Maintaining Cyber Readiness in an Evolving Threat Landscape

Brent Benson
Brent.benson@logrhythm.com
320-492-6011
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.
No End In Sight

Motivated Threat Actors

Expanding Attack Surface

Cyber-crime Supply Chain
Modern threats take their time
and leverage the holistic attack surface

The Cyberattack Lifecycle

Recon. & Planning  ->  Initial Compromise  ->  Command & Control  ->  Lateral Movement  ->  Target Attainment  ->  Exfiltration, Corruption, Disruption
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.
Obstacles To Faster Detection & Response

- Alarm Fatigue
- Swivel Chair Analysis
- Forensic Data Silos
- Fragmented Workflow
- Lack of Automation
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
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
Steps To Faster Detection & Response

- Understanding What You Have
- Holistic Visibility
- Deception Based Defenses
- Round The Clock Monitoring
- Security Awareness
End-to-End Threat Lifecycle Management Workflow

**TIME TO DETECT**

1. **Discover**
   - Forensic Data Collection
     - Security event data
     - Log & machine data
     - Forensic sensor data
   - Search analytics
     - Machine analytics

2. **Qualify**
   - Assess threat
     - Determine risk
     - Is full investigation necessary?

**TIME TO RESPOND**

3. **Investigate**
   - Analyze threat
     - Determine nature and extent of incident

4. **Neutralize**
   - Implement countermeasures
     - Mitigate threat & associated risk

5. **Recover**
   - Clean up
   - Report
   - Review
   - Adapt
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
HolisIc Approach

Forensic Data Collection
Discover
Qualify
Investigate
Neutralize
Recover
Brent Benson
Brent.benson@logrhythm.com
320-492-6011