Data Sheet

# The LogRhythm Current Active Threats Module

LogRhythm
The Security Intelligence Company

When the next WannaCry or NotPetya strikes, you must act immediately to ensure you protect critical assets and detect targeted or compromised systems. However, within a dynamic threat landscape, it's difficult to remain confident in your ability to protect your organization against fast-moving, high-impact attacks.

While patching systems is an effective method for dealing with exploits, patching delays are common for several reasons, including lagging vendor response times, application dependencies, and performance concerns. This leaves your systems vulnerable.

## Detect Known and Unknown Threats

LogRhythm's Current Active Threats (CAT) Module is designed to recognize and alert on newly discovered and critical threats. With the CAT Module, the LogRhythm Labs team does the resource-intensive work for you, gathering and synthesizing threat intel, performing malware analysis, and studying persistent bad actor methods. They are also experts at quickly creating analytics content to recognize these new threats. To best protect your data and assets, new content is rapidly provided directly to your LogRhythm NextGen SIEM Platform.

Like LogRhythm's other Threat Detection Modules, the CAT Module is available at no charge to current LogRhythm customers through the Knowledge Base (KB) update.

### LogRhythm's Current Active Threats Module Benefits:

- **React faster**
  - Within 24–48 hours from the first announcement of a newly discovered threat, be assured you can detect it and have mitigating controls in place
  - Secure your company, inform your board of directors, and calm your customers faster with a prompt response to emerging threats
- **Act automatically**
  - LogRhythm identifies major new attacks and quickly provides relevant content directly to your LogRhythm platform
  - Content is activated automatically to ensure rapid protection
- **Conserve resources**
  - Let LogRhythm Labs' embedded intelligence to do threat validation, malware analysis, and rule creation for you
  - Augment your SOC with pre-tuned AI Engine content that identify and alert on IOCs
  - Focus on threat remediation, not intensive IOC analysis

## How it Works

The CAT Module consists of:

- Pre-tuned AI Engine content focused on recognizing trending industry threats
  - AI Engine content is based on LogRhythm Lab's reverse malware analysis and network behavior analysis, recognizing how threats are manifested in log and network data. The content spots specific indicators of compromise (IOCs) of threats (e.g., IP addresses, hash values, specific command-line prompts, and registry keys).
  - Leveraging LogRhythm's Machine Data Intelligence (MDI) Fabric and Lists, CAT Module content is vendor-agnostic, allowing you to take immediate advantage without additional tuning requirements or restrictions per your underlying infrastructure.
  - New content is delivered through the KB in as little as 24–48 hours of a credible new threat disclosure and automatically activated.
- Canary lists
  - Like a canary in a coal mine, canary lists contain early indicators of potentially harmful events. While one canary event may not be too suspicious, several canary events increases the probability of an actual attack.
  - The CAT Module currently has seven canary lists:
    - Hash values
    - Process names
    - Process paths
    - Registry keys
    - Domains
    - IP addresses
    - User names
- Web console dashboard
  - Quickly visualize current threat status and drill down to critical data.

## CAT Module in Action

The CAT Module detects both known and unknown threats. The module takes a different approach to both types of threats to ensure IOCs are recognized and your security team is rapidly alerted.

### Known Threats

Many cyberthreats have already been identified, analyzed, and patched, but systems in your environment may still be vulnerable. Take NotPetya as an example: This disk-wiping malware propagates quickly, sometimes only needing to infect one machine to take down all systems in your network. Catching a threat this serious is paramount for security teams. Fortunately, LogRhythm Labs has researched NotPetya and knows the specific IOCs (e.g., hash value, file names, and IP addresses). They have created content to identify and alarm if any of NotPetya's IOCs are hit. This content is provided automatically to your LogRhythm NextGen SIEM Platform through the CAT Module. As any NotPetya IOC is indicative of infection, all NotPetya IOC-related alarms have a high risk-based prioritization (RBP) score, ensuring they're displayed at the top of your LogRhythm dashboard so your team sees them immediately. Once alerted, your team can act (e.g. quarantine a compromised endpoint or disable a suspect user account) to stop the attack before infection spreads.

### Unknown Threats

New threats arise constantly. These threats (typically referred to as emerging threats) require highly experienced analysts to identify, investigate, and contain. The CAT Module's core capabilities are designed around detecting these emerging threats. The module identifies emerging threats in your environment using canary lists, comprised of suspicious IOCs often present during the initial stages of an attack against an endpoint. Due to the relatively high false-positive rates these indicators can represent, the CAT Module uses analytics that recognize the progression of an attack, dynamically raising the risk-based prioritization (RBP) score of generated alarms based on the number of canary list IOCS a single endpoint or user has experienced. For example, if an endpoint generates four events matching IOCs on four separate canary lists or within the same canary list, the CAT Module will generate an alarm with a higher RBP value than if that same endpoint only generated two IOC events. This provides your security analysts an opportunity to identify an emerging threat early within the Cyber Attack Lifecycle and take remediation steps before the threat has a chance to significantly embed itself in your environment.

### LogRhythm Labs

The LogRhythm Labs team delivers security research, analytics, incident response, and threat intelligence services to protect organizations from damaging cyberthreats. The team created and maintains LogRhythm's Holistic Threat Detection Suite, including the User and Entity Behavior Analytics (UEBA) Module, the Network Threat Detection Module, and the Core Threat Detection Module, as well as a range of industry-specific and compliance mandate-specific module offerings. These offerings are updated regularly and are offered to LogRhythm customers at no cost.

## Additional Reading:

- Documentation: User and Deployment Guides on LogRhythm Community
- Dashboard: CAT Module dashboard on LogRhythm Community