Advantage®

TAILORED TECHNOLOGY SOLUTIONS

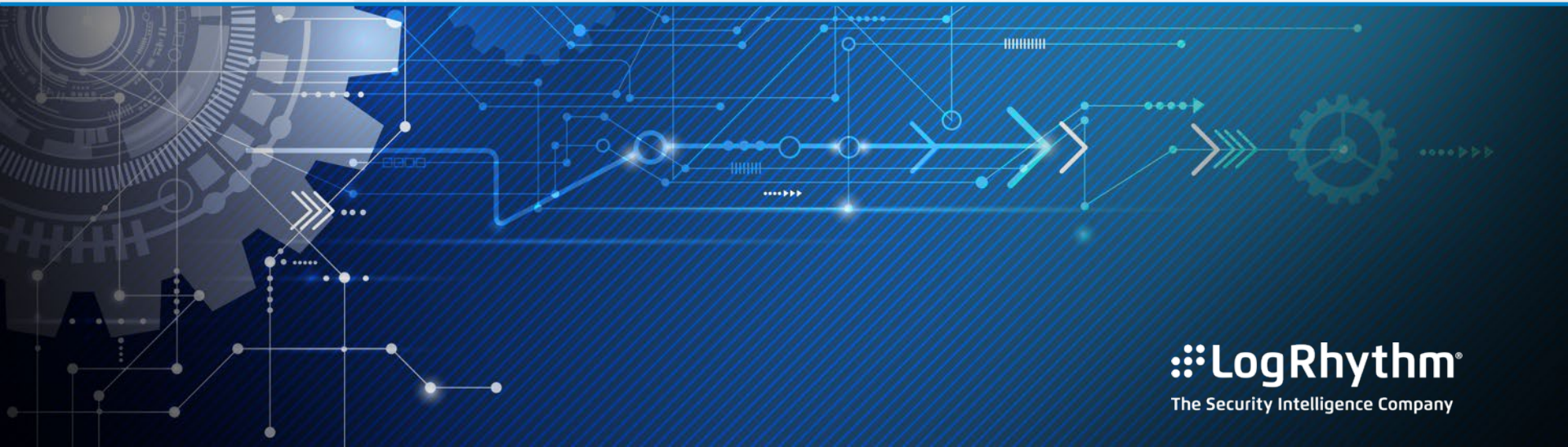
LogRhythm®

The Security Intelligence Company

CHILLISOFT

“Avoiding message fatigue”

Simon Howe, APAC Director
Karthik Murthy, Senior Architect



Advantage
TAILORED TECHNOLOGY SOLUTIONS

LogRhythm
The Security Intelligence Company

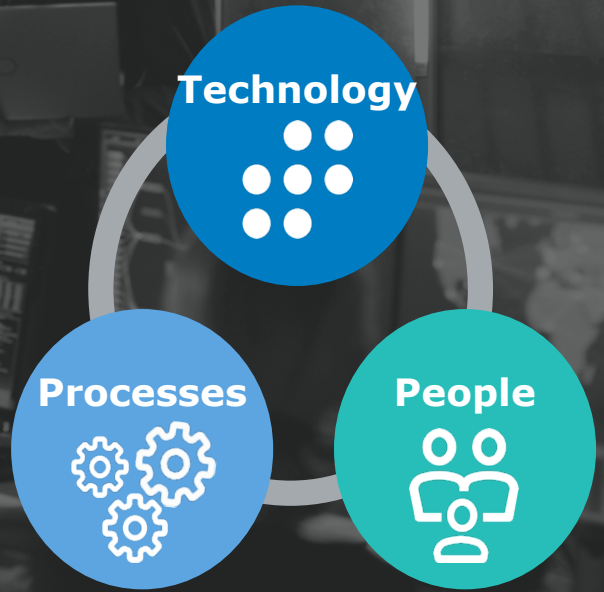
The SOC Mission

The heart of Security Operation Center (SOC) mission is to execute the following programs:

- ✓ **Threat monitoring**
- ✓ **Threat hunting**
- ✓ **Threat investigation**
- ✓ **Incident response**

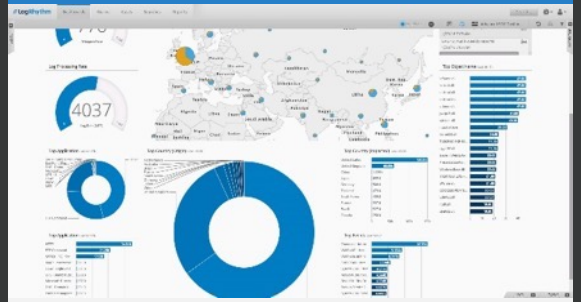
"The SOC is a team, not a facility."

Gartner: How to Plan, Design, Operate and Evolve a SOC



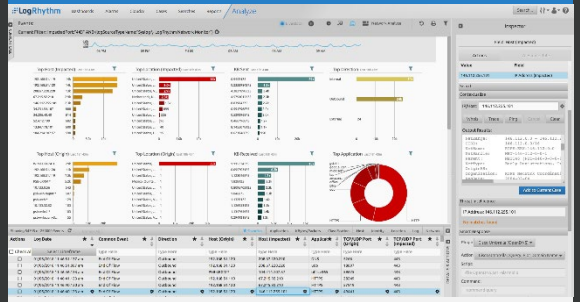
Single integrated platform for Security Operations

Threat hunting



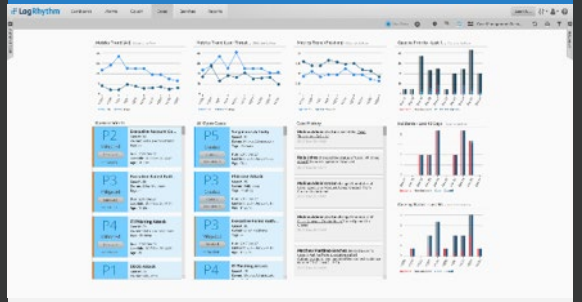
- Access to a library of OOTB widgets, all updating in real-time to surface high-risk activities
- Customisable options and filtering across over 100 searchable fields present the right details in the most effective way
- Guided search enables immediate access to underlying evidence

Threat Investigation



- Colour-coded charts for quick recognition of risky activities
- Access to OOTB and custom contextual lookups (e.g., AD, threat intel, WHOIS) for fast recognition of related evidence
- Immediate access to underlying log data enable quick sorting and column filtering to hone in on pertinent data

SOC management

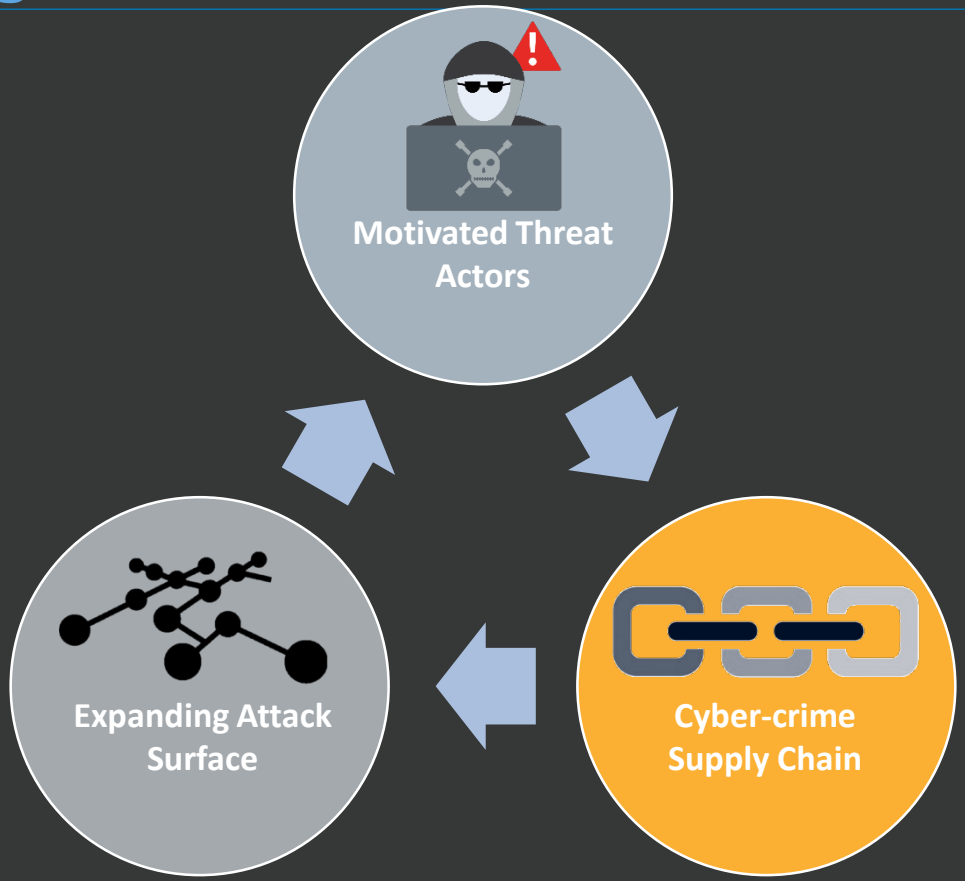


- Access to customisable activity trends views show overall risk
- Case metrics and trends enable continual improvement in organisational effectiveness
- Filtering dashboards by case tags reveals effectiveness across different threat types

LogRhythm's Threat Lifecycle Management Framework

Our Threat Lifecycle Management (TLM) Framework, describes the collection of integrated operational capabilities required to realize the SOC mission.

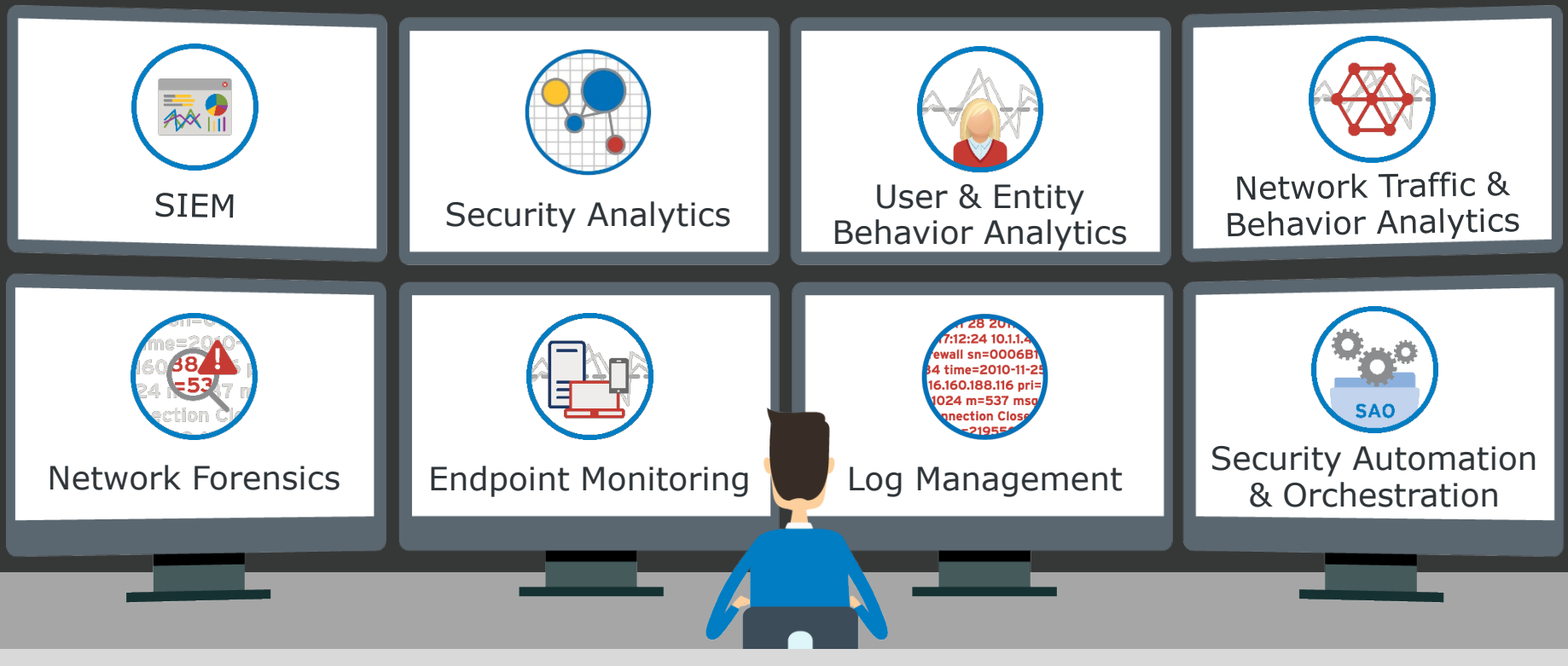
No End In Sight



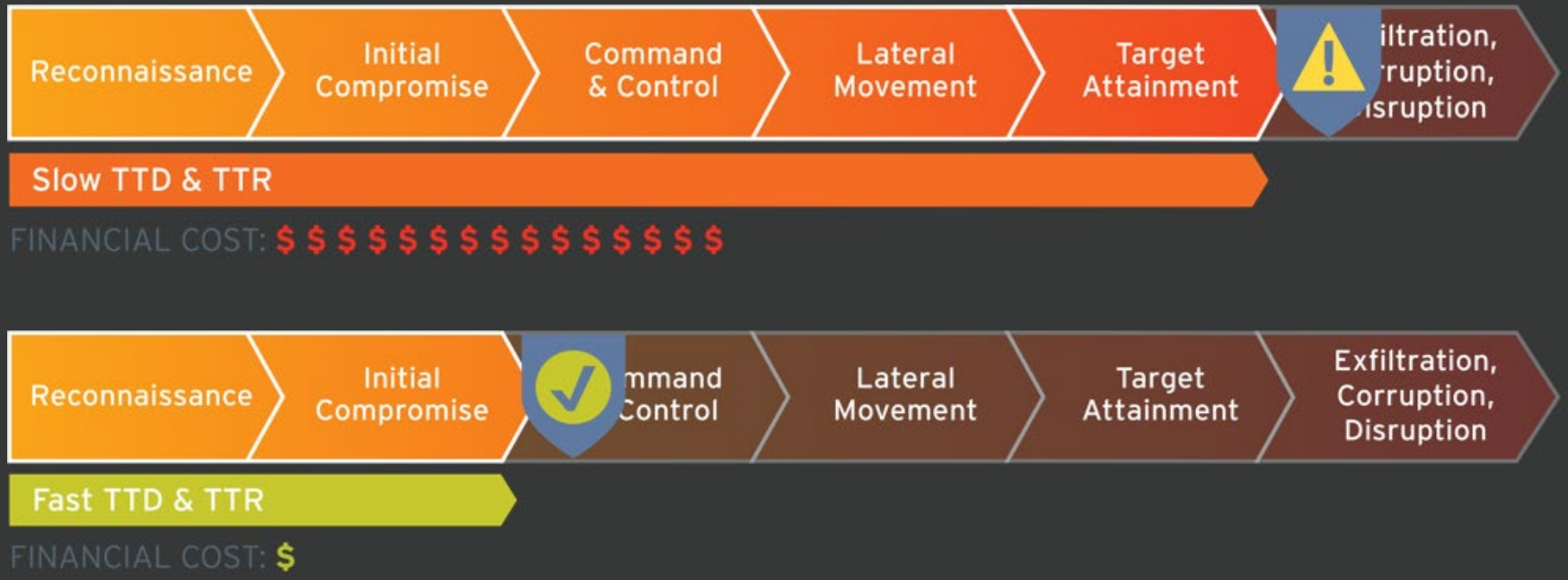
Organizations Continue to Struggle

IT / OT Environment Challenges	Threat Landscape Challenges	Operational Challenges
Digital Disruption	Expanding Attack Surface	Alarm Fatigue
Perimeter erosion	Motivated Threat Actors	Cost of Operation
Volume of Data	Cybercrime Supply Chain	Workflow Efficiency

Inefficient Workflow and Swivel Chair Insanity



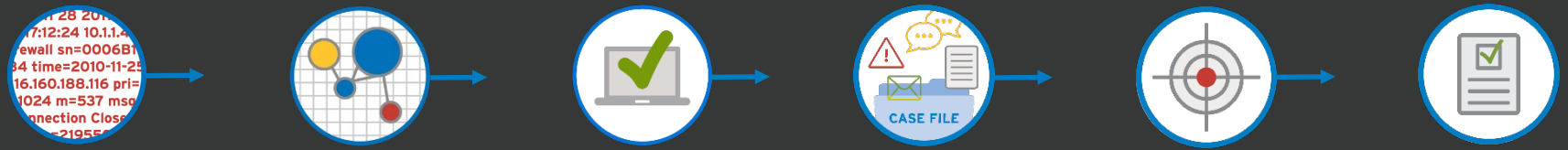
Effective Enterprise TLM Reduces Cyber-incident Risk



The Fundamental Goal of a NextGen SIEM Platform

Deliver enterprise Threat Lifecycle Management, of highest efficacy, at lowest TCO

LogRhythm's NextGen SIEM Platform



Forensic Data Collection | Discover | Qualify | Investigate | Neutralize | Recover

SOAR — Security Orchestration, Automation and Response

SIEM | UEBA | NDR | EDR — Security Analytics

powered by LogRhythm CloudAI and AI Engine

Data Collection
Endpoint Monitoring
Network Monitoring

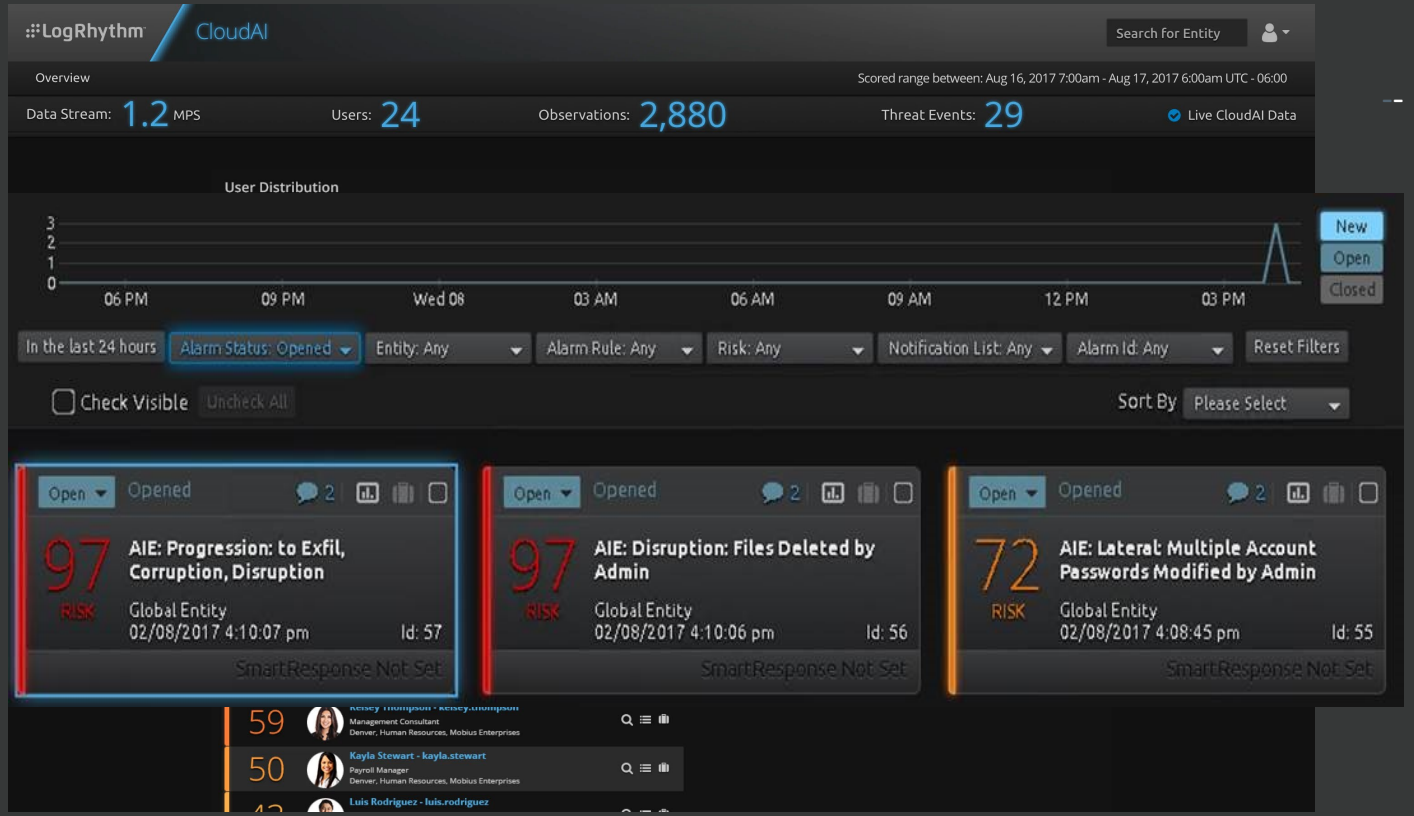
MDI Fabric

Enterprise Log Management

Enterprise Security Data Lake

powered by Elasticsearch

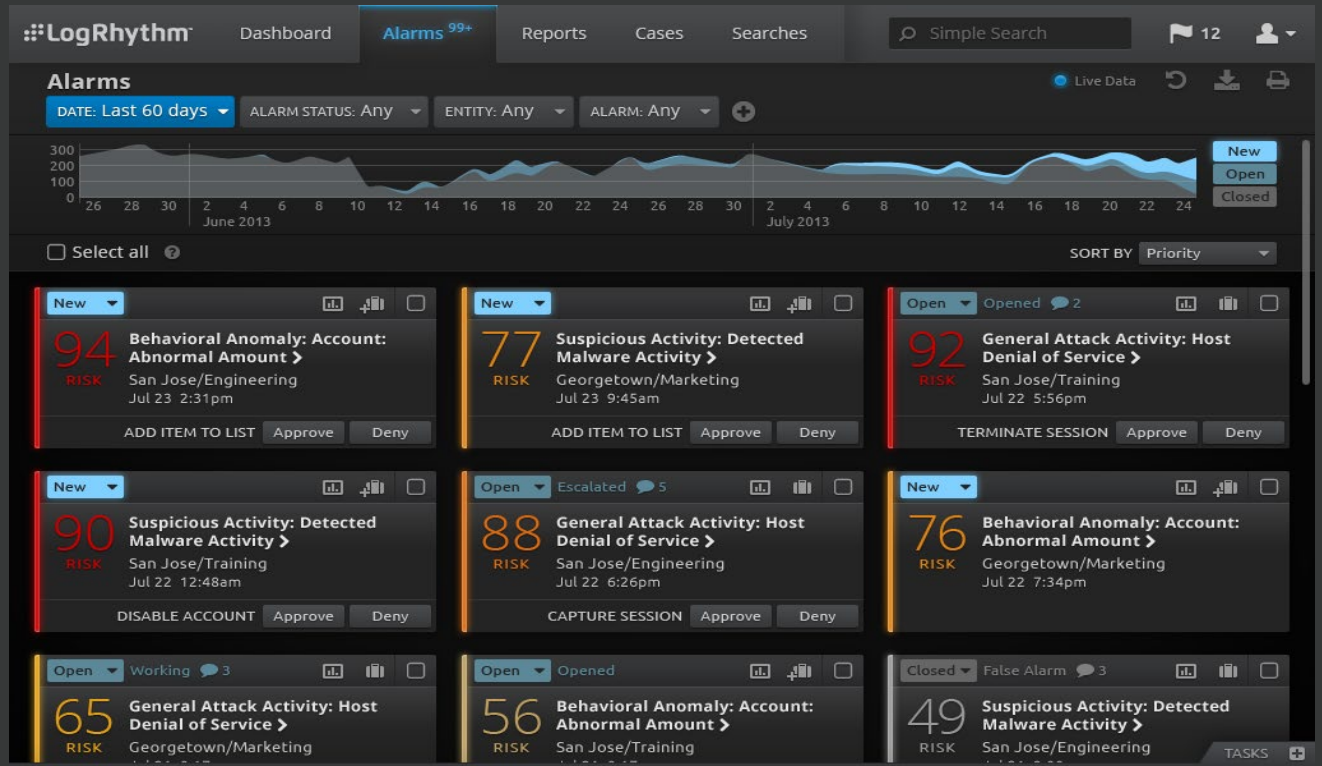
LogRhythm inbuilt UEBA



- User behaviour analysis

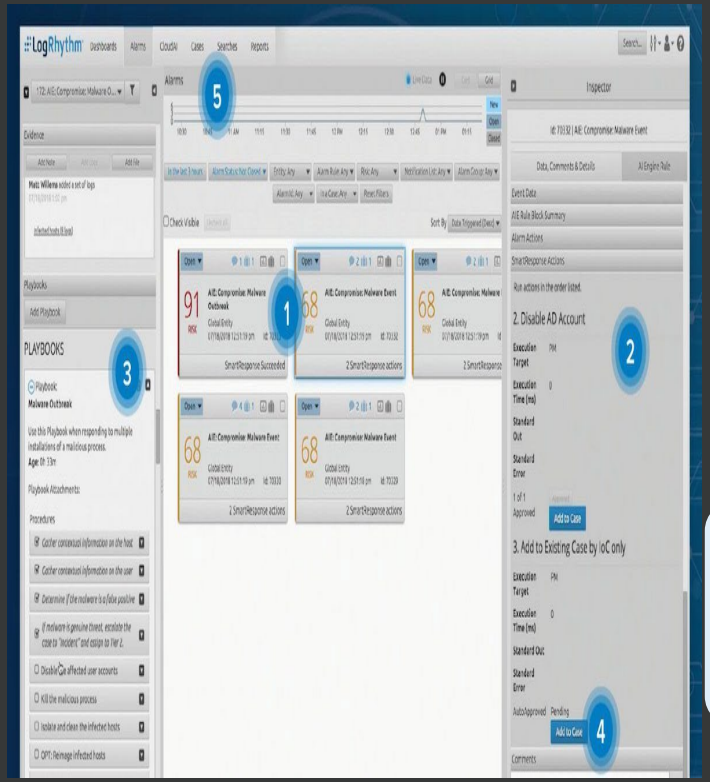
Risk scoring of all users on the network

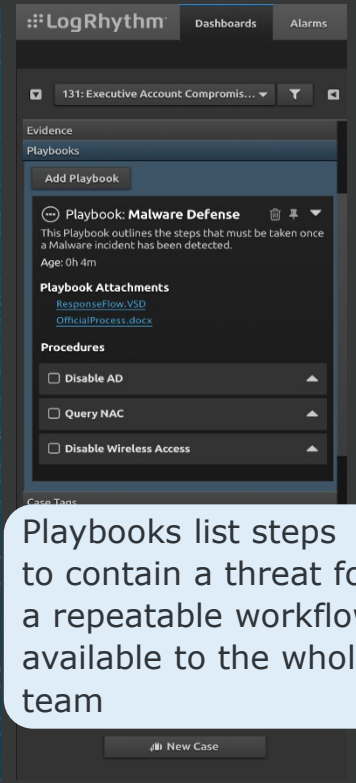
LogRhythm Built-in SOAR



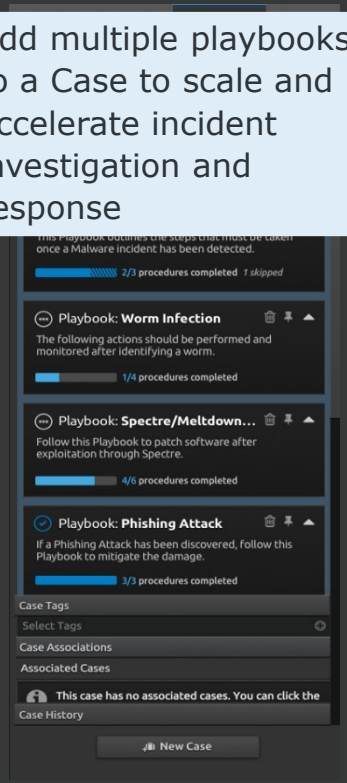
- Prioritised alarms
- Centralising all security incidents
- Built-in Incident response and case management
- No charge
- One product

LogRhythm inbuilt SOAR – Playbooks and smart responses





Playbooks list steps to contain a threat for a repeatable workflow available to the whole team



Add multiple playbooks to a Case to scale and accelerate incident investigation and response

- Playbooks make SOC analyst work easy and faster
- Smart responses automate actions when under attacks

And We Lead Again, with Our 15 Critical Capabilities

Data	1. Pervasive Forensic Visibility 2. Uniform Data Processing and Enrichment 3. Efficient and Flexible Architecture
Analytics	4. Integrated Threat and Business Context 5. High Performance Search Analytics 6. IOC and TTP-based Scenario Analytics 7. User & Network Behavior Analytics
Workflow	8. Holistic & Rapid, Risk-based Threat Triage 9. Machine Assisted Threat Hunting 10. Enterprise Orchestration & Collaboration 11. Automation & Autonomous Workflows
Platform	12. Comprehensive Compliance Automation 13. End-to-end Security Operations Metrics 14. Open Yet Secure 15. Broader IT/OT Leverage

And We Lead Again, with Our 15 Critical Capabilities

Data

1. Pervasive Forensic Vis
2. Uniform Data Process
3. Efficient and Flexible A

ELM

Analytics

4. Integrated Threat and
5. High Performance Sea
6. IOC and TTP-based Sc
7. User & Network Behav

SIEM | **UEBA** | **NDR** | **EDR**

Workflow

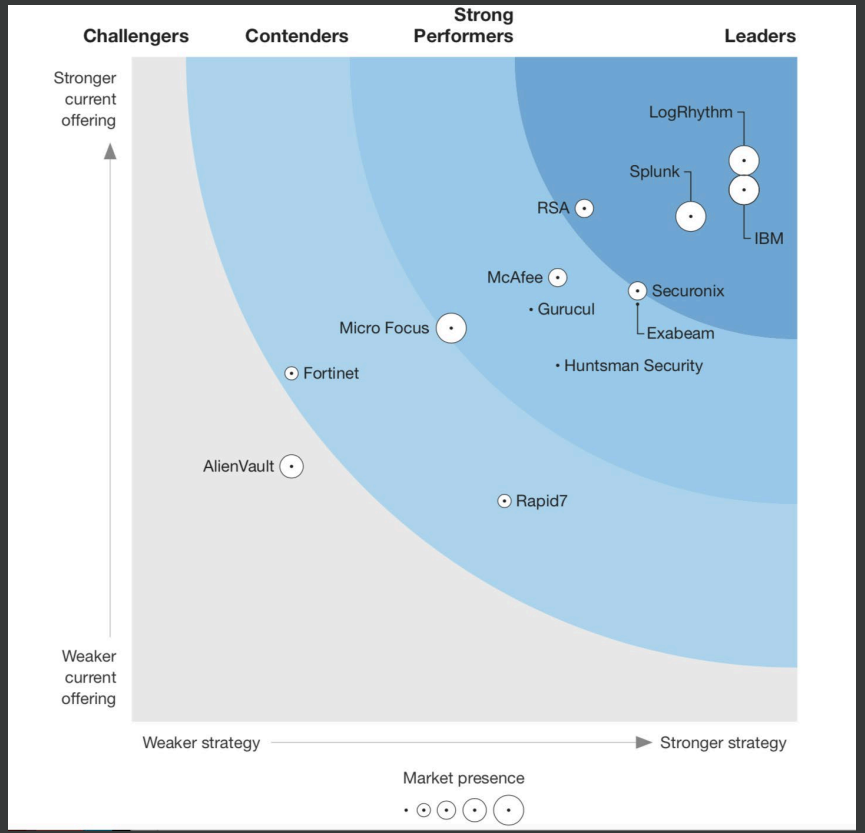
8. Holistic & Rapid, Risk
9. Machine Assisted Th
10. Enterprise Orchestra
11. Automation & Auton

SOAR

Platform

12. Comprehensive Compliance Automation
13. End-to-end Security Operations Metrics
14. Open Yet Secure
15. Broader IT/OT Leverage

Forrester Wave:



Forrester evaluated 13 vendors based on 30 criteria, and LogRhythm received **the highest possible score in 20 of those categories.**

In the report, Forrester stated:
"LogRhythm remains the largest standalone pure-play security analytics platform provider in the market… customers seeking a full-featured security analytics platform should consider LogRhythm."

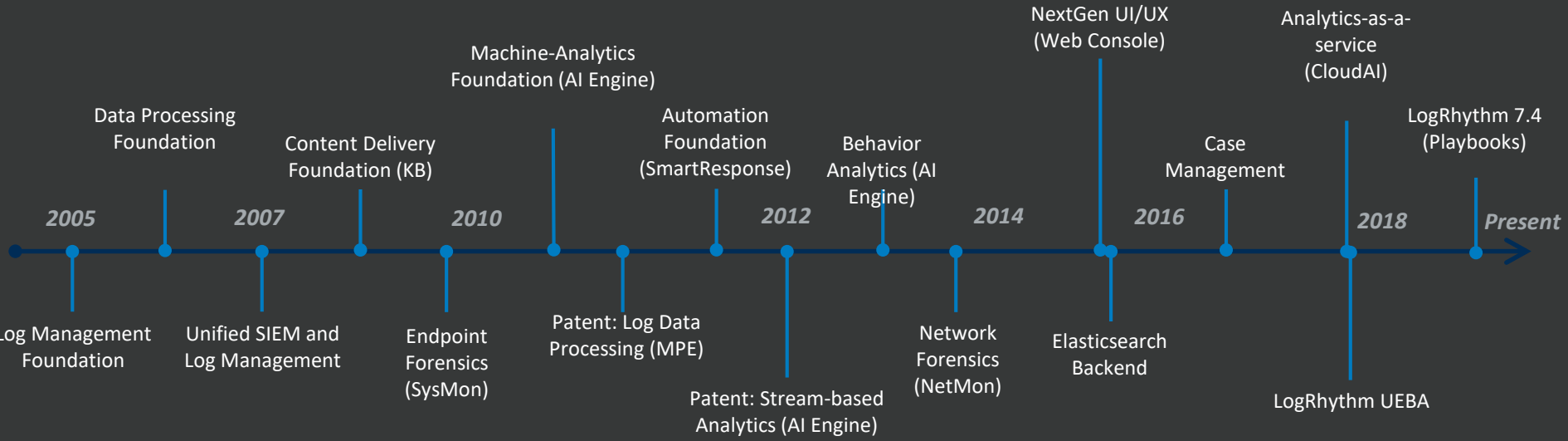
LogRhythm Named a Leader in Gartner's Magic Quadrant for SIEM

The 2018 Gartner Magic Quadrant for SIEM

LogRhythm Recognized as Market Leader for 7th Consecutive Year

"LogRhythm offers a single vendor approach for buyers that want an SIEM solution that offers complementary and self-contained options for network and host-level monitoring, as well as UEBA capabilities." – Gartner

We've Led the Way!




LogRhythm®
The Security Intelligence Company