, enabling your enterprise to better detect the presence of malicious actors within a network, as well as reveal the nature of threats and the extent of breaches.

Unified search across your enterprise's network traffic metadata is also critical for detecting network-borne threats. When coupled with powerful visualizations and analysis tools, unified search empowers threat hunting and accelerates incident response. Rapid access to the most relevant packet metadata and, if needed, the full packet capture, helps ensure these threats are detected and mitigated as early in the attack lifecycle as possible.

Centralized machine-based analytics and search come together in a network detection and response (NDR) solution. NDR is a subset of network traffic analytics/analysis (NTA), which is the process of collecting and analyzing network traffic. There are a lot of different approaches for addressing NTA, but the best approach is NDR. Where NTA focuses on real-time monitoring and analysis to detect suspicious activity, NDR goes beyond detection with comprehensive, rapid response, and mitigation capabilities to reduce risk. An NDR solution is a focused network security solution that detects advanced network-borne threats in real time and features integrated security orchestration, automation, and response (SOAR) capabilities.

NDR provides comprehensive network visibility, relevant insights, and rapid response options to help security analysts discover, investigate, and mitigate advanced threats across the network.

NDR addresses the need for continuous network monitoring and response to advanced threats. Unlike IPS and NGFWs, NDR analyzes multiple data points over time to recognize threat indicators. Response orchestration, including automation, reduces the time to respond to threats while eliminating manual, repeatable tasks. In short, NDR is the advanced technology security organizations need to complete their mission.

How NDR Works

NDR provides an integrated set of capabilities and workflows that enable you to detect, qualify, investigate, and respond to advanced threats more efficiently and effectively.

Detection

An NDR solution rapidly and efficiently detects threats before they cause damage. Using purposed, versatile sensors that generate rich network details, the most effective NDR solutions incorporate multiple machine analytics approaches to detect threats more effectively. These include:

- Scenario-based modeling for known tactics, techniques, and procedures (TTPs)
- Deep inspection of traffic metadata against known indicators of compromise (IoC)
- Behavioral analysis and anomaly detection to detect unknown threats

Cross-corroboration of different alarms provides high-accuracy threat detection without requiring heavy tuning or lengthy supervised machine learning training periods. Sensors are also utilized for distributed and high-scale network traffic acquisition. The sensors pick up all network traffic, not just logs. The sensor itself includes additional threat detection capabilities via an integrated deep packet analytics engine. The engine enables sophisticated, near real-time analysis of high-rate network traffic. The sensor also forwards application-aware network traffic metadata for broader centralized analysis and threat detection.

An effective NDR solution can recognize thousands of applications at Layer 7 with advanced analytics performed at wire speed to identify threat indicators as they emerge, without relying on lengthy learning periods or anomaly scoring, which is prone to false positives. To further reduce false positives, NDR can corroborate high-risk network activities at both the network and application levels. Such solutions can detect custom, company-specific threat scenarios without requiring data science or deep network forensics backgrounds.

Investigation

NDR empowers your team with real-time network insights and analytics. Risk-based and corroborated alarms can identify the most critical threats, so you don't get alarm burnout. Access to relevant, contextual information helps streamline your investigations. For example, an NDR solution can provide rich metadata, identification, and categorization of your enterprise's applications. An NDR solution can generate irrefutable network-based evidence for threat analysis, policy enforcement, audit support, and legal action.

Threat hunting is also made easier with NDR. You can quickly and easily identify suspicious activity. Dashboards provide views into suspicious IP addresses, categorized application traffic, and other valuable security information.

Response

You can accelerate and automate the security workflow when NDR solutions include SOAR capabilities. SOAR helps minimize response time, increase efficiency, and ensure high-quality incident response. SOAR also gives you the ability to easily automate a wide variety of investigative and response efforts aligned to determinations made through automated or search-based analytics to contain and eliminate threats.

Typical Architecture of NDR Tools

Figure 1: Process for network detection and response tools

LogRhythm NetworkXDR

Technology for a Successful Mission

LogRhythm NetworkXDR is an NDR solution that provides full coverage against known and unknown threats. It provides an integrated set of capabilities and aligned workflows for detecting, qualifying, investigating, and responding to advanced threats that can only, or best, be seen through the centralized analysis of network traffic data. LogRhythm NetworkXDR can help detect and respond to both known and unknown network-borne threats and related incidents, including:

- The transfer of data to unauthorized cloud services
- Malware traffic missed by traditional security tools
- Major breaches of industrial control grids
- The harvesting and exfiltration of data by malicious insiders

LogRhythm NetworkXDR recognizes applications at Layer 7, bringing immediate visibility to the applications on the network. To enable more accurate machine-based analytics, the solution generates rich metadata, nuanced by the application type. Analytics are performed both at the sensor and centrally, economically distributing resource consumption while providing optimal insights into malicious activity.

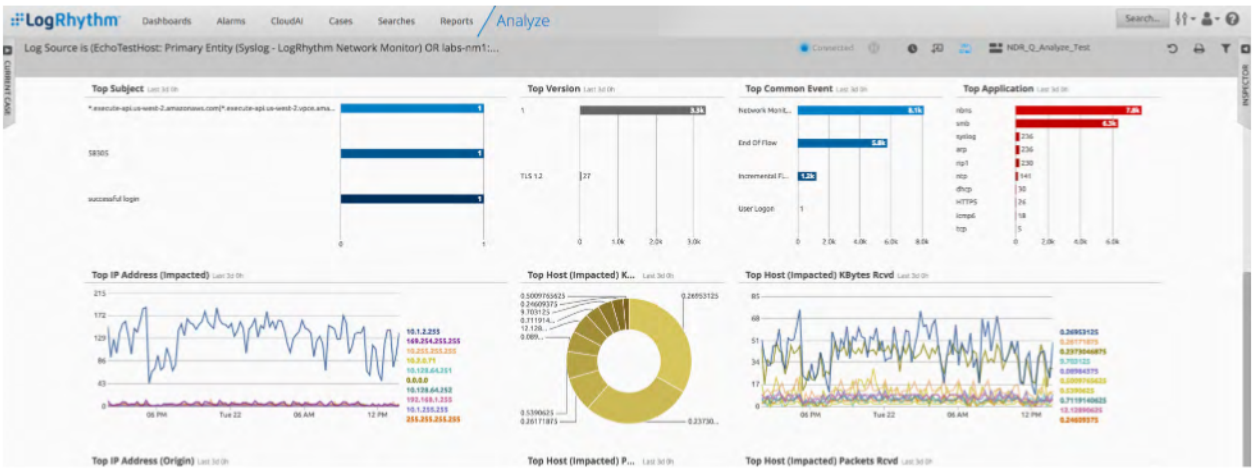

Figure 2: Network visibility integrated within in the LogRhythm NextGen SIEM Platform

The software-based sensors acquire data in a variety of ways, including from a network TAP, SPAN port, GRE connection, or third-party packet broker. Virtual sensors improve visibility into cloud infrastructure. Customizable dashboards, widgets, and guided workflows help analysts recognize and mitigate threats effectively, providing fast and immediate forensic drilldown. Full and intelligent selective packet capture is available for when you need complete detail. You can also replay captured data for additional analysis or search rich Layer 2-7 network traffic metadata. LogRhythm NetworkXDR easily integrates with existing hardware and can be deployed as a dedicated hardware appliance or virtual machine.

SOAR capabilities, including playbooks, can also help further accelerate threat investigation and response efforts. Guided, customizable playbooks give your team tracking, documentation, and enforcement of defined workflows. They support multi-party approval and help increase productivity and consistency. SOAR also includes case management for end-to-end collaboration and management of alerts, evidence, and escalations. Automated, flexible, and scriptable responses increase investigative efficiency. Metrics help measure and improve SOC responsiveness.

Benefits of LogRhythm NetworkXDR:

- **Gain the speed and full visibility** required to combat network-borne attacks across your on-premises, remote, and cloud environments—with a single solution
- **Detect custom company-specific threat scenarios** without requiring data science or deep network forensics backgrounds
- **Empower incident responders** with real-time network insights and analytics, allowing them to catch threats before there is damage
- **Reduce alert fatigue** with cross-corroborated, high-fidelity alerts
- **Accelerate and automate** your security workflow with embedded SOAR capabilities
- **Grow your security operations** maturity at your own pace thanks to integration with SIEM for a flexible, end-to-end platform

SIEM and NDR: Better Together

By itself, NetworkXDR offers immediate value and ease of use without requiring sophisticated network forensics experience—but it gets even better. NetworkXDR is a complete solution enabled through the same advanced security analytics, centralized search and visualizations, and SOAR functionality as the LogRhythm NextGen SIEM Platform. This integration delivers even more value to IT organizations.

The shared capabilities with the LogRhythm NextGen SIEM Platform make NetworkXDR expandable to grow with the organization. NetworkXDR is fully configurable with the option to add capacity and log sources, such as NetFlow, IPFIX, and network infrastructure and security log data. You can use excess capacity to monitor additional network and log data sources or add capacity to fulfill additional security use cases across other attack surfaces, such as endpoint and user (UEBA) activity.

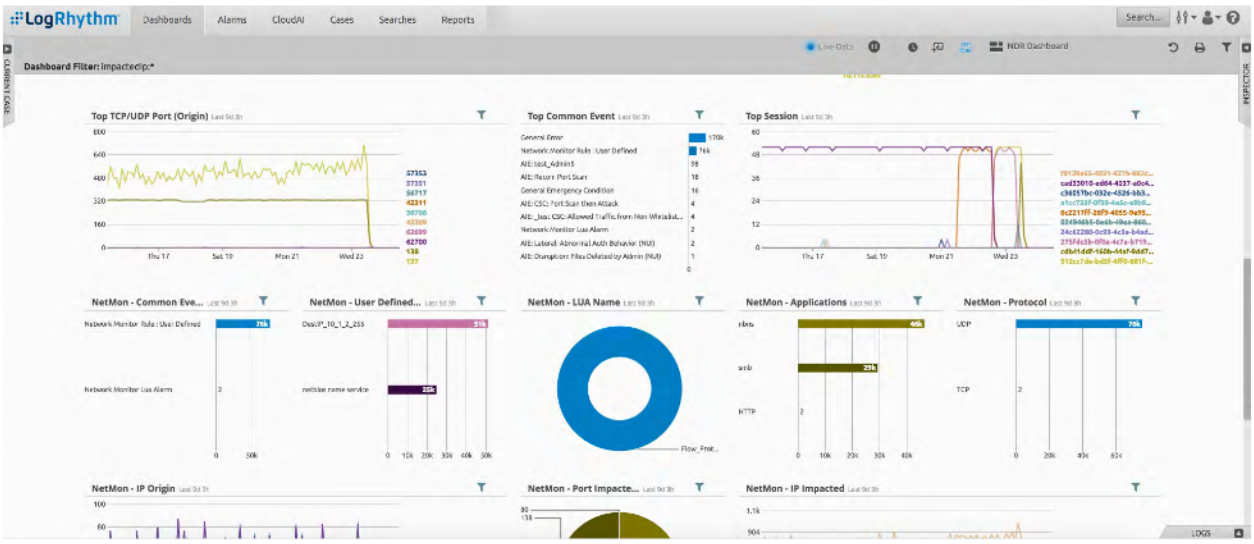

Figure 3: Dashboard of the NetworkXDR integration with the LogRhythm NextGen SIEM

NetworkXDR in Action

Four Use Cases for Network Detection and Response

LogRhythm NetworkXDR addresses a wide variety of network-borne threats, including network reconnaissance, compromised hosts/devices, lateral movement, data exfiltration, command and control detection, and ransomware. Let's look at several use cases where LogRhythm empowers security organizations to detect and remediate advanced, persistent, and internal threats.

Detect and Stop Data Transfer to Unauthorized Cloud Services

There are thousands of cloud services and applications, with new ones emerging daily. Their popularity continues to grow due to how easy it is to share information with co-workers, contractors, and even between their personal devices. The problem, of course, is that sensitive, proprietary, or confidential data can potentially be exposed to malicious actors when it's shared on personal devices. The earlier these data transfers can be detected and investigated, the lower the risk of data loss to an organization. That's where NetworkXDR comes in.

You can deploy NetworkXDR sensors at key points throughout your network to analyze traffic in real time and analyze thousands of applications – including cloud services. NetworkXDR can alert on transfers to and from these services and take automated action. Automated response options include blocking the origin IP from inbound and perimeter firewalls, quarantining a host, adding users to watchlists for further assessment, disabling user accounts, and more.

Sophisticated tools give your team control to either observe and collect more data, including full packet captures, to respond manually, or to initiate an automated response. The solution also supports detection and tailored metadata extraction for dozens of cloud services and thousands of protocols. Organizations can explicitly whitelist or blacklist individual applications and give visibility and control back to the security team.

Detect and Respond to Malware Traffic

Malicious actors use a variety of techniques in their malware to evade detection by point solutions like endpoint protection platforms and IDS/IPS. Because NetworkXDR looks at the entire network, it can detect malware that other security controls miss. For a real-world example, a security analyst experienced the following scenario himself.

An endpoint on his organization's network was causing a built-in NetworkXDR Deep Packet Analytics rule for a suspicious top-level domain to fire an alert. At first, the analyst thought it was a false positive because the organization's other security tools showed the endpoint to be clean. He pulled in additional information from the endpoint using the LogRhythm SysMon agent and saw which process was responsible for outbound communications. It was "svchost.exe" communicating over HTTP outbound to the suspicious domain. The analyst used automation to remove the endpoint from the network and ran follow-up scans with other tools to confirm the endpoint was indeed infected.

By using built-in rules in NetworkXDR, the analyst was able to quickly detect suspicious network activity that existing security systems missed. He was able to efficiently identify, remediate, and contain the issue in short order even when their other security tools weren't raising the alarm due to NetworkXDR's deep packet analytics.

Protect SCADA Systems Against Cyberattacks

Supervisory Control and Data Acquisition (SCADA) systems are critical for industrial organizations, such as oil and gas companies, electric utilities, and automotive manufacturers. SCADA systems typically communicate through the ubiquitous Modbus SCADA protocol. Unfortunately, this antiquated protocol lacks security, encryption, and authentication controls. Attacks against SCADA systems can cause extensive damage, including loss of life.

NetworkXDR provides real-time visibility into SCADA environments. It can be deployed in a variety of locations to inspect the traffic flow between devices. It collects network traffic, identifies the specific Modbus protocol (as well as over 20 other SCADA protocols), and decodes packets in real time. NetworkXDR is also flexible enough to allow you to choose which write functions to alert on.

By detecting and responding to compromises, NetworkXDR helps prevent major breaches of industrial control grids. A LogRhythm customer experienced this firsthand. The organization deployed NetworkXDR in their SCADA environment and configured the solution to alert on specific Modbus functions that an analyst would rarely expect to see. NetworkXDR detected and alerted on the unexpected function. The analyst was able to immediately investigate the activity, determine that the action was unauthorized, and remediate the incident before any damage was done.

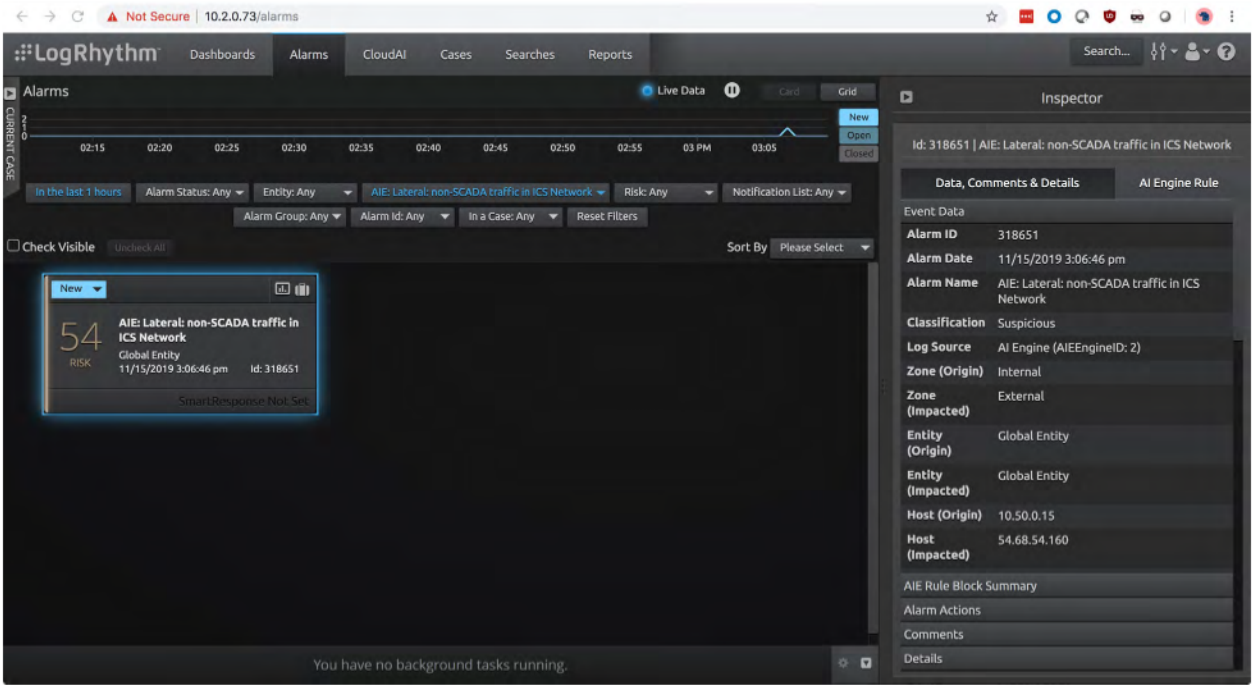

Figure 4: Web Console displaying non-SCADA traffic coming from a SCADA entity

Detect and Act on Insider Threats

Trusted insiders represent a great risk, regardless of industry or the size of the company. For instance, a disgruntled employee planning to leave the company can easily take proprietary information to a new employer or a competitor.

NetworkXDR can automatically detect and act on potentially damaging insider threats, protecting your organization's sensitive and valuable information. It detects early activities that are indicative of an insider threat, such as attempts to access certain internal file repositories or other unusual attempts to access files.

NetworkXDR also alerts on network activity like large file transfers. Such alerts are corroborated and elevated based on the severity of the threat.

Once the insider threat is detected, either manual or automated action can be taken with NetworkXDR. In the manual action, you can automatically create an incident case in NetworkXDR and prepopulate it with data relevant for an investigation, including rich network session metadata. Or, it can take automated action and immediately quarantine the account, limiting data loss.

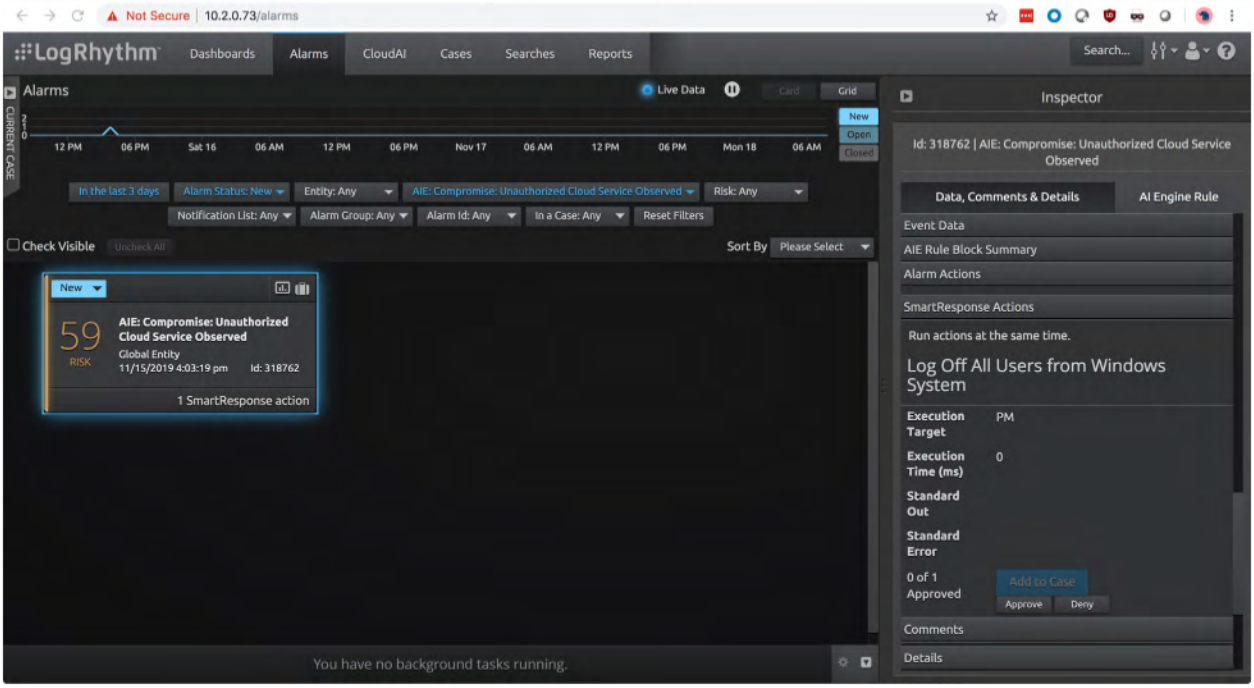

Figure 5: AIE alarm for unauthorized cloud services observed with a suggested SmartRespose action

CONCLUSION

It's your job to detect and respond to network-borne threats in a timely manner. It seems like an impossible mission, but only because the tools you have are unfit for the job. The mission becomes possible once your team is armed with the right data to see the threat and the right solution to remediate it. Network detection and response is that solution.

LogRhythm NetworkXDR is capable of surfacing threats that evade detection by traditional tools, yet it is intuitive, so you don't need sophisticated network forensics expertise to accomplish your mission. It uses the power of the LogRhythm NextGen SIEM Platform to deliver a full range of real-time network monitoring, forensics, and analytics capabilities, alongside comprehensive case management and automated incident response. With NetworkXDR, your team can better understand your organization's exposure to network-borne threats while strengthening its overall security posture and threat resiliency.

Curious how NetworkXDR can help your team defend your network? Schedule a demo today. www.logrhythm.com/demo

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301