Security Operations Maturity Model

Darren Cathey, Sr. Systems Engineer, LogRhythm

October 16, 2019

LogRhythm
The Security Intelligence Company

Introductions and Agenda

LogRhythm
The Security Intelligence Company

LogRhythm Attendees

Role	Contact Info
Regional Sales Manager	Andy Spielman Andrew.Spielman@logrhythm.com
Systems Engineer	Darren Cathey Darren.Cathey@logrhythm.com
Regional Sales Director	Steve Mosley Steve.Mosley@logrhythm.com
Sales Engineering Director	Isaac Thompson Isaac.Thompson@logrhythm.com

Agenda

The World as it Is

The LogRhythm Threat Lifecycle Management (TLM) Framework

The LogRhythm Security Operations Maturity Model (SOMM)

Real-Time SOMM Assessment

Building a SOC with Limited Resources (if time permits)

Next Steps

The World as it Is

LogRhythm
The Security Intelligence Company

Can you see the threat?

The Problem is Getting Worse…

Organizations continue to suffer disastrous data breaches

Company	Location	People Impacted	Date of Occurence
Careem	Dubai	14 million	2018
Cathay Pacific Airlines	Hong Kong	9.4 million	2018
SingHealth	Singapore	1.5 million	2015 - 2018
British Airways	UK	380,000	2018
Exactis	US	340 million	2018
Cambridge Analytica	US	87 million	2015
Chegg	US	50 million	2018
Ticketfly	US	27 million	2018
SHEIN	US	6.42 million	2018
Saks and Lord & Taylor	US	5 million	unknown
Orbitz	Global	880 million	2016 - 2017
MyHeritage	Global	92 million	2018
Google+	Global	52.5 million	2015 - 3/2018; 11/2018
Facebook	Global	29 million	2017 - 2018
Timehop	Global	21 million	2017 - 2018
myPersonality	Global	4 million	before 2012
T-Mobile	Global	2 million	2018

2019

Mandiant M-Trends 2018

- ✓ 4 in 10 breaches were detected via outside organizations versus internally
- ✓ Only ~21% of compromises were detected in under 2 weeks, and > ~60% took 2 months or longer to detect
- ✓ Threat actors were present on victims' networks for a median of 101 days before being detected.

The Cyber Attack Lifecycle

Modern threats take their time
and leverage the holistic attack surface

Effective Security Requires 100% Visibility

Security is of paramount importance, and it's all pervasive. Data is being generated at the edge, access, campus, branch, data center and cloud. **CISOs shouldn't be forced to restrict the amount of the data and what they protect, but unfortunately, that's often the case.**

Vinu Thomas
CTO of Presidio

Analysts Define What's Necessary for Effective Security

In order to be secure, Analysts say it's essential for SIEMs to empower customers to do the following:

Collect the Data	*"…need to be able to ingest where there are high (and increasing) **volumes** of data, from an increasing **variety** of sources, at potentially high **velocities** too…"*
Search the Data	*"…the ability to search through **data collected** by the SIEM over long periods of time is important to support **real-time** incident investigations, as well as threat hunting….need to perform fast searches across their log and event data with results in seconds, rather than minutes or hours…"*
Make Sense of the Data	*"SIEM tools now must solve big data issues for events…**enrichment** of raw machine data **with context** is becoming mandatory…expected to **enable the end-to-end threat detection and response process** while helping triage and prioritize alerts…"*

Gartner 2018 MQ Critical Capabilities & Gartner Technology Insights for the Modern SIEM 2018

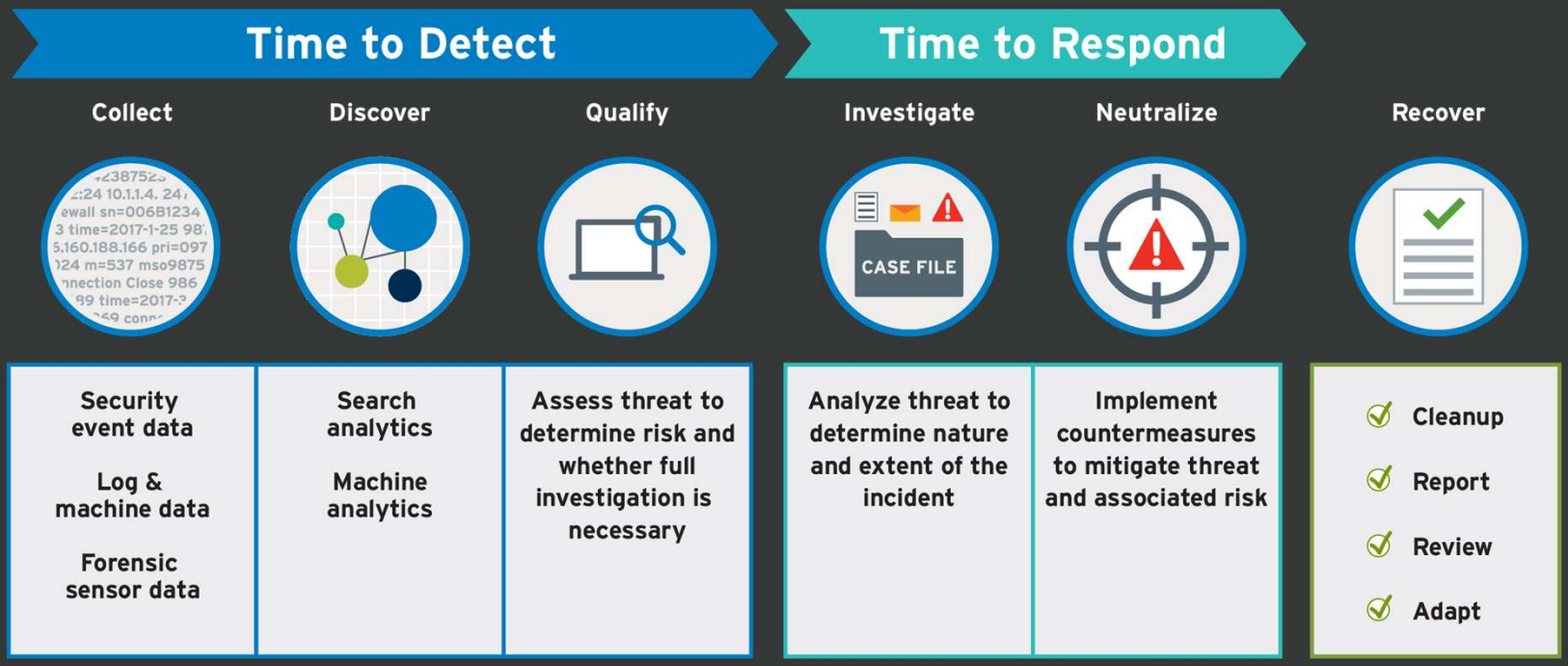
The Threat Lifecycle Management Framework

LogRhythm
The Security Intelligence Company

Threat Lifecycle Management Framework

- To make significant reductions in mean time to detect (MTTD) and mean time to respond (MTTR), you need an enterprise capability to detect and respond to threats across your entire IT/OT landscape.
- The Threat Lifecycle Management (TLM) framework describes the critical security operations capabilities and workflow processes you need to realize efficient and optimal reductions in MTTD/MTTR.
- MTTD and MTTR are the key measurable indicators of security operations maturity.

LogRhythm NextGen SIEM Platform and TLM

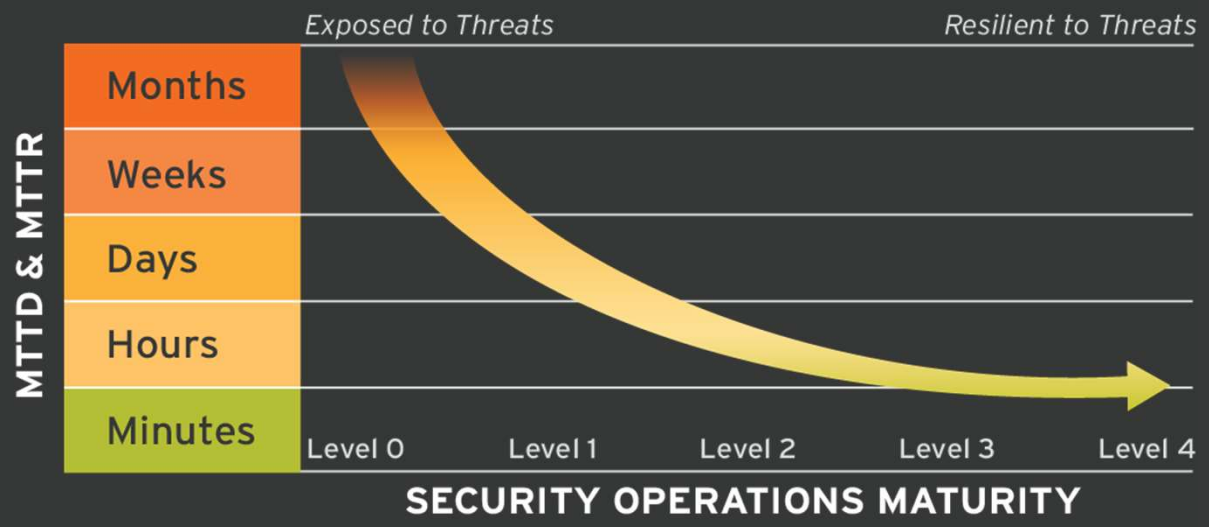


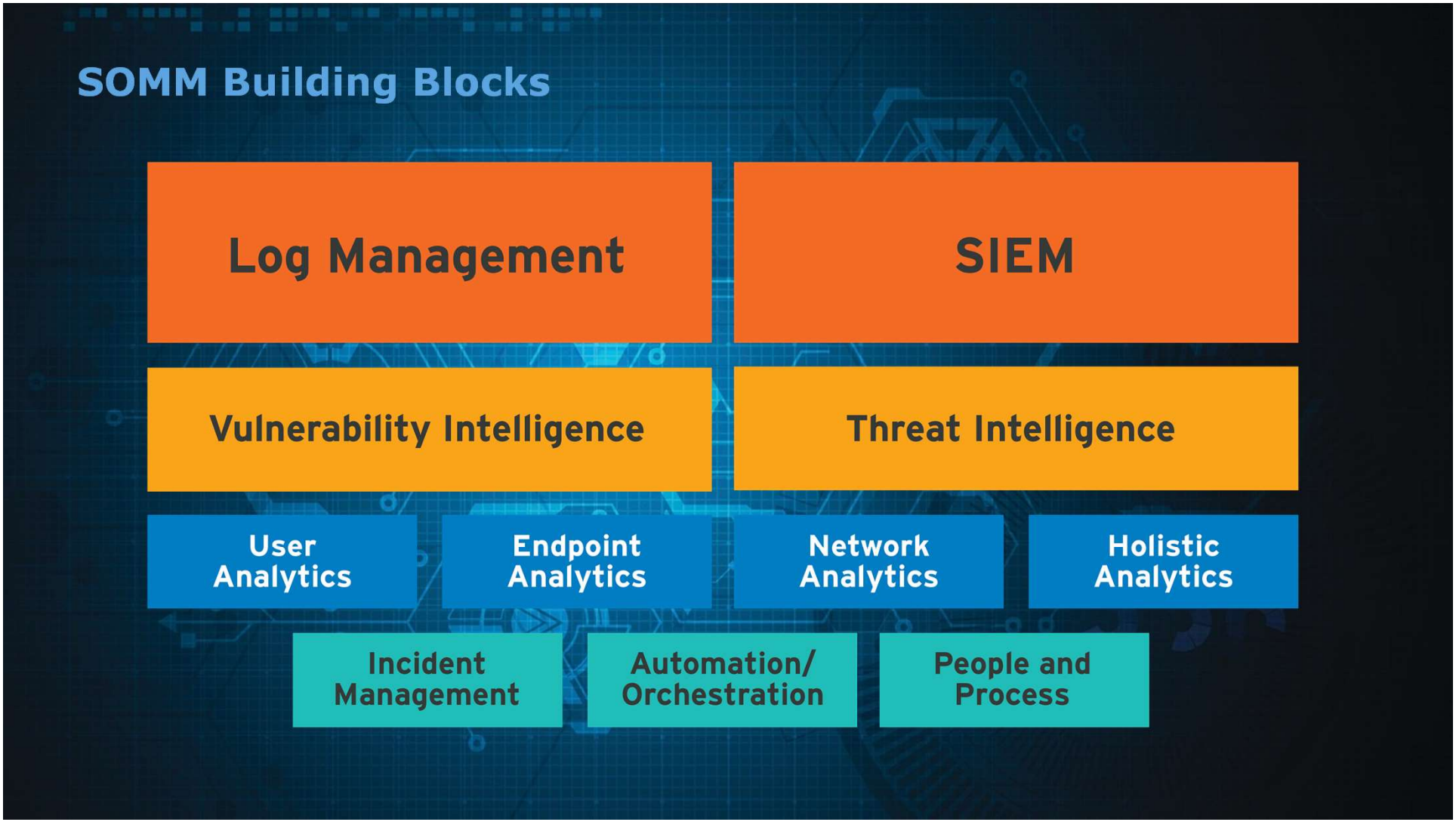
The LogRhythm Security Operations Maturity Model

LogRhythm
The Security Intelligence Company

The LogRhythm Security Operations Maturity Model

Level
0: Blind
1: Minimally Compliant
2: Securely Compliant
3: Vigilant
4: Resilient

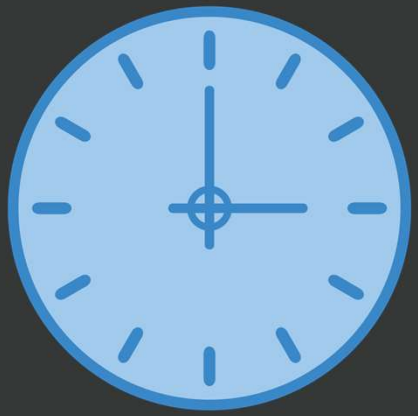



SOMM Building Blocks
Log Management
SIEM
Vulnerability Intelligence
Threat Intelligence
User Analytics
Endpoint Analytics
Network Analytics
Holistic Analytics
Incident Management
Automation/ Orchestration
People and Process

Log Management

100% Log Collection

Time Normalization



Log Protection

LOG MANAGEMENT

Self-Assessment: Log Management

Level	Description
0: Blind	Logs are not centrally collected
1: Minimally Compliant	Log collection and retention are primarily driven by audit requirements
2: Securely Compliant	Log collection is performed from all security devices, networking infrastructure, production servers, applications, and databases
3: Vigilant	Log collection also includes physical security systems and/or highest value endpoint systems, plus some personal devices
4: Resilient	Log collection is performed from all systems generating log and audit data

Security Information and Event Management (SIEM)

Structured & Unstructured

Correlation

Compliance

SIEM

Self-Assessment: SIEM

Level	Description
0: Blind	No SIEM
1: Minimally Compliant	SIEM is primarily used to demonstrate audit compliance
2: Securely Compliant	SIEM is used to monitor for and respond to compliance and security threats
3: Vigilant	SIEM is used to understand cybersecurity risk across the entire production environment
4: Resilient	SIEM is used to understand cybersecurity risk across the entire logical, physical, and social environment

Vulnerability Intelligence

Situational Awareness

Incident Validation

Visibility

VULNERABILITY INTELLIGENCE

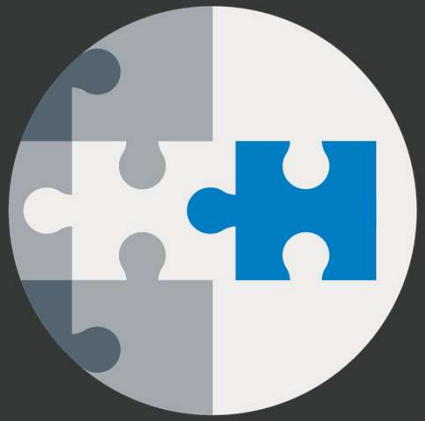
Self-Assessment: Vulnerability Intelligence

Level	Description
0: Blind	No vulnerability-management system (VMS)
1: Minimally Compliant	VMS scans only the systems in scope for compliance
2: Securely Compliant	VMS periodically scans network perimeter systems and highest-risk systems
3: Vigilant	Holistic vulnerability intelligence, with basic correlation and workflow integration
4: Resilient	Holistic vulnerability intelligence, with advanced correlation and automation workflow integration

Threat Intelligence

Structured IOAs & IOCs

Open Source & Commercial TI



Honey Pots

THREAT INTELLIGENCE

Self-Assessment: Threat Intelligence

Level	Description
0: Blind	No threat intelligence
1: Minimally Compliant	Limited use of open source threat intelligence
2: Securely Compliant	Reactive and manual threat intelligence workflow
3: Vigilant	IOC-based threat intelligence integrated into analytics and workflow
4: Resilient	Industry specific and internally generated IOC- and TTP-based threat intelligence integrated into analytics and workflow; sandboxing discovered malware to generate additional threat intel

User & Entity Behavior Analytics (UEBA)

User Monitoring

User Analytics

Privileged User Monitoring

USER ANALYTICS

Self-Assessment: UEBA

Level	Description
0: Blind	No specific monitoring of user activity
1: Minimally Compliant	Monitoring privileged users
2: Securely Compliant	Scenario-based monitoring all users for known bad activity
3: Vigilant	Real-time UEBA to monitor trends and patterns
4: Resilient	Real-time forensic monitoring deployed on every production server and user workstation in the environment in combination with UEBA

Endpoint Analytics

Server, Workstation, & Mobile Devices

Unusual or Malicious Activity

ENDPOINT ANALYTICS

Self-Assessment: Endpoint Analytics

Level	Description
0: Blind	No endpoint monitoring
1: Minimally Compliant	Endpoint monitoring is deployed on a limited number of servers within compliance scope
2: Securely Compliant	Real-time forensic monitoring, including FIM and process monitoring, is deployed to some production servers
3: Vigilant	Real-time forensic monitoring, including FIM and process monitoring, is deployed to all production servers
4: Resilient	Real-time forensic monitoring is deployed on every production server and user workstation

Network Analytics

Network Audit Logging

Layer 7 Monitoring

NETWORK ANALYTICS

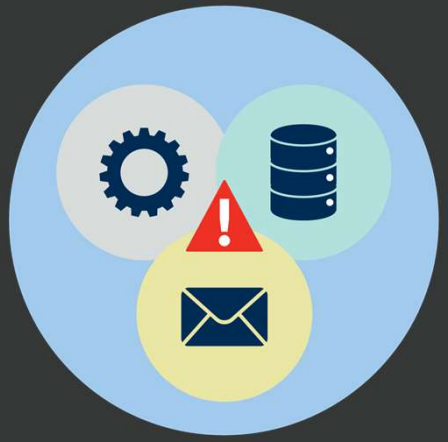
Self-Assessment: Network Analytics

Level	Description
0: Blind	No network forensic solution
1: Minimally Compliant	Ad-hoc packet capture used for troubleshooting
2: Securely Compliant	Ad-hoc packet capture used for after-the-fact analysis
3: Vigilant	Real-time network forensic monitoring solutions deployed at internet egress points
4: Resilient	Real-time network forensic monitoring solutions deployed at multiple locations

Holistic Analytics

Holistic Correlation

Corroborated Threat Indicators



HOLISTIC ANALYTICS

Self-Assessment: Holistic Analytics

Level	Description
0: Blind	No analytics applied to log data
1: Minimally Compliant	Real-time analytics on exception-based data to detect compliance violations
2: Securely Compliant	Real-time scenario-based analytics corroborated across log source types
3: Vigilant	Real-time scenario-based analytics across all systems; behavior-based analytics for targeted use cases
4: Resilient	Detailed mapping and implementation of both scenario and behaviour-based analytics across wide ranging data sources for holistic security analytics

Incident-Management Tools

Case Management

Digital Evidence Locker

INCIDENT MANAGEMENT

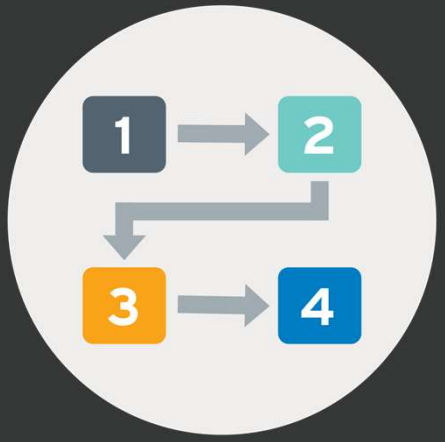
Self-Assessment: Incident Management

Level	Description
0: Blind	No tools for incident management
1: Minimally Compliant	Best efforts for incident management
2: Securely Compliant	Disparate tools and systems to manage incidents
3: Vigilant	Security tools integrated with centralized help desk-style ticketing platform; incident triage and response process documented
4: Resilient	Centralized incident-management platform with rapid access to all log data; secure storage for evidence and case-management workflow; communication plans in place; response tested by table-top exercises.

Security Orchestration and Automation

SmartReponse™

Playbooks



SECURITY ORCHESTRATION & AUTOMATION

Self-Assessment: Security Orchestration & Automation

Level	Description
0: Blind	No tools for orchestration & automation
1: Minimally Compliant	Limited ad-hoc re-usage of some pre-built scripts
2: Securely Compliant	Limited internal automation of SIEM tooling
3: Vigilant	Basic automation to improve the efficiency and speed of threat investigation and incident response processes; playbooks defined for most common threats
4: Resilient	Extensively automated threat qualification, investigation, and response processes; playbooks defined for advanced threats (e.g., APTs)

People and Process: Your SOC

Process

People

Routine Checks

PEOPLE & PROCESSES

Self-Assessment: People & Process

Level	Description
0: Blind	No trained or skilled security analysts
1: Minimally Compliant	Ad-hoc monitoring and response on a best effort basis; some formal processes
2: Securely Compliant	Basic processes for monitoring alarms and responding to security incidents; tiered responsibilities; potentially an outsourced incident response capability
3: Vigilant	Formal playbooks document processes; basic metrics collected; 8x5 virtual or physical SOC; dedicated analysts but skillset not yet comprehensive
4: Resilient	Advanced operational metrics and reporting; continual review of processes; 24x7 virtual or physical SOC; dedicated and skilled analysts cross trained, with extensive reactive and proactive capabilities.

Real-Time SOMM Assessment

LogRhythm
The Security Intelligence Company

SOMM Assessment Survey

- Use the Survey below to Assess your Maturity:

https://surveyhero.com/c/12b8f887

- There are 11 Questions… multiple choice

  … Works on both Computers and Phones

- We'll take about 10 Minutes for the Survey

  … then take a Look at the Responses!

SOMM Survey Results

Let’s Take a Look at the Assessment Results

Next Steps

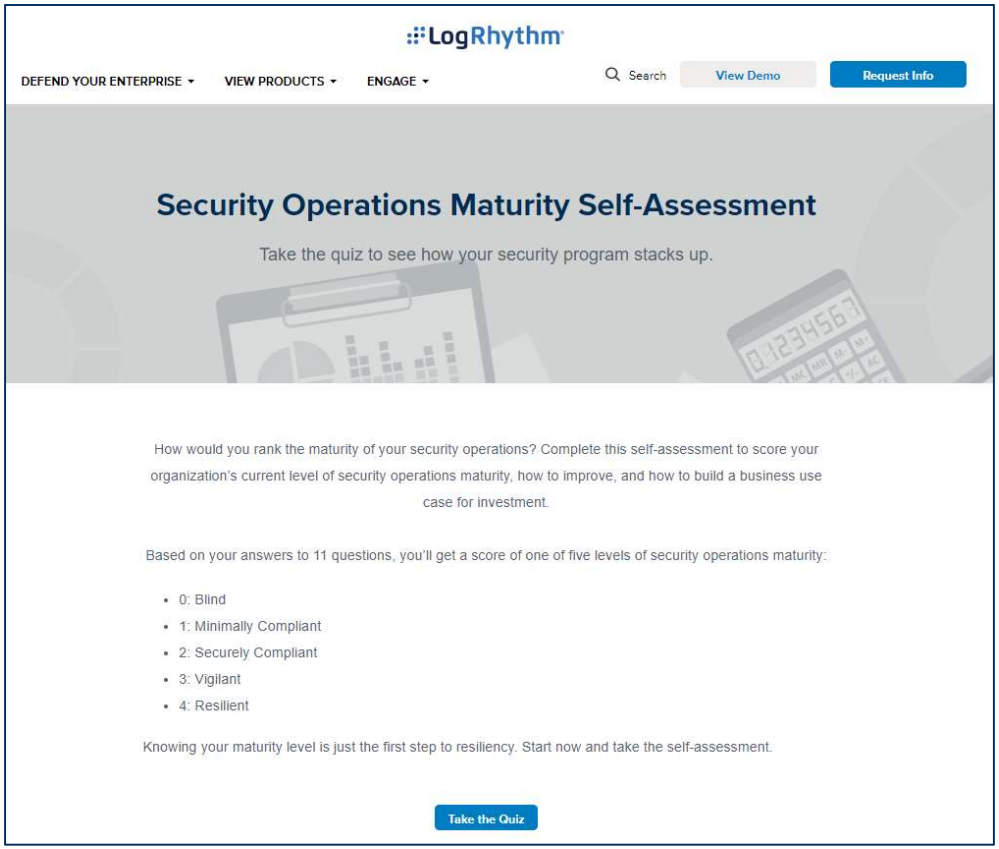
LogRhythm
The Security Intelligence Company

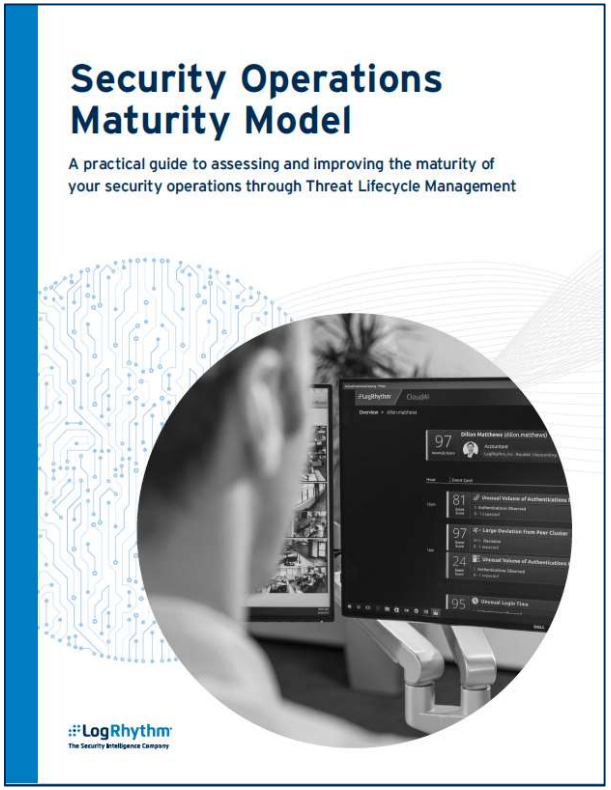
SOMM Survey Results

- **Get a Sample SOMM Maturity Report**
- **Based on the Results from Today**
- **Email me:**

Darren.Cathey@logrhythm.com

Online SOMM Assessment and White Paper

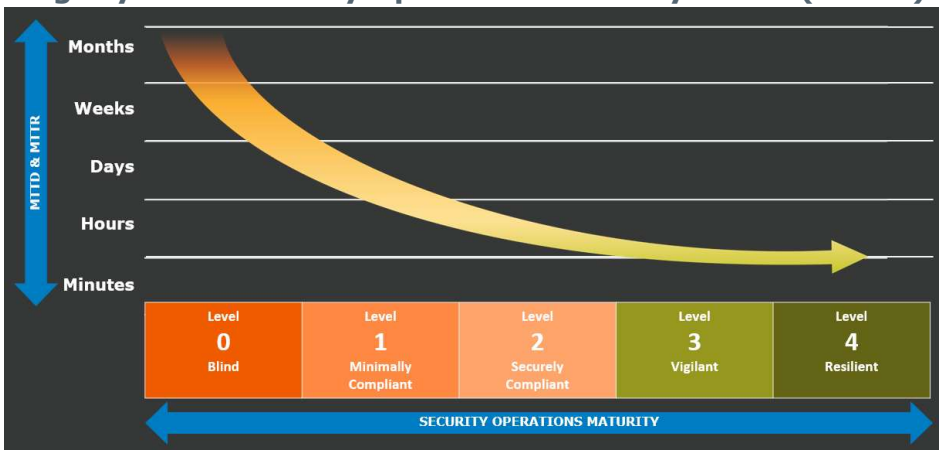




Let Us Support Your Ongoing Security Maturity Journey

- Reaching your desired level of **security maturity is a journey**
- As a committed partner, we use our **Security Operations Maturity Model** to help you evaluate your current posture and build a **roadmap to reach your security goals**

LogRhythm's Security Operations Maturity Model (SOMM)



Gartner peerinsights customers' choice 2019

Our customers appreciate our partnership on their Security Maturity journey. This typically starts with a SOMM Workshop. If you are interested in hearing more about this, let us know.

7 steps to building an efficient and effective SOC

If your organization cannot justify the overwhelming expense of a 24x7 SOC, **there is a solution**.

To get in-depth guidance on how to build and budget for a SOC, download the *How to Build a SOC with Limited Resources White Paper.*

Download Now


LogRhythm®
The Security Intelligence Company
Thank You!

Building a SOC with Limited Resources

LogRhythm
The Security Intelligence Company

The state of the understaffed SOC

Most organizations don't have the resources to staff a 24x7 security operations center (SOC).

The result?

- Events not monitored around the clock
- Major delays in detecting and responding to incidents
- Inability to hunt for threats proactively

It's a dangerous situation.

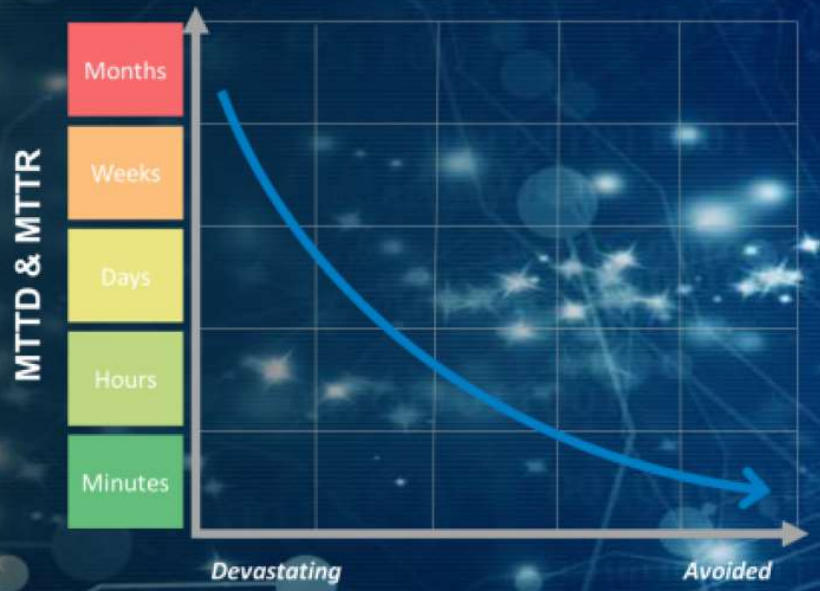
But there is a solution

With an automated SOC built for scale, your team can:

Detect threats swiftly: Your team can perform constant event monitoring.

Respond to threats rapidly. Your team can expedite incident response.

Building an efficient, automated SOC with the resources you have is about **combining people, process, and technology to achieve your goals**.




7 Steps to Building a SOC with Limited Resources
Learn to build a SOC that efficiently leverages Threat Lifecycle Management to rapidly detect and respond to threats.


LogRhythm
The Security Intelligence Company
Step 1
Step 2
Step 3
Step 4
Step 5
Step 6
Step 7

Develop your strategy

The key to developing your strategy is to understand the current state of your organization.

- ✓ Assess your existing capabilities
- ✓ At first, limit your scope to core functions:
  - Monitoring
  - Detection
  - Response
  - Recovery
- ✓ Delay non-core functions until your core functions are sufficiently mature
- ✓ Identify and define business objectives

Design the solution

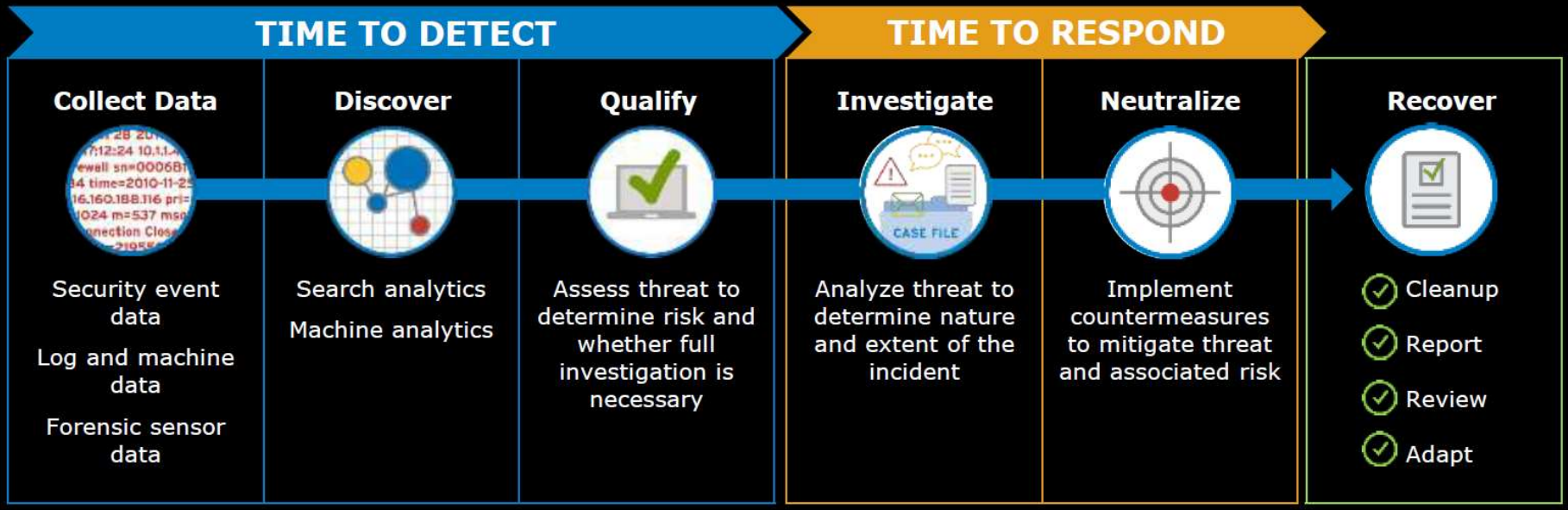
Good places to start.

- ✓ Choose a few business-critical use cases (e.g., a phishing attack)
- ✓ Define your initial solution based on these use cases
- ✓ Consider that your solution must be able to meet future needs

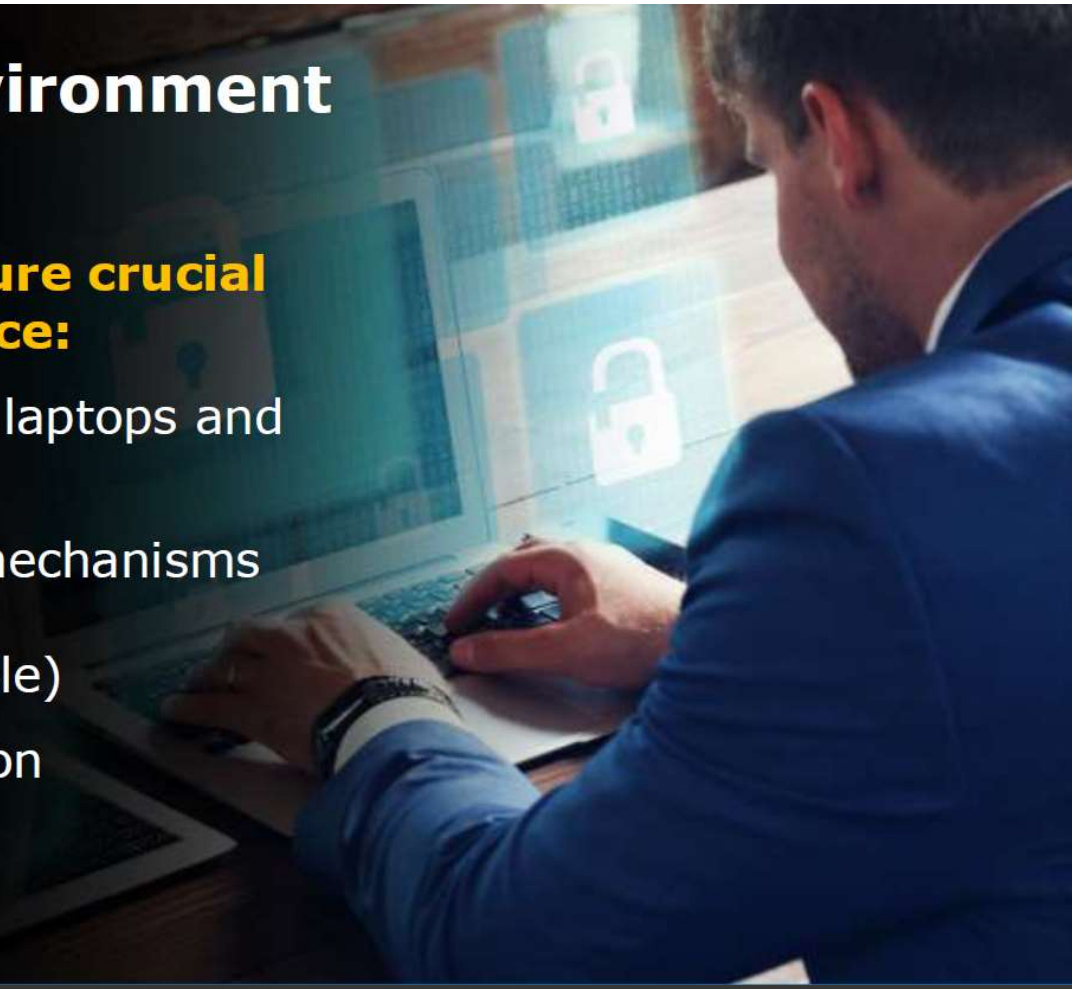
A narrow scope will reduce the time to initial implementation which will help you achieve results faster.

Create processes, procedures and training

In Step 3, it's important to make sure that all six phases of the Threat Lifecycle Management Framework are covered.



Prepare your environment



Before deployment, make sure crucial security elements are in place:

- ✓ Ensure SOC staff desktops, laptops and mobile devices are secure
- ✓ Put secure remote access mechanisms in place for SOC staff (and outsourcers if applicable)
- ✓ Require strong authentication

Implement your solution

Take full advantage of your technology to minimize the workload on your staff:

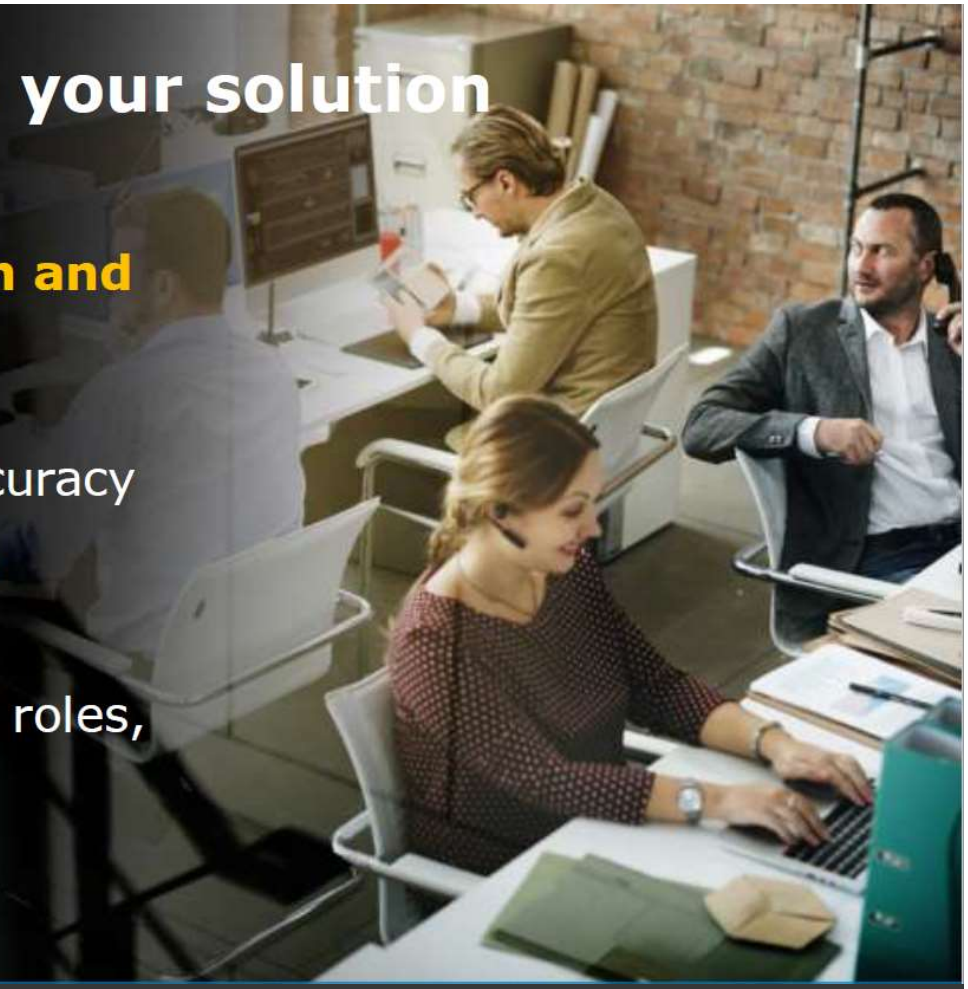
1. Bring up your log management infrastructure.
2. Onboard your minimum collection of critical data sources.
3. Bring up your security analytics capabilities.
4. Onboard your security automation and orchestration capabilities.
5. Begin deploying use cases to focus on end-to-end threat detection and response realization.

Deploy end-to-end use cases

Your tech is in place and your capabilities are deployed. Now for the fun part.

- ✓ Implement your use cases across your analytics and security automation and orchestration tiers.
- ✓ Test your use cases rigorously over a variety of shifts and during shift changes.
- ✓ Proof the reliability and security of your solution.

Maintain and evolve your solution



A SOC isn't something to turn on and stop thinking about. It requires ongoing maintenance, such as:

- ✓ Tuning to improve detection accuracy
- ✓ Adding other systems as inputs or outputs
- ✓ Reviewing the SOC model, SOC roles, staff counts


LogRhythm
The Security Intelligence Company
Step 1
Step 2
Step 3
Step 4
Step 5
Step 6
Step 7


LogRhythm®
The Security Intelligence Company
Thank You!