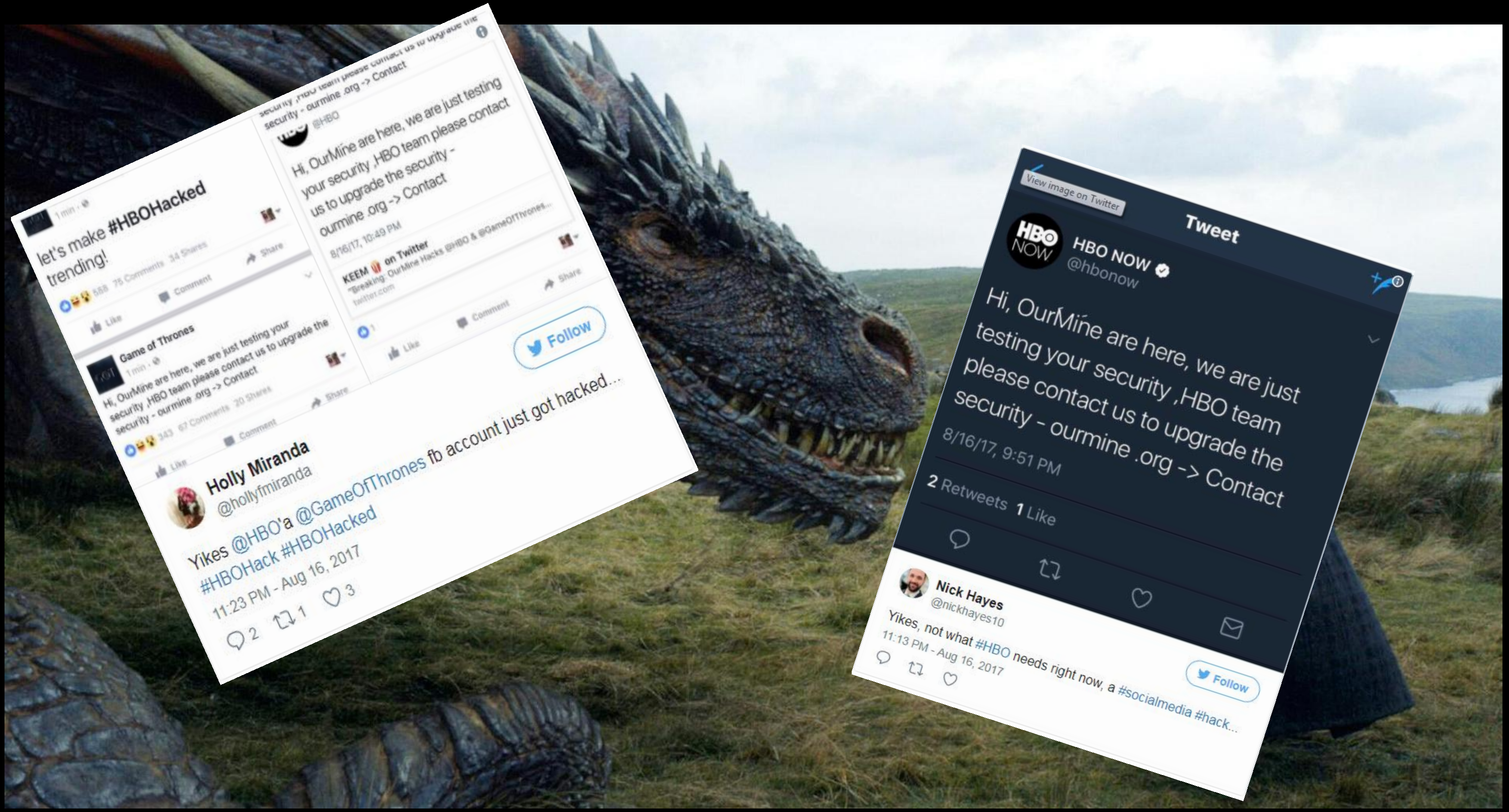
LogRhythm
The Security Intelligence Company

Threat Lifecycle Management –
Helping to Solve Today's Cyber Threats

ISSA Central Maryland Chapter

August 23, 2017

HBO social media accounts hacked in another cyberattack



security ,HBO team please contact us to upgrade the security - ourmine .org -> Contact

@HBO

Hi, OurMine are here, we are just testing your security ,HBO team please contact us to upgrade the security - ourmine .org -> Contact

8/16/17, 10:49 PM

KEEM on Twitter
"Breaking: OurMine Hacks @HBO & @GameOfThrones...
twitter.com

1 min ·

let's make #HBOHacked trending!

558 75 Comments 34 Shares

Like Comment Share

Game of Thrones
1 min ·

Hi, OurMine are here, we are just testing your security ,HBO team please contact us to upgrade the security - ourmine .org -> Contact

343 67 Comments 20 Shares

Like Comment Share

Holly Miranda
@hollyfmiranda

Follow

Yikes @HBO'a @GameOfThrones fb account just got hacked... #HBOHack #HBOHacked

11:23 PM - Aug 16, 2017

2 1 3

View image on Twitter

Tweet

HBO NOW
@hbonow

Hi, OurMíne are here, we are just testing your security ,HBO team please contact us to upgrade the security - ourmine .org -> Contact

8/16/17, 9:51 PM

2 Retweets 1 Like

Nick Hayes
@nickhayes10

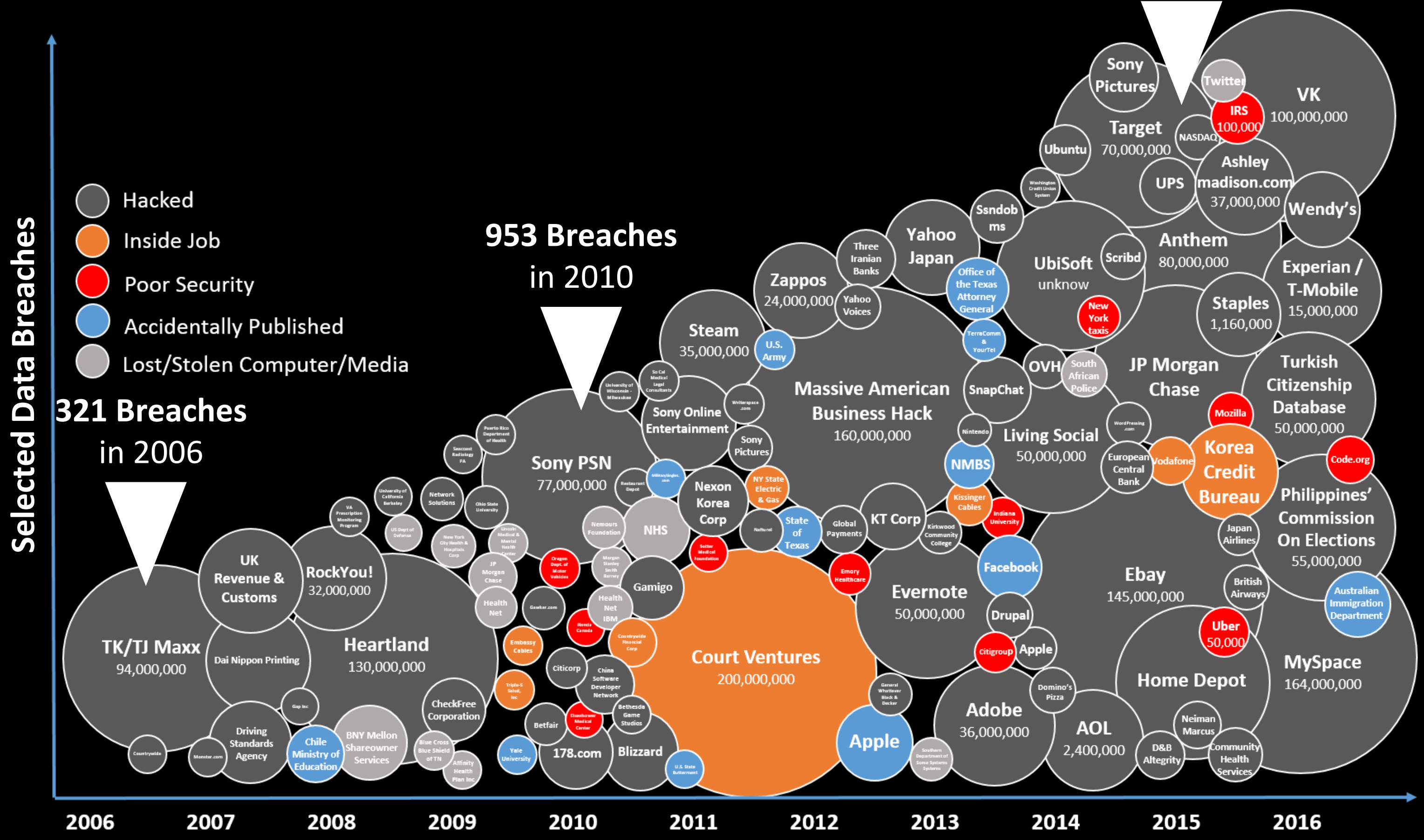
Follow

Yikes, not what #HBO needs right now, a #socialmedia #hack...

11:13 PM - Aug 16, 2017

https://www.cnbc.com/2017/08/17/hbo-social-media-accounts-hacked-in-another-cyberattack.html

The Modern Cyber Threat Pandemic



3,930 Breaches in 2015

953 Breaches in 2010

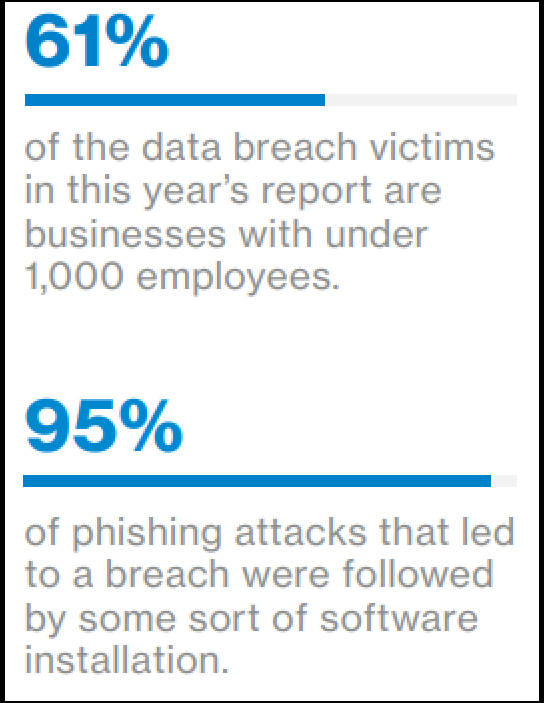
321 Breaches in 2006

736 million records were exposed in 2015, compared to **96 million records** in 2010

The security industry is facing serious **talent and technology shortages**

Source: World's Biggest Data Breaches, Information is Beautiful

No one thinks it’s going to be them. Until it is.



61%

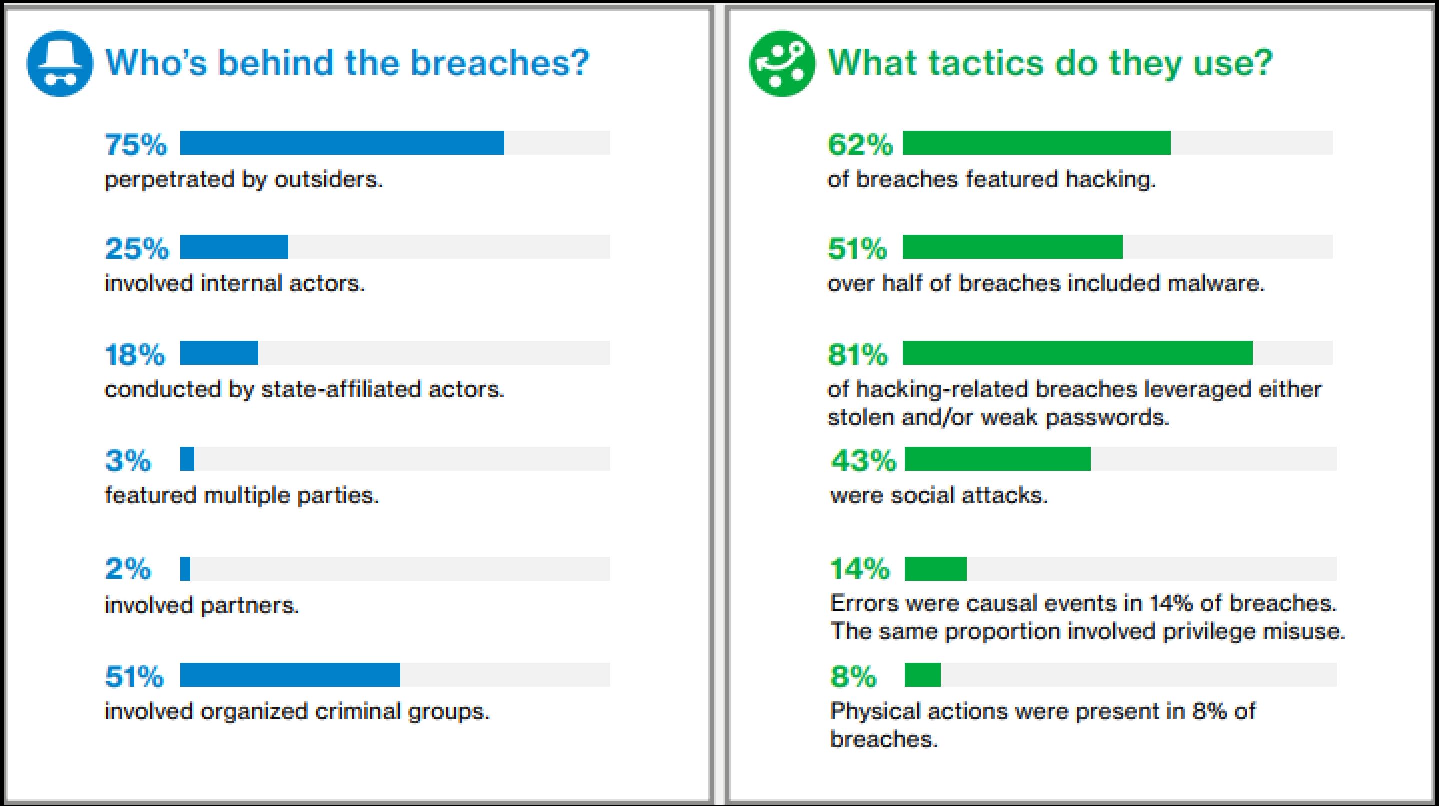
of the data breach victims in this year’s report are businesses with under 1,000 employees.

95%

of phishing attacks that led to a breach were followed by some sort of software installation.

Users/michelle.lapuente/Downloads/rp_DBIR_2017_Report_execsummary_en_xg%20(1).pdf

No one thinks it’s going to be them. Until it is.



Who’s behind the breaches?

75%
perpetrated by outsiders.

25%
involved internal actors.

18%
conducted by state-affiliated actors.

3%
featured multiple parties.

2%
involved partners.

51%
involved organized criminal groups.

What tactics do they use?

62%
of breaches featured hacking.

51%
over half of breaches included malware.

81%
of hacking-related breaches leveraged either stolen and/or weak passwords.

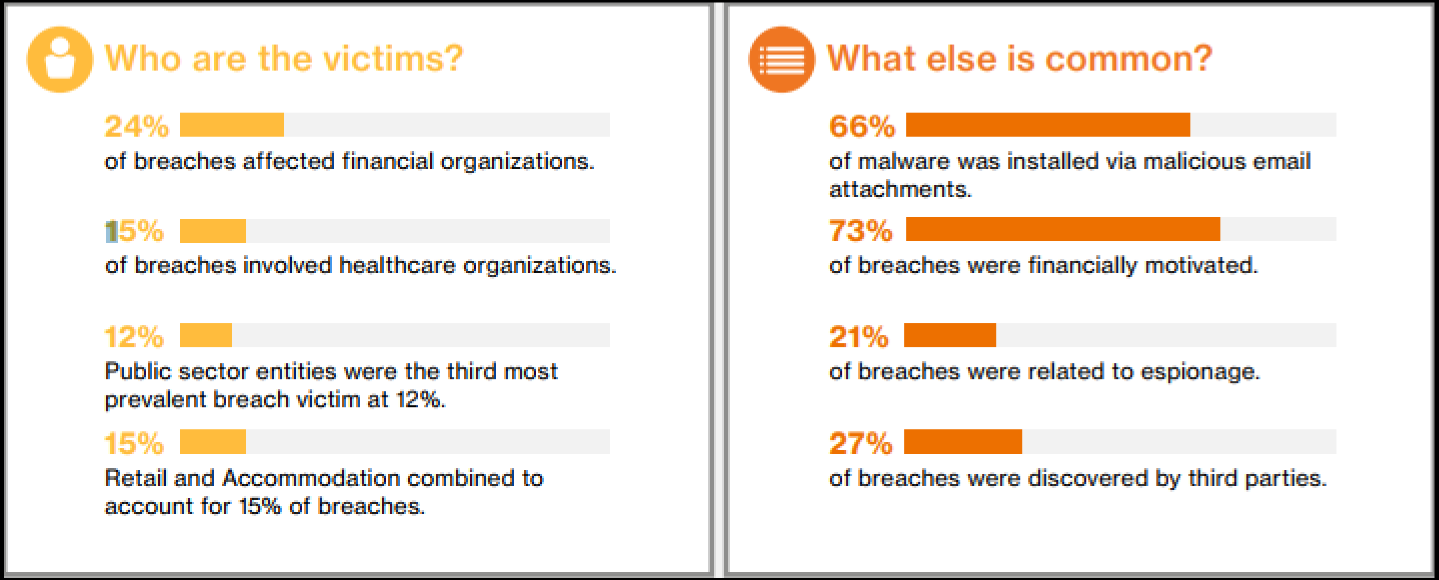
43%
were social attacks.

14%
Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8%
Physical actions were present in 8% of breaches.

Users/michelle.lapuente/Downloads/rp_DBIR_2017_Report_execsummary_en_xg%20(1).pdf

No one thinks it's going to be them. Until it is.



Who are the victims?

24%
of breaches affected financial organizations.

15%
of breaches involved healthcare organizations.

12%
Public sector entities were the third most prevalent breach victim at 12%.

15%
Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66%
of malware was installed via malicious email attachments.

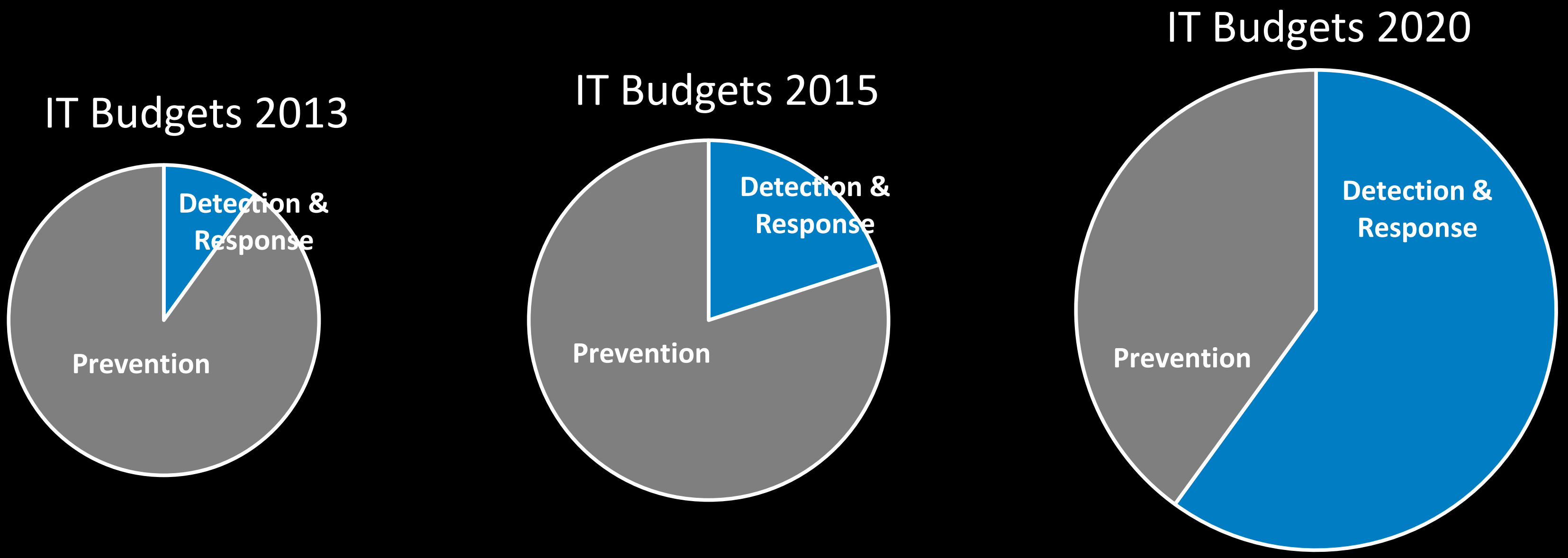
73%
of breaches were financially motivated.

21%
of breaches were related to espionage.

27%
of breaches were discovered by third parties.

Users/michelle.lapuente/Downloads/rp_DBIR_2017_Report_execsummary_en_xg%20(1).pdf

Strategic Shift to Detection and Response is Occurring



By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from 20% in 2015. *–Gartner, 2016*

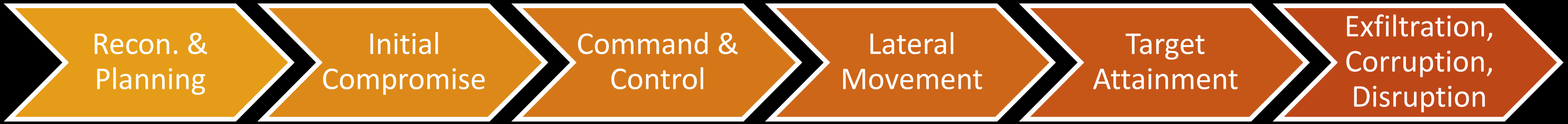
Sources: Gartner, Shift Cybersecurity Investment to Detection and Response, January 2016; Gartner, Forecast: Information Security, Worldwide, 2014-2020, 1Q16 Update, April 2016
Note: Excludes security services from estimated overall market spend for enterprise information security

LogRhythm
The Security Intelligence Company

The Cyber Attack Lifecycle

Modern threats take their time

and leverage the holistic attack surface


Recon. & Planning

Initial Compromise

Command & Control

Lateral Movement

Target Attainment

Exfiltration, Corruption, Disruption

LogRhythm
The Security Intelligence Company

Can you see the threat?

© Caters News Agency

LogRhythm
The Security Intelligence Company

© Caters News Agency

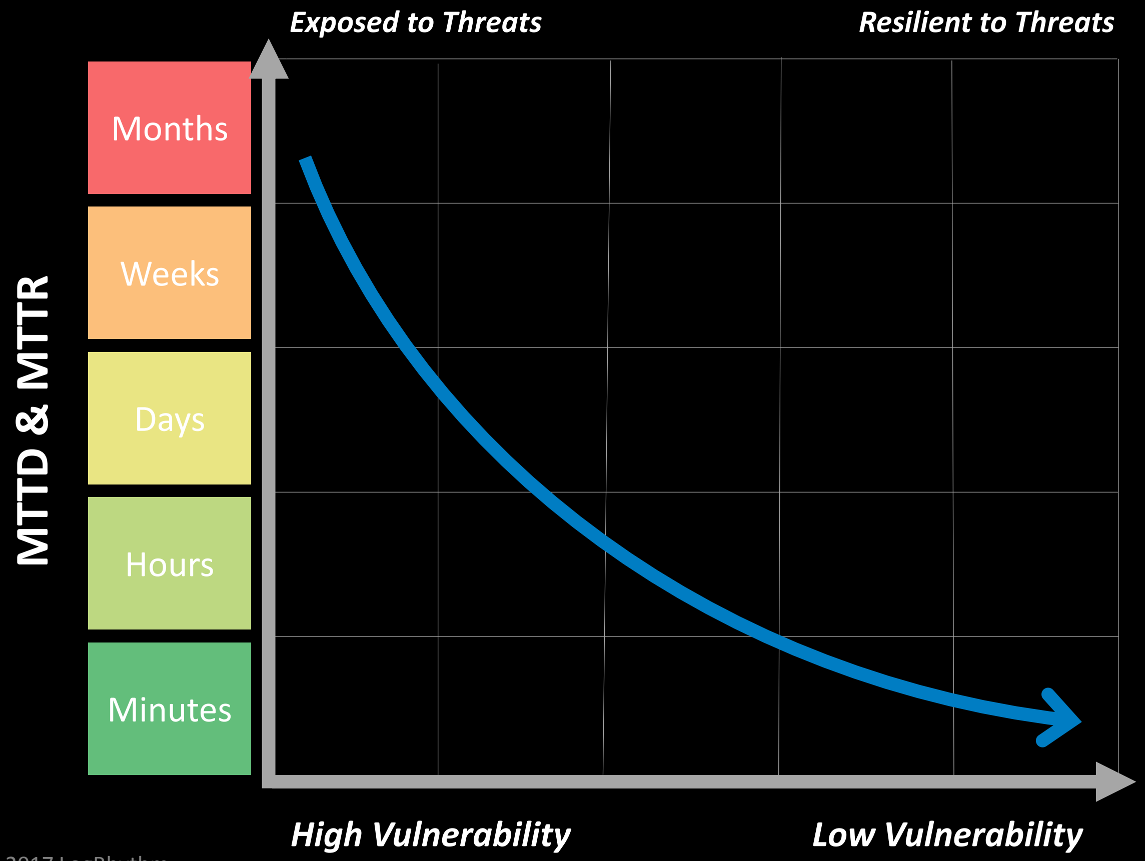
LogRhythm
The Security Intelligence Company

Obstacles To Faster Detection & Response

- Alarm Fatigue
- Swivel Chair Analysis
- Forensic Data Silos
- Fragmented Workflow
- Lack of Automation

LogRhythm
The Security Intelligence Company

Protection Through Faster Detection & Response



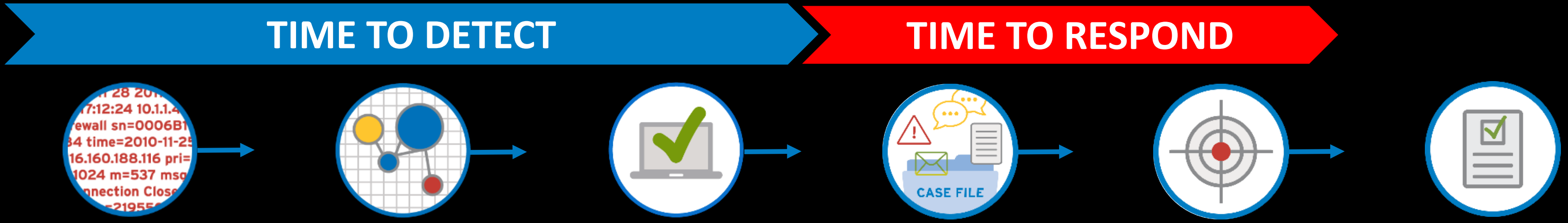
MEAN TIME TO DETECT (MTTD)
The average time it takes to recognize a threat requiring further analysis and response efforts

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

As organizations improve their ability to quickly detect and respond to threats, the risk of experiencing a damaging breach is greatly reduced

LogRhythm
The Security Intelligence Company

End-to-End Threat Lifecycle Management Workflow



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

Putting the Technology to Work

LogRhythm
The Security Intelligence Company

Why Advanced Intelligence Engine

"You need a machine to understand a machine."

The Imitation Game

Alan Turing - *Computer scientist, mathematician, logician, cryptanalyst and theoretical biologist*

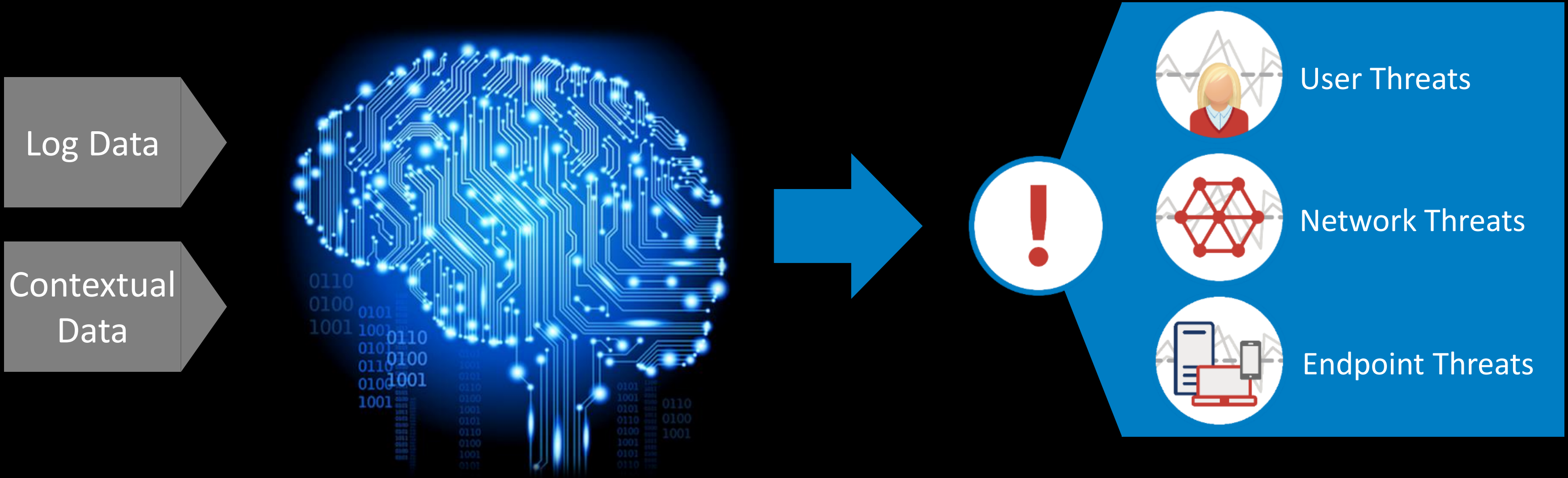
Enigma Code

- 150,738,274,937,250 combinations
- Cipher changed daily

8 ACADEMY AWARD® NOMINATIONS
INCLUDING
BEST PICTURE
BEST ACTOR · BEST DIRECTOR · BEST SUPPORTING ACTRESS
BENEDICT CUMBERBATCH
KEIRA KNIGHTLEY
THE IMITATION GAME
BASED ON THE INCREDIBLE TRUE STORY

https://en.wikipedia.org/wiki/Alan_Turing

Holistic Threat Detection Powered by AI Engine



Log Data

Contextual Data

User Threats

Network Threats

Endpoint Threats

Benefits

- ✓ Real-time advanced threat detection
- ✓ Detection across full attack lifecycle
- ✓ Easily customizable
- ✓ Lower false negatives AND false positives

Precision Search Powered by Elasticsearch

Structured Search

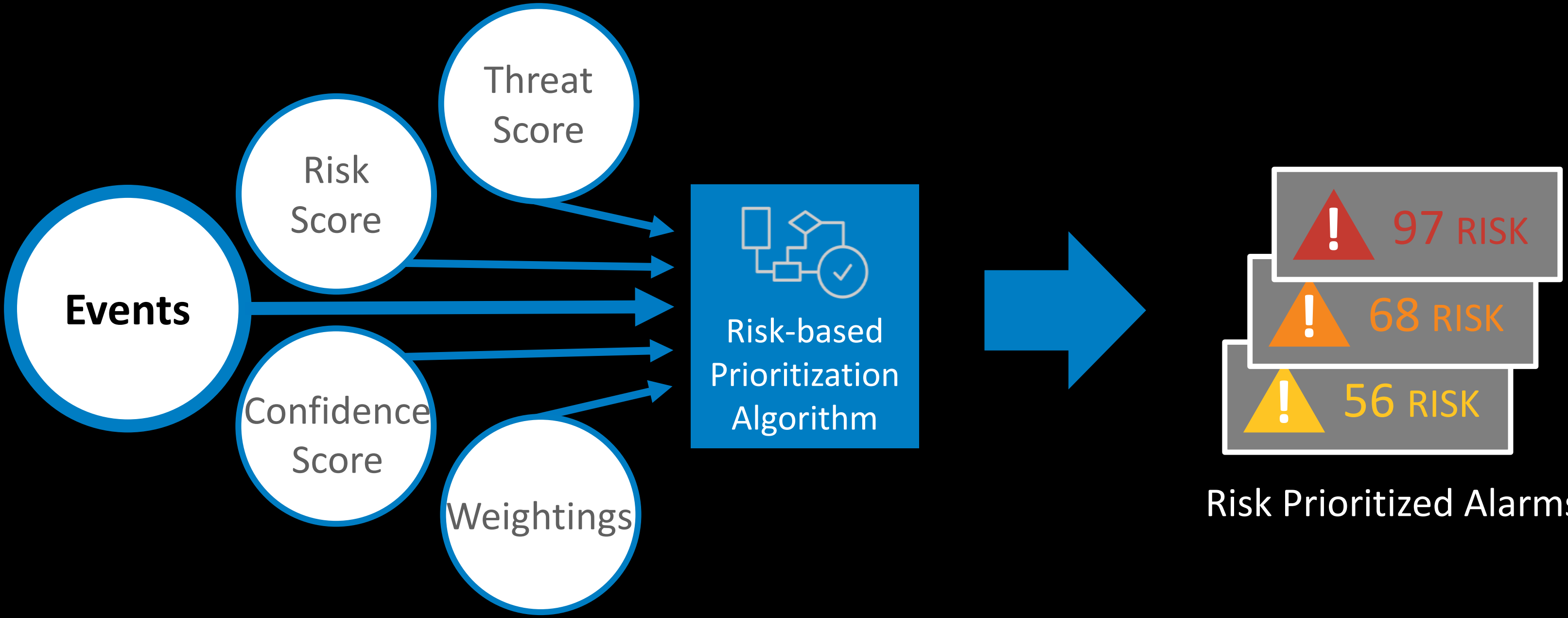
Unstructured Search

Machine-Assisted Search

Benefits

- ✓ Quick results
- ✓ Less “noise”
- ✓ Investigation automation
- ✓ Fast and accurate decisions

Risk-based Monitoring



Risk Prioritized Alarms

Benefits

- ✓ Focuses analysts’ time where it matters most
- ✓ Faster recognition of threats that need attention
- ✓ Reduces alarm fatigue

LogRhythm
The Security Intelligence Company

Embedded Security Automation and Orchestration

Case Management

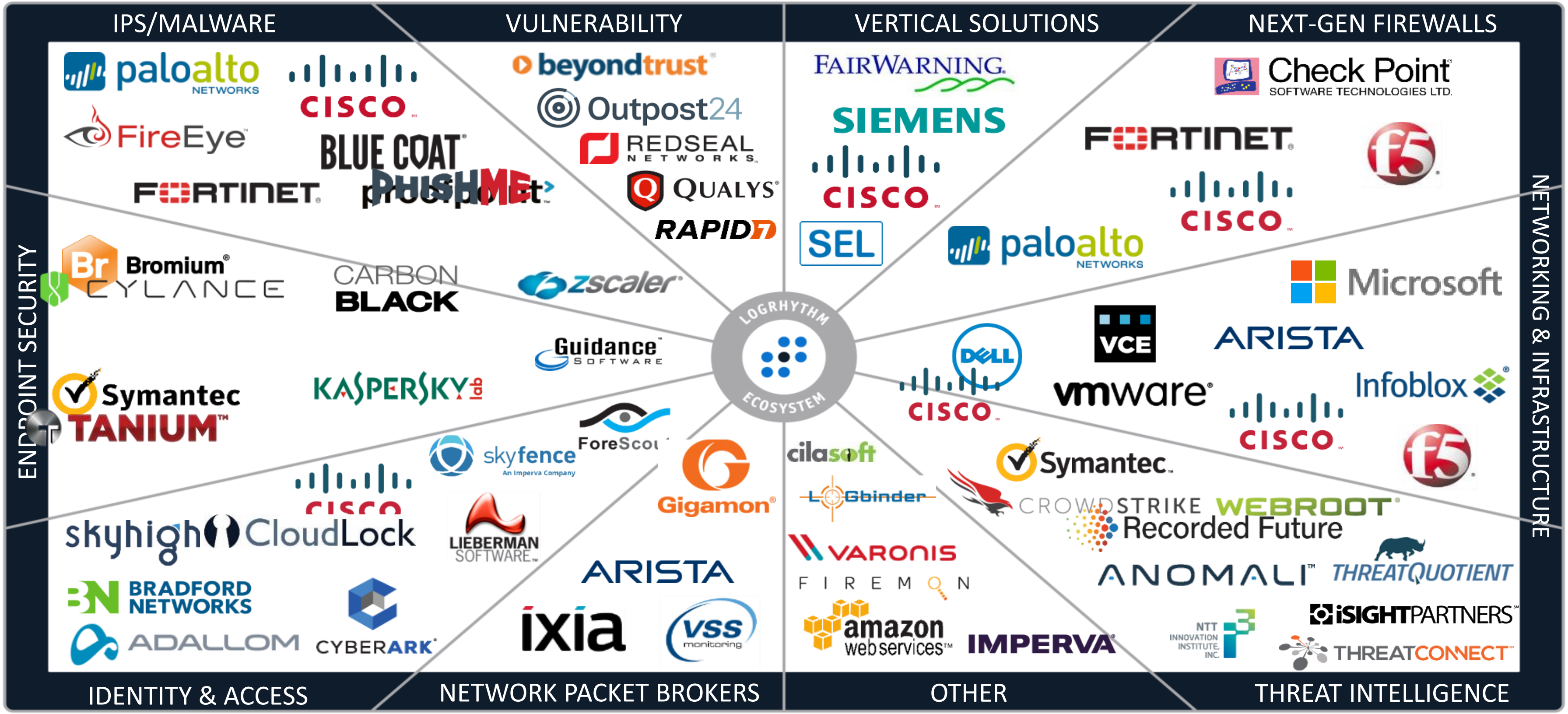
SmartResponse Automation

Benefits

- ✓ Centralizes security investigations
- ✓ Faster investigations with single toolset
- ✓ Efficient, confidential collaboration
- ✓ Automates workflows and responses
- ✓ Reduces mean time to respond (MTTR)

LogRhythm
The Security Intelligence Company

Current Technology Alliance Ecosystem



IPS/MALWARE

VULNERABILITY

VERTICAL SOLUTIONS

NEXT-GEN FIREWALLS

ENDPOINT SECURITY

NETWORKING & INFRASTRUCTURE

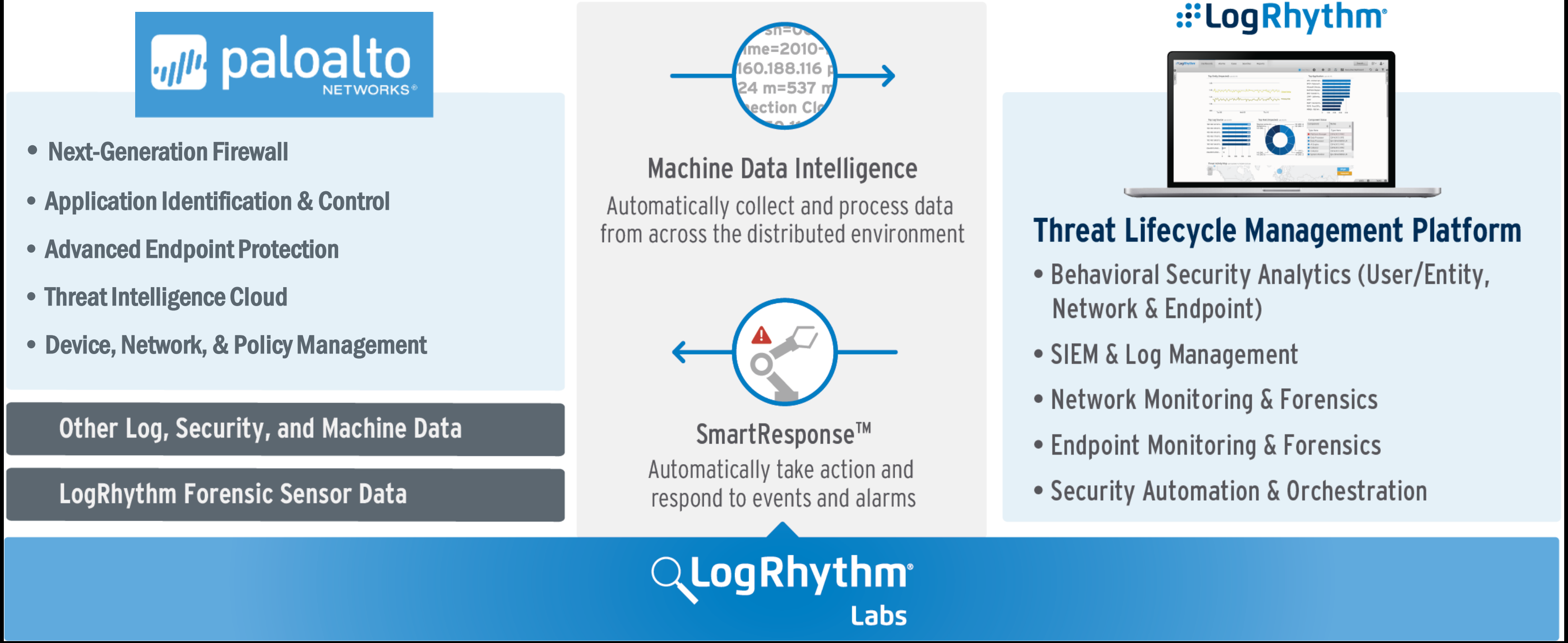
IDENTITY & ACCESS

NETWORK PACKET BROKERS

OTHER

THREAT INTELLIGENCE

LogRhythm & Palo Alto Networks: Integrated Enterprise Security



- Next-Generation Firewall
- Application Identification & Control
- Advanced Endpoint Protection
- Threat Intelligence Cloud
- Device, Network, & Policy Management

Other Log, Security, and Machine Data

LogRhythm Forensic Sensor Data

Machine Data Intelligence

Automatically collect and process data from across the distributed environment

SmartResponse™

Automatically take action and respond to events and alarms

Threat Lifecycle Management Platform

- Behavioral Security Analytics (User/Entity, Network & Endpoint)
- SIEM & Log Management
- Network Monitoring & Forensics
- Endpoint Monitoring & Forensics
- Security Automation & Orchestration

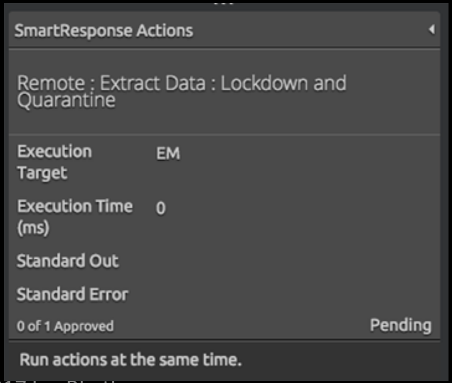
LogRhythm
The Security Intelligence Company

LogRhythm & Palo Alto Networks: Overview

In partnership, LogRhythm & Palo Alto Networks deliver the market's most innovative automated analytics for advanced threat detection & response.

Together, we deliver end-to-end TLM capabilities for protecting the network & reducing MTTD & MTTR through:

- Fully interactive visualization tools
- Context-aware event management
- Automated incident response orchestration & remediation
- Advanced behavioral analytics for user, network, & endpoint
- Rich user & application context captured by Palo Alto Network's NGFW



SmartResponse Actions

Remote : Extract Data : Lockdown and Quarantine

Execution Target EM

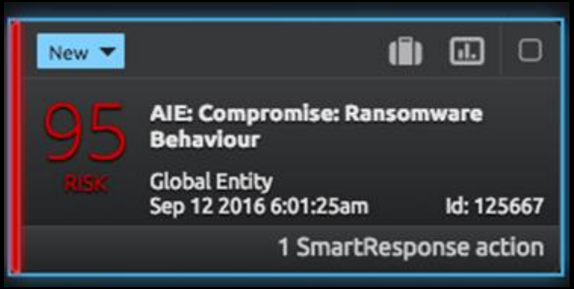
Execution Time (ms) 0

Standard Out

Standard Error

0 of 1 Approved Pending

Run actions at the same time.



95 RISK

AIE: Compromise: Ransomware Behaviour

Global Entity

Sep 12 2016 6:01:25am Id: 125667

1 SmartResponse action

Use Case: Detect & Respond to Advanced Threats

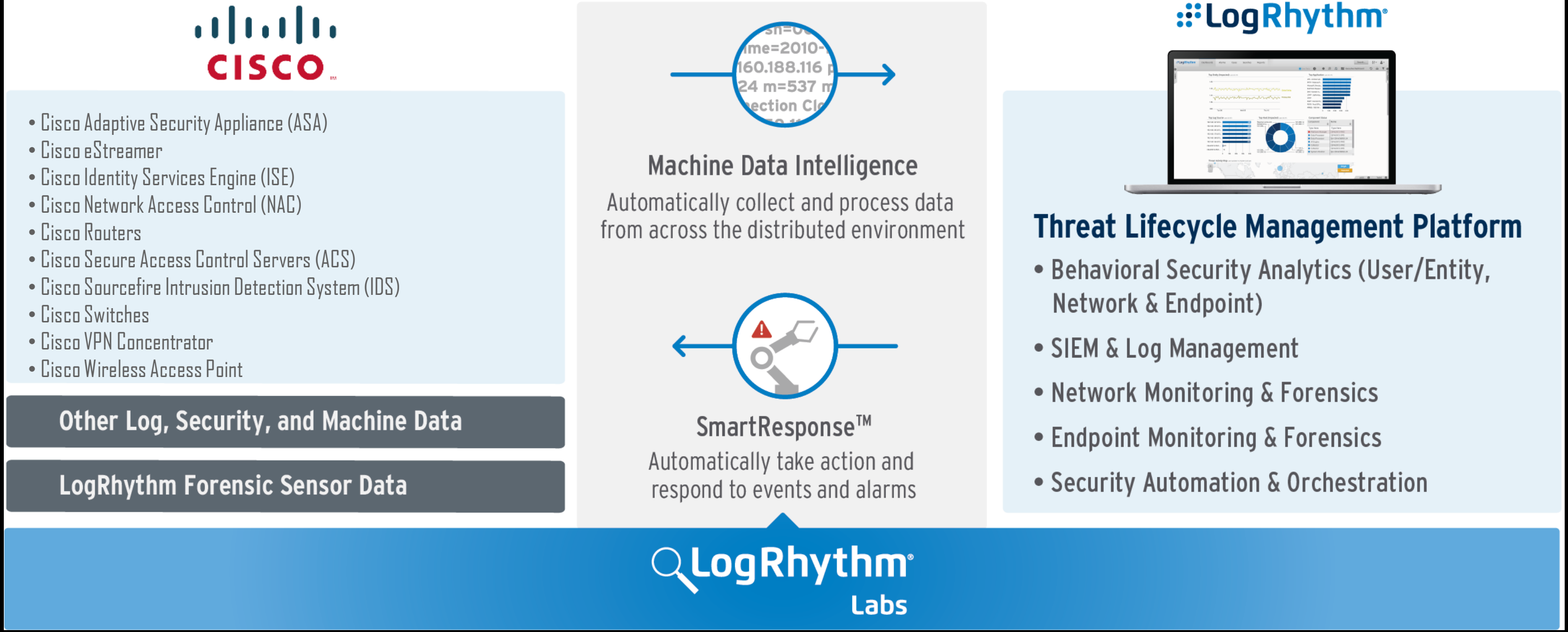
Challenge: Advanced persistent threats often leverage customized, zero-day malware to evade detection by traditional perimeter solutions. Once an intrusion gets through, organizations are unable to detect malicious behavior.

Solution: LogRhythm's advanced machine analytics can perform behavioral profiling using application & user data collected by Palo Alto Networks NGFW to detect abnormal activity, such as excessive outbound connections with non-whitelisted locations.

Response: A LogRhythm SmartResponse™ plug-in can automatically shut down unauthorized processes or services, immediately adding suspicious IPs to Palo Alto Networks NGFW policy to prevent network access.

LogRhythm®
The Security Intelligence Company

LogRhythm & Cisco: Integrated Enterprise Security



- Cisco Adaptive Security Appliance (ASA)
- Cisco eStreamer
- Cisco Identity Services Engine (ISE)
- Cisco Network Access Control (NAC)
- Cisco Routers
- Cisco Secure Access Control Servers (ACS)
- Cisco Sourcefire Intrusion Detection System (IDS)
- Cisco Switches
- Cisco VPN Concentrator
- Cisco Wireless Access Point

Other Log, Security, and Machine Data

LogRhythm Forensic Sensor Data

Machine Data Intelligence

Automatically collect and process data from across the distributed environment

SmartResponse™

Automatically take action and respond to events and alarms

Threat Lifecycle Management Platform

- Behavioral Security Analytics (User/Entity, Network & Endpoint)
- SIEM & Log Management
- Network Monitoring & Forensics
- Endpoint Monitoring & Forensics
- Security Automation & Orchestration

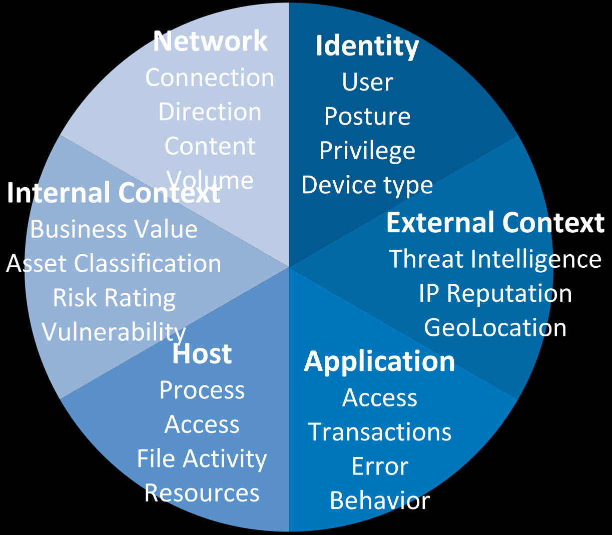
LogRhythm Labs

LogRhythm
The Security Intelligence Company

LogRhythm & Cisco: Identity Services Engine (ISE)

Integration

- LogRhythm TLM platform incorporates identity, access, and activity telemetry from Cisco ISE
- LogRhythm performs advanced analytics & pattern recognition across expanded data sets



Network
Connection
Direction
Content
Volume

Identity
User
Posture
Privilege
Device type

Internal Context
Business Value
Asset Classification
Risk Rating
Vulnerability

External Context
Threat Intelligence
IP Reputation
GeoLocation

Host
Process
Access
File Activity
Resources

Application
Access
Transactions
Error
Behavior

Benefits

- Allows users to monitor & secure entire range of endpoints, systems, & applications across organization
- Real-time cyber threat protection
- Compliance enforcement based on up-to-date situational awareness
- Greater visibility across networks

Use Case: Compromised Credentials

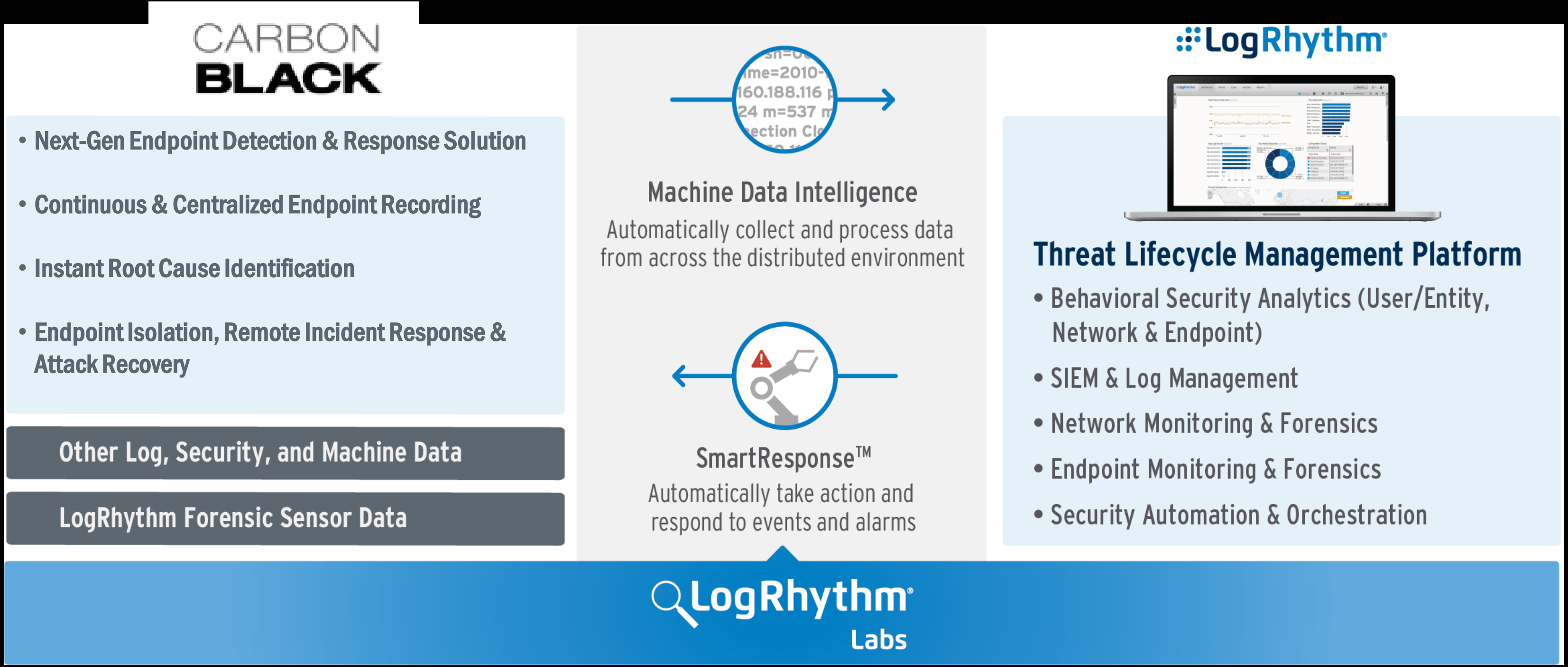
Monitor: LogRhythm incorporates telemetry from Cisco ISE & applies advanced analytics & correlation against all other log & event data. Provides deep visibility into devices/users accessing the network. Establishes a "normal" behavior profile.

Detect: LogRhythm can trigger a high-priority alert when a device/user violates policy or deviates in a threatening way from an established behavior pattern based on type, peer group, or identity.

Respond: LogRhythm SmartResponse™ plugin initiates an automated response by instructing ISE to quarantine device/user.

LogRhythm
The Security Intelligence Company

LogRhythm & Carbon Black: Integrated Threat Discovery & Remediation



CARBON BLACK

- Next-Gen Endpoint Detection & Response Solution
- Continuous & Centralized Endpoint Recording
- Instant Root Cause Identification
- Endpoint Isolation, Remote Incident Response & Attack Recovery

Other Log, Security, and Machine Data

LogRhythm Forensic Sensor Data

Machine Data Intelligence

Automatically collect and process data from across the distributed environment

SmartResponse™

Automatically take action and respond to events and alarms

LogRhythm

Threat Lifecycle Management Platform

- Behavioral Security Analytics (User/Entity, Network & Endpoint)
- SIEM & Log Management
- Network Monitoring & Forensics
- Endpoint Monitoring & Forensics
- Security Automation & Orchestration

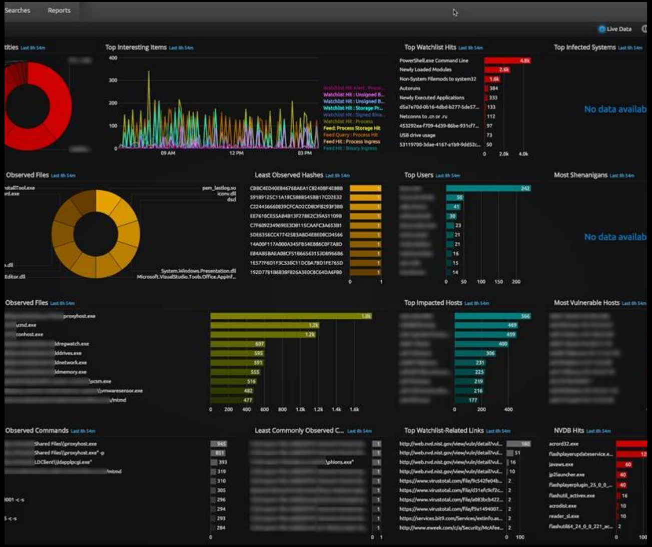
LogRhythm Labs

LogRhythm
The Security Intelligence Company

LogRhythm & Carbon Black: Overview

Together, LogRhythm & Carbon Black deliver enterprise-wide threat detection and response, providing a holistic view of attack activity.

Cb Response's complete endpoint detection & response solution combined with the advanced analytics & incident response capabilities of LogRhythm's TLM platform helps our customers:



- Visualize high priority events in Carbon Black-specific dashboard within LogRhythm's centralized console
- Automate adaptive threat response & expedite incident response
- Proactively identify malicious activity involving endpoints
- Streamline processes & prioritize investigations

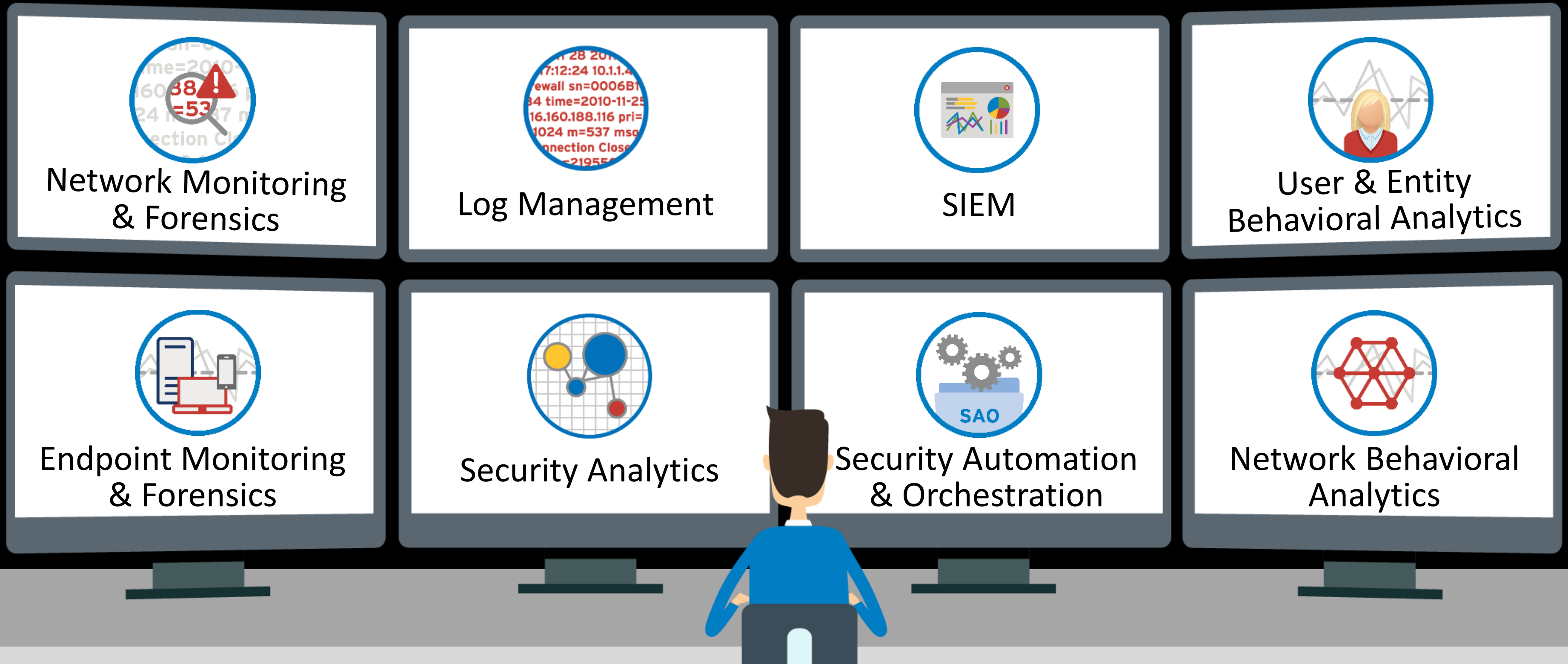
Use Case: Endpoint Lockdown

Challenge: Attacker-controlled endpoints can compromise additional systems. Left undetected, malware can quickly propagate across the network.

Solution: Cb Response sends recorded endpoint activity to LogRhythm's TLM platform. LogRhythm performs real-time analytics on received data & other flow, event, & machine data to quickly provide visibility into behavioral anomalies & indicators of compromised endpoints.

Additional Benefit: When a compromised endpoint is detected, a LogRhythm SmartResponse™ plugin can instruct Carbon Black to isolate the endpoint from the network until the malware is eradicated.

This Approach Is Not Effective



Network Monitoring & Forensics

Log Management

SIEM

User & Entity Behavioral Analytics

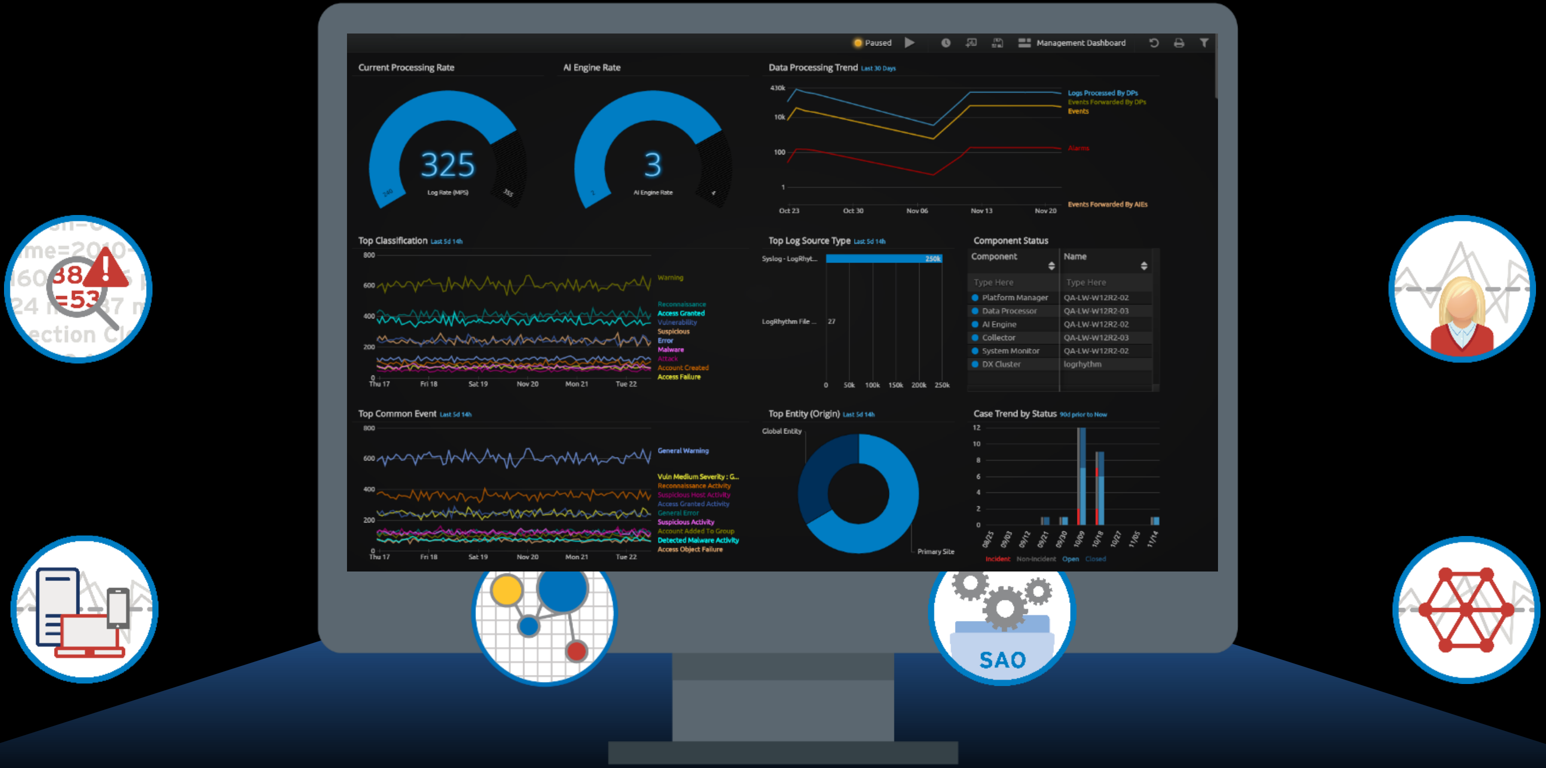
Endpoint Monitoring & Forensics

Security Analytics

Security Automation & Orchestration

Network Behavioral Analytics

Our Approach



Component Status

Component	Name
Type Here	Type Here
Platform Manager	QA-LW-W12R2-02
Data Processor	QA-LW-W12R2-03
AI Engine	QA-LW-W12R2-02
Collector	QA-LW-W12R2-03
System Monitor	QA-LW-W12R2-02
DX Cluster	logrhythm

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

LogRhythm™

The Security Intelligence Company

LogRhythm®

The Security Intelligence Company