LogRhythm®
The Security Intelligence Company

# Q4 Security Matters

Kev Eley
Insurance Sector Lead
kevin.eley@logrhythm.com

# About LogRhythm


- Founded 2003
- HQ Boulder, Co. EMEA / APJ
- 700+ employees WW
- Numerous patents granted, pending & awards
- Privately held, top-tier investors
- Adopted by many insurers

# Improving Insurers Cyber Detection & Response Capability

LogRhythm®
The Security Intelligence Company

# Relentless Attacks are the Norm


LogRhythm
The Security Intelligence Company

# The LogRhythm Mission

*To improve the Information Security teams ability to detect and respond to Cyber Threats in whatever form they take by raising your security posture though a partnership approach that expands your team to include LogRhythm & our Partners … reducing the risk of a damaging data breach*

*We call this Threat Lifecycle Management*

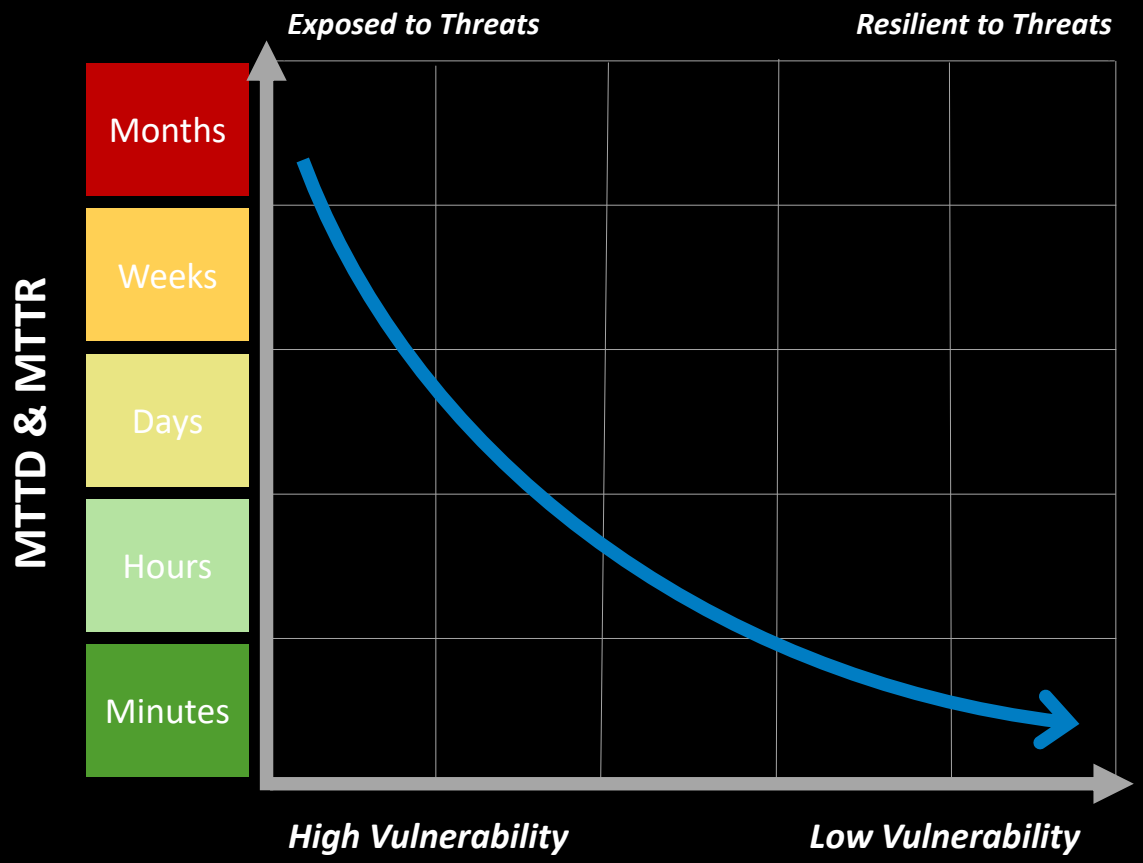
LogRhythm®
The Security Intelligence Company

# Conflict Scenario

“What is of the greatest importance in war is extraordinary speed”

LogRhythm
The Security Intelligence Company

# Speed in the Cyber Context




**MEAN TIME TO DETECT (MTTD)**
The average time it takes to recognise a threat requiring further analysis and response efforts

**MEAN TIME TO RESPOND (MTTR)**
The average time it takes to respond and ultimately resolve the incident

***Delivering positive change to your security posture***

LogRhythm
The Security Intelligence Company

# Streamlining Workflow Ensures Speed & Action

## TIME TO DETECT

## TIME TO RESPOND

### Forensic Data Collection

Security event data

Log & machine data

Forensic sensor data

### Discover

Search analytics

Machine analytics

### Qualify

Assess threat

Determine risk

Is full investigation necessary?


### Investigate

Analyze threat

Determine nature and extent of incident

### Neutralize

Implement counter-measures

Mitigate threat & associated risk

### Recover

Clean up

Report

Review

Adapt

LogRhythm
The Security Intelligence Company

| Adversary Action | LR Countermeasure |
|---|---|
| Ransomware Attack | ▪ Detection of ransomware activity & production of appropriate alert & notifications to SOC<br>▪ Analysis / forensics including C2 communication<br>▪ Automated exclusion of infected devices via smart response and integration |
| Malware Attack | ▪ Detection of malicious / suspicious endpoint process activity<br>▪ Detection of lateral movement activity<br>▪ Provide near real-time intelligence, alerting & notifications (including C2) to SOC |
| HVT & MVE Attack | ▪ Privileged User / Executive Monitoring and alarming on unusual activity<br>▪ Anti Phishing (PIE) countermeasures for O365 users<br>▪ Collection / Generation of data from MVE (including Cloud properties) with TTP rules enabled<br>▪ Detection & appropriate forensics, alerting & notifications to SOC |
| General Network Intrusion | ▪ True Application Identification for anomalous activity including TOR, unusual port and C2<br>▪ Full packet capture and packet re construction<br>▪ Unusual network connection activity on servers and SCADA environment<br>▪ Provide forensics, alerting & notifications to SOC |
| Attacker Recon | ▪ Network IP Services e.g. DNS servers & ability to detect activity such as zone transfer<br>▪ Unauthorised port scanning detection & activity e.g. telnet, ssh, (s)ftp(s)<br>▪ Provide appropriate alerting & notifications to SOC tooling |
| Data Theft | ▪ Detection of data & document exfiltration<br>▪ Ingress/egress beaconization of fake & real documents alerted in real-time<br>▪ Provide forensic details e.g. file origination, destination, IP address, GPS etc |
| Attacker Intention | ▪ Enabling SOC team hunting for adversary actions gleaned from DarkWeb<br>▪ Standards based threat intelligence feeds including data enrichment & contextualization |

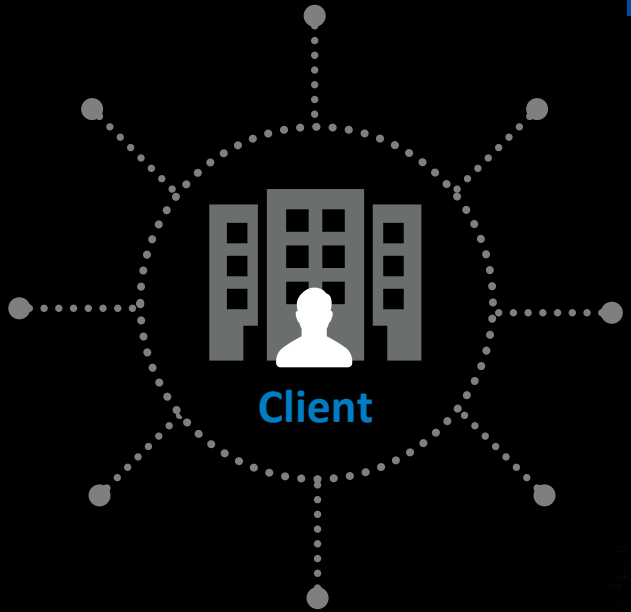
Meaningful, High Quality Information Derived from LR Machine Data Intelligence (MDI) Fabric Layer

LogRhythm
The Security Intelligence Company

# Announcing LogRhythm Ecosystem for Cyber Insurers

LogRhythm®
The Security Intelligence Company

# Cyber Dangers We All Face





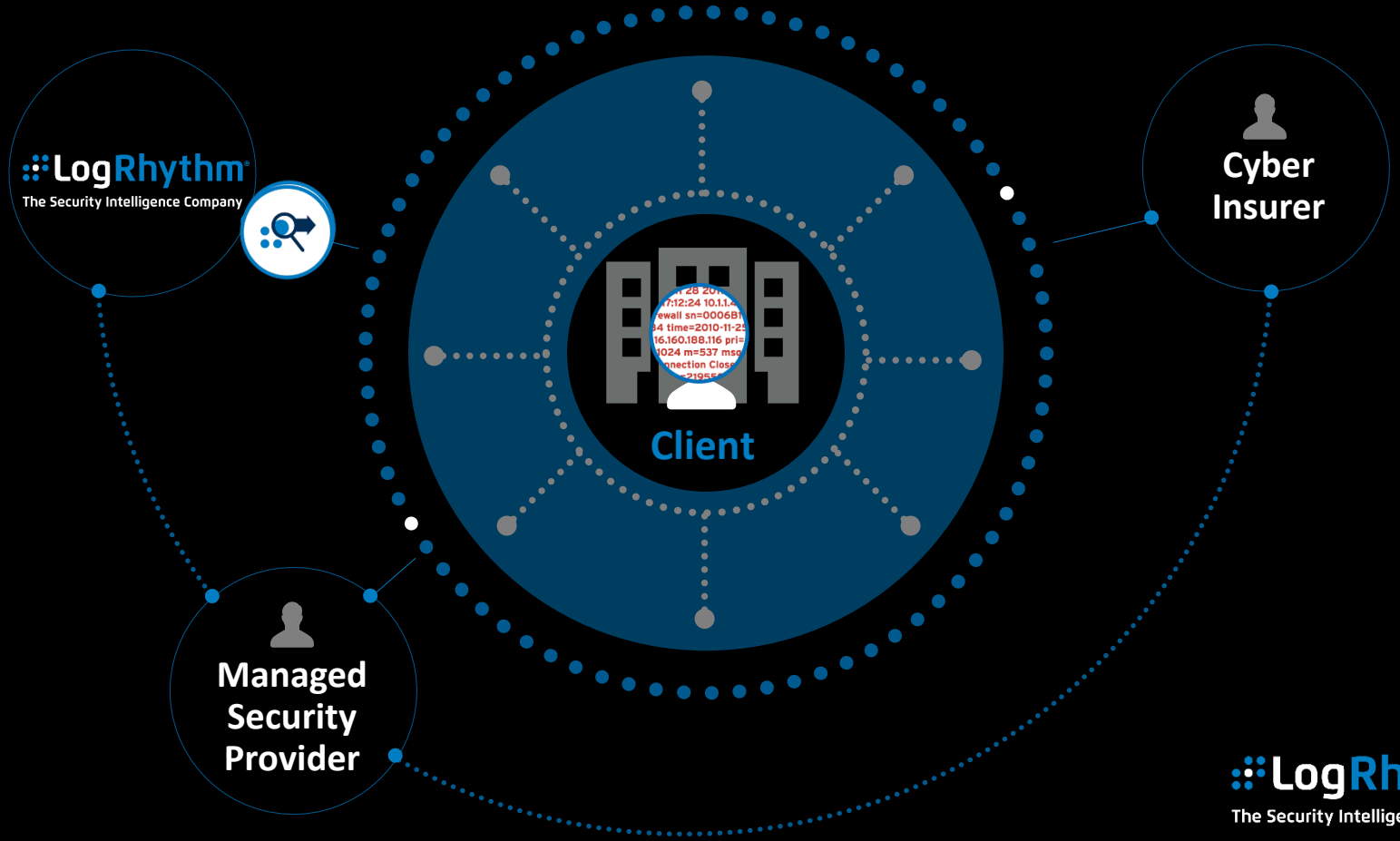
LogRhythm
The Security Intelligence Company

# Cyber Dangers We All Face

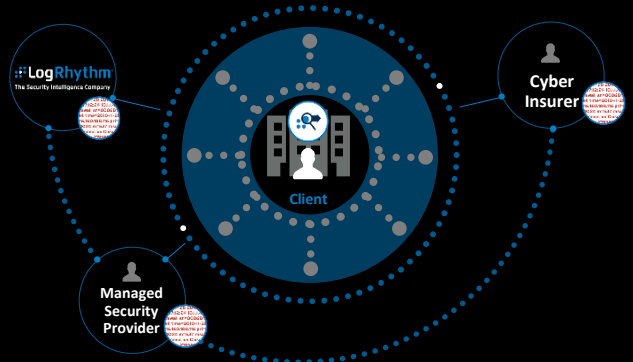


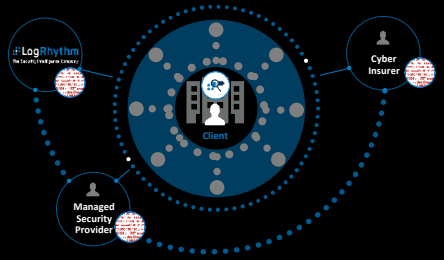
LogRhythm
The Security Intelligence Company

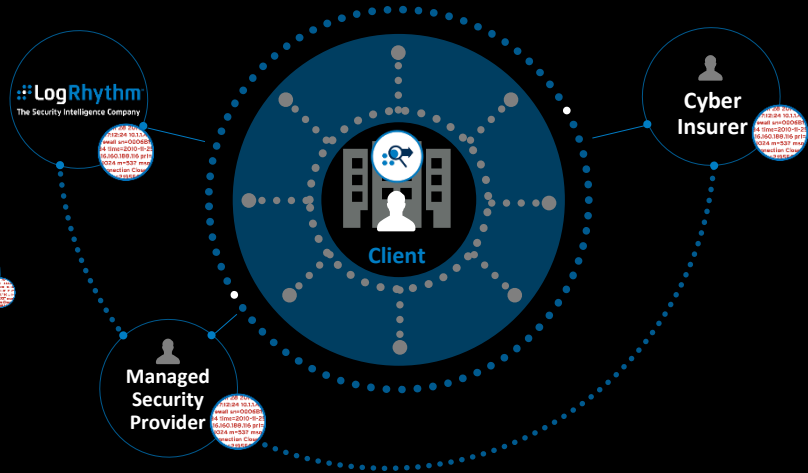
# Ecosystem for Cyber Insurers

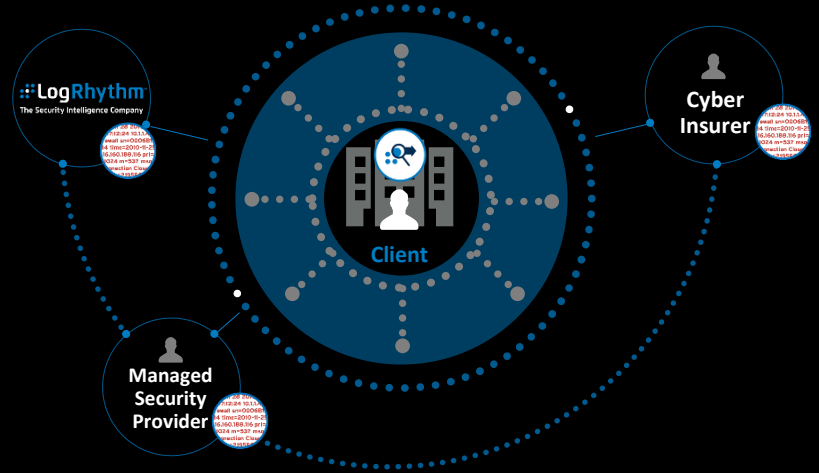


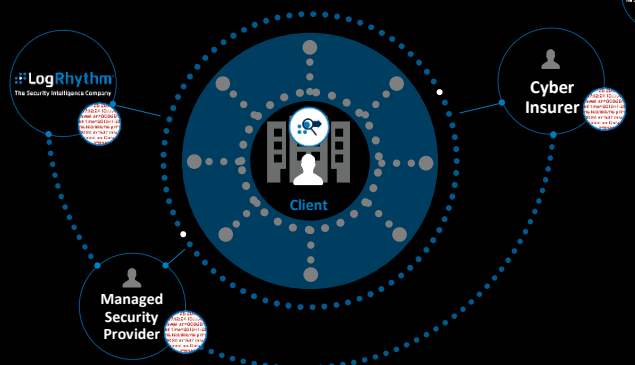
# Grow the Ecosystem

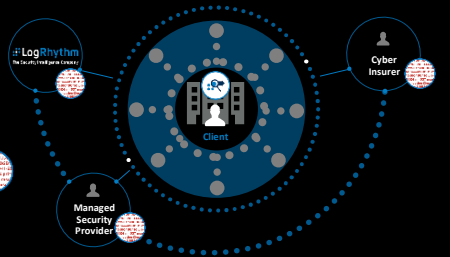



LogRhythm
The Security Intelligence Company

# Advantages of the Ecosystem

Focused, Proven Detection & Response with Augmented Capabilities

Accurate Near Real Time Telemetry for Underwriters

Platform Scalability & Flexibility

Innovation

Reciprocity, success for stakeholders, we're consulting with MSPs and Cyber Insurers now!

LogRhythm
The Security Intelligence Company


LogRhythm®
LogRhythm®
The Security Intelligence Company