LogRhythm
The Security Intelligence Company

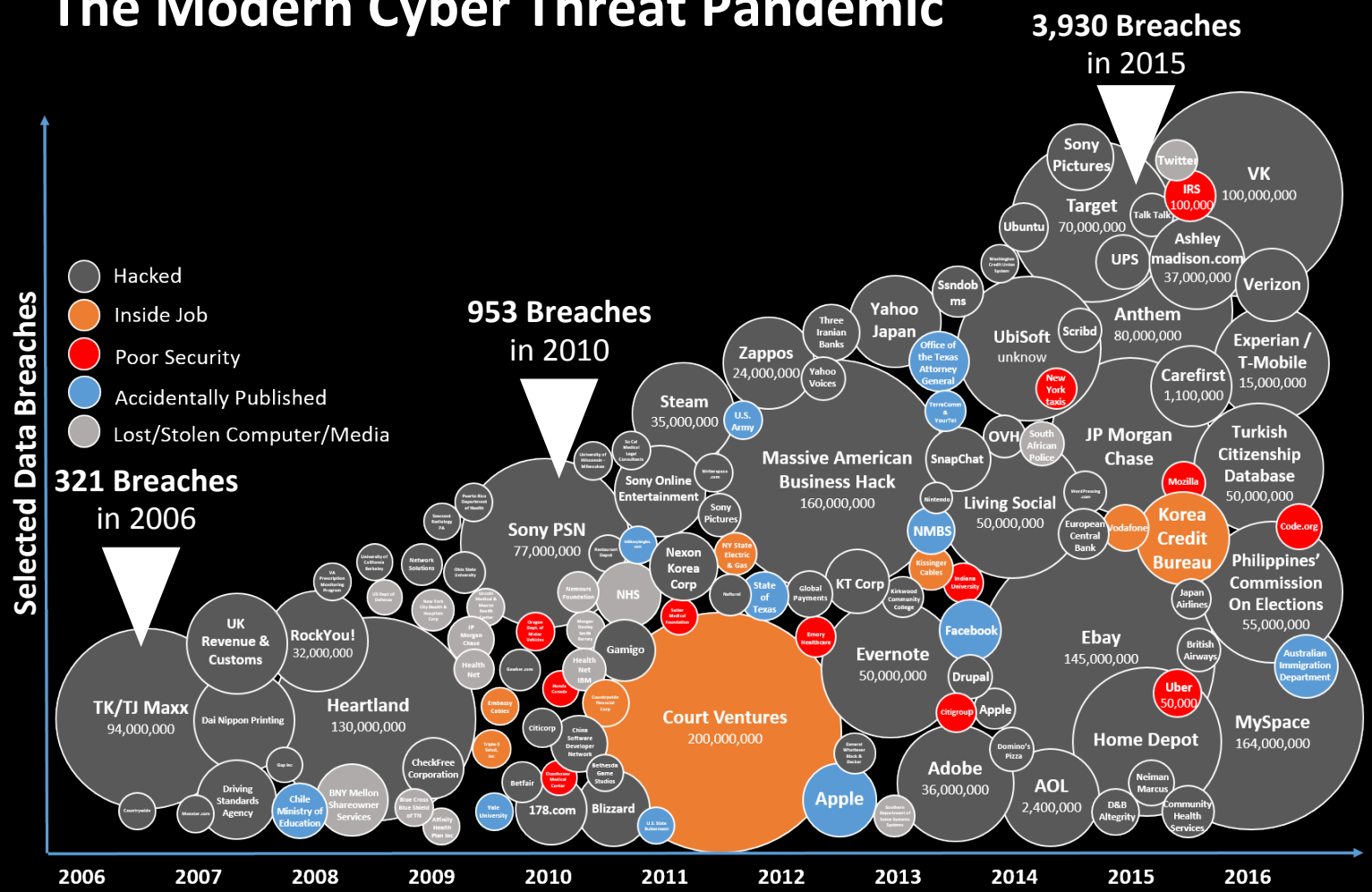
Maintaining Cyber Readiness in an Evolving Threat Landscape

Brent Benson

Brent.benson@logrhythm.com

320-492-6011

The Modern Cyber Threat Pandemic

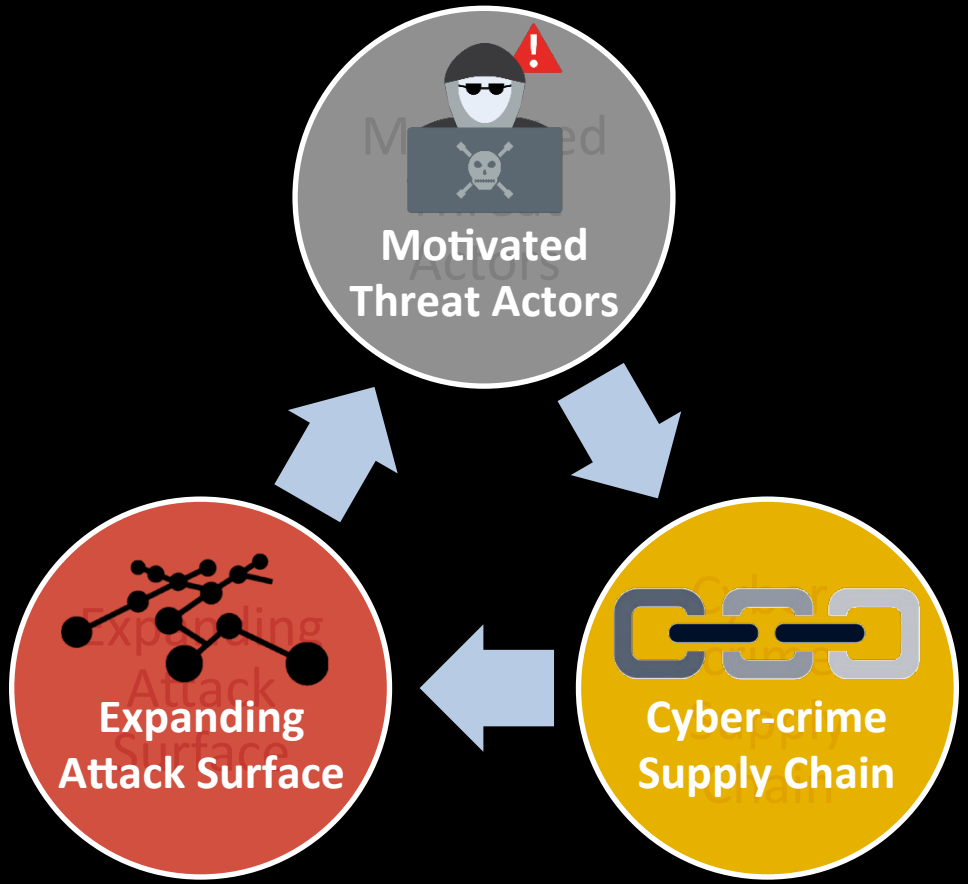


736 million records were exposed in 2015, compared to **96 million records** in 2010

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

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

No End In Sight



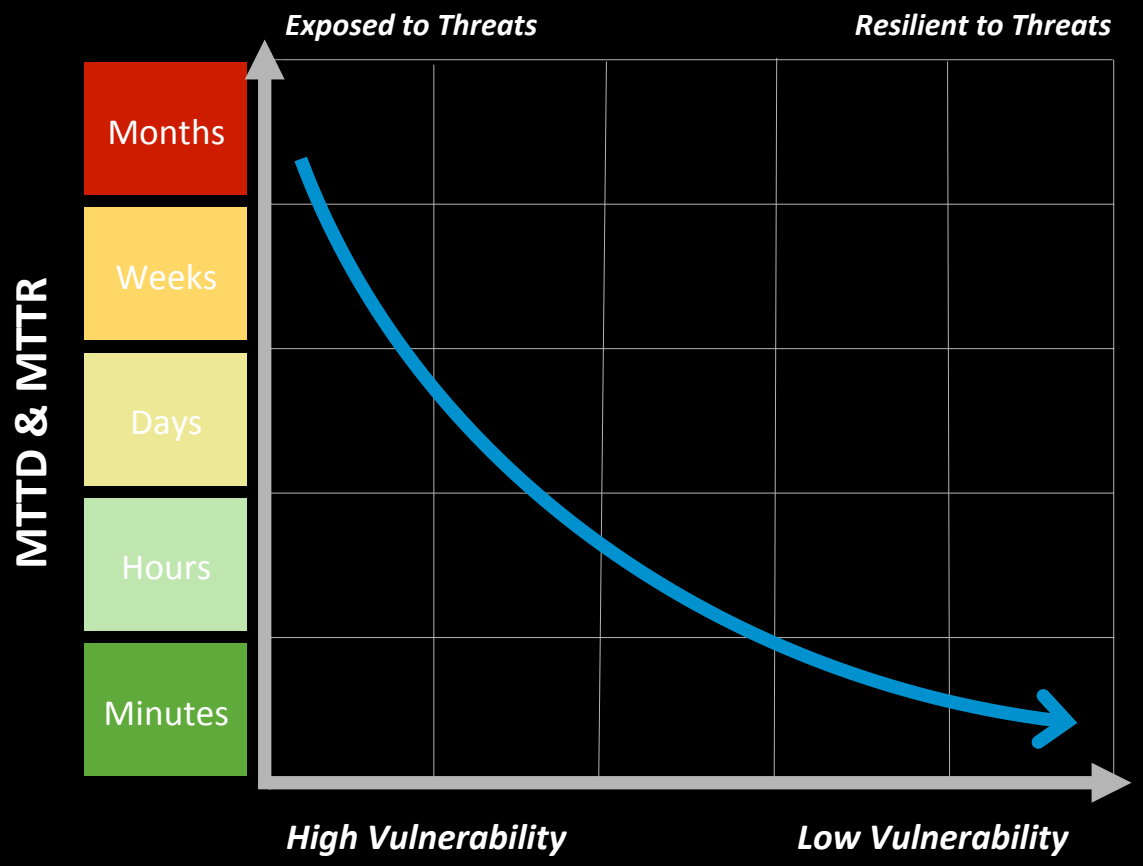
LogRhythm
The Security Intelligence Company

The Cyberattack Lifecycle

Modern threats take their time
and leverage the holistic attack surface

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

Obstacles To Faster Detection & Response

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

LogRhythm
The Security Intelligence Company

Obstacles To Faster Detection & Response


Alarm Fatigue


Swivel Chair Analysis


Forensic Data Silos


Fragmented Workflow


Lack of Automation

Effective

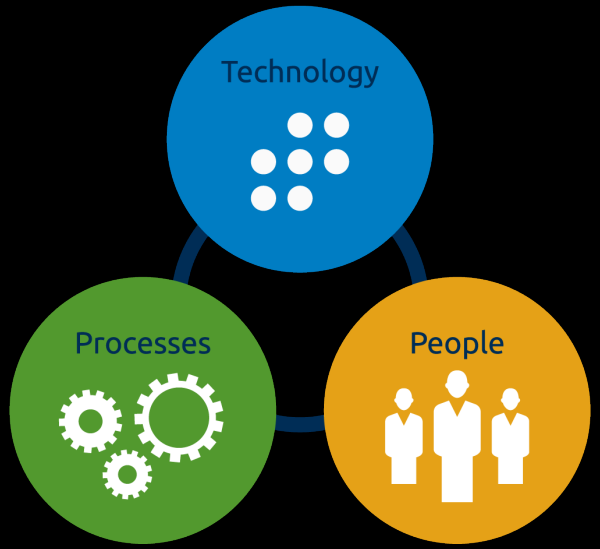
Threat Lifecycle Management

- ✓ Addresses these obstacles
- ✓ Enables faster detection and response to threats

LogRhythm
The Security Intelligence Company

Threat Lifecycle Management (TLM)

- Series of aligned security operations capabilities
- Begins with ability to “see” broadly and deeply across distributed IT environment
- Finishes with ability to quickly neutralize and recover from security incidents



Goal: reduce mean time to detect (MTTD) and mean time to respond (MTTR), without requiring increased staffing levels

LogRhythm
The Security Intelligence Company

Steps To Faster Detection & Response

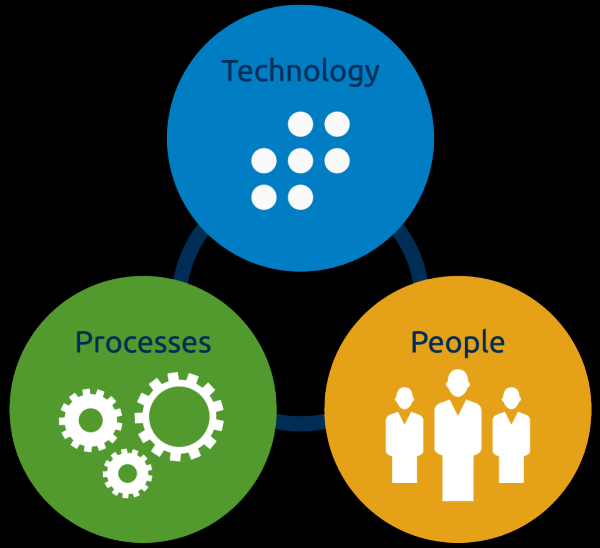
Understanding What You Have

Holistic Visibility

Deception Based Defenses

Round The Clock Monitoring

Security Awareness



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

This Approach Is Not Effective

Holistic Approach

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

Brent Benson

Brent.benson@logrhythm.com

320-492-6011

LogRhythm®
The Security Intelligence Company