PRODUCT OVERVIEW

Threat Management Foundations (TMF) Service

Organisations get the most value from their LogRhythm deployment when it becomes part of their daily routine, used not just for log management or compliance automation, but for end-to-end threat detection and response. That's why we've created our Threat Management Foundations (TMF) Service. It pairs you with a dedicated LogRhythm consultant who helps you maximise your LogRhythm deployment's threat management capabilities.

Is TMF Service right for your organisation?

Are you concerned that threats might be slipping through the cracks? Do you want to make sure you get the most value out of your LogRhythm investment? If you aren't yet using LogRhythm for end-to-end threat management, you should consider TMF Service. It helps you leverage LogRhythm to detect and respond to the threats facing your organisation.

TMF Service At-A-Glance

- ☑ Implement Core Threat Detection module
- ☑ Tune analytics to realise risk-prioritised alarms for your environment
- ☑ Document operational procedures
- ☑ Install Smart**Response**™ plug-ins for automated user and endpoint lockdown
- ☑ Validate deployment configuration based on LogRhythm best practices

How TMF Service works

TMF Service is designed to accelerate attainment of your most important security goals. We guide you through the implementation of the most important components of your Security Intelligence Platform. Once this is done, you have tools in place to protect you from several user and endpoint compromise use cases.

TMF Service checklist

- ☑ Implement the Core Threat Detection Module, designed to detect compromised accounts and endpoints:
  - ☑ Deploy threat detection dashboards
  - ☑ Configure and optimise threat detection rules
- ☑ Optimise LogRhythm to identify threats and prioritise alarms:
  - ☑ Configure AI Engine
  - ☑ Tune key environmental risk characteristics
  - ☑ Set up whitelists and blacklists
  - ☑ Enable and tune open source threat intelligence feeds
- ☑ Document processes and train:
  - ☑ Alarm monitoring and qualification
  - ☑ Threat investigation
  - ☑ Incident response
- ☑ Enable automated responses, and any applicable approval workflows for disabling compromised accounts and endpoints

TMF Service helps you use LogRhythm's machine analytics, integrated threat intelligence, and incident response orchestration and remediation capabilities, helping you detect and respond to compromises before they become damaging breaches.

Threat detection use cases

Threat Management Foundations Service helps customers begin using machine analytics to protect their organisation from cyber threats. The service's keystone is the implementation of our Core Threat Detection Module (CTDM), a powerful set of security analytics tools that can reveal a wide range of suspicious activity, such as:

Account compromise use cases

Compromised VPN account A legitimate user's VPN account is compromised by an attacker. LogRhythm finds the attacker when he authenticates from a new origin host or when he establishes a simultaneous connection.

Account probe An unsuccessful account probe from an external source with the idea that an attacker knows a password but not the user name.

Privilege escalation after attack This is an indicator that the initial attack was successful and that the malicious actor is moving further into the attack cycle.

User created and then added to admin group Tracking administrator actions is useful both for auditing potential privilege abuse and for security monitoring. This rule will alarm when an account is added to a group that has elevated privileges.

Endpoint compromise use cases

Compromised endpoint An IDS detects malicious hacking activity from a host. Later, LogRhythm sees the same host successfully authenticating with an internal host, indicating a successful network penetration.

Connection to TOR exit node Internal connections to TOR exit nodes indicate that someone on the network has a compromised host or that users are intentionally hiding their network activity from inspection.

Compromised endpoint A worm is successfully spreading throughout the network.

Malware outbreak Several malware events emanating from different hosts within the organisation may be an indication that malware has begun to spread throughout the network.

TMF Service outcomes

Achieve rapid time-to-value on your security investment.

Detect and quickly neutralise compromised accounts and compromised endpoints.

Establish effective monitoring, investigation and incident response processes for your organisation.

Protect your organisation from a data breach or other damaging cyber incident.