RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

SESSION ID: AIR-W11

Diagnosis SOC-Atrophy: What To Do When Your SOC Is Sick

Tony Cole
VP / Global Government CTO
FireEye
@nohackn

Apply: Fixing Your Sick SOC

Educate + Learn = Apply

I'm here to provide the principles on how to make your SOC more effective

Attendees will learn how to identify a sick SOC and take the steps to heal it

This knowledge can be applied at your organization to make your SOC work

Take every session at RSA as a learning opportunity and then apply those principles!

Adversaries Continue to Evolve TTPs

Offense

CodeRed

Melissa

Spam

SPAM

Spyware

Trojans

Worms, Bots

Zero-days

Phishing

Rootkits

APTs

Ransom-Ware

Mobile Threats

IoT Threats

Opportunistic

Targeted

1990s

2000s

2010s

Today

Defense

Birth of AntiVirus

URL Filtering

Data Loss Filtering

Grey-listing

Whitelisting

Heuristics

Behavioral Analysis

Detonation Chambers

Lots of New Stuff

Intelligence

FireEye
SECURITY REIMAGINED

Has Your SOC Evolved With Them?

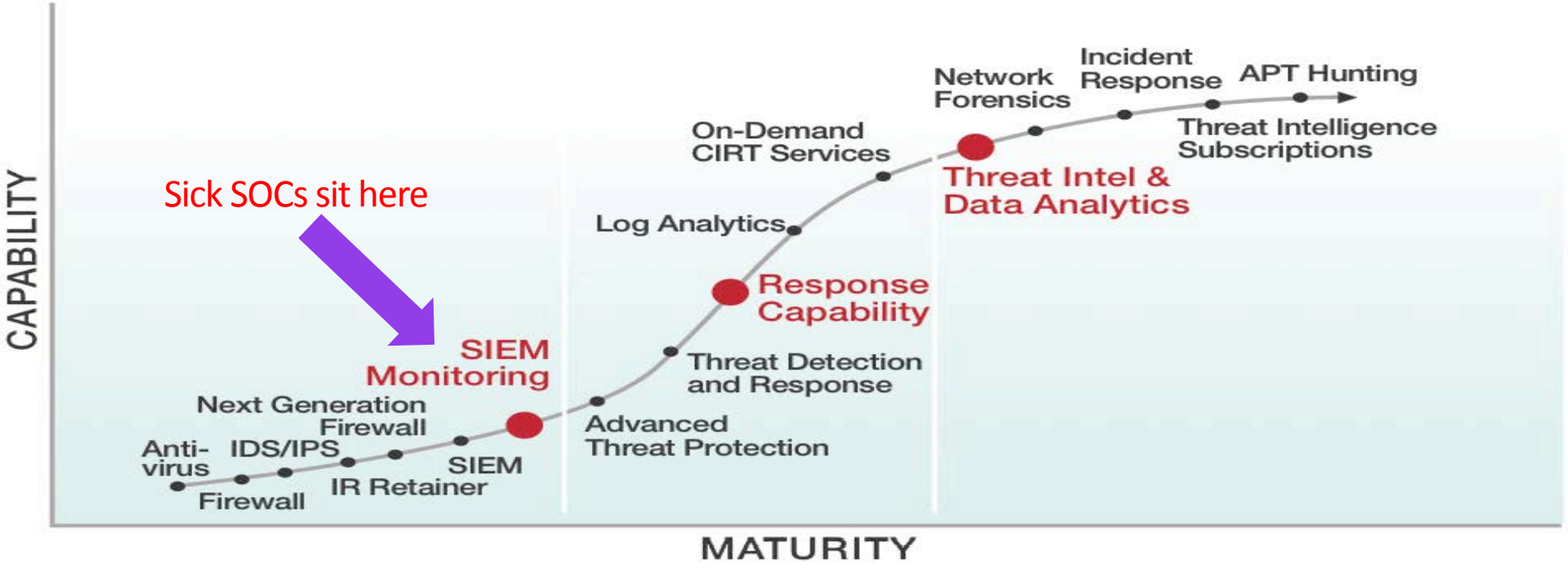
It's unlikely if it looks like this one.

If it does, go home, you're in the wrong line of business.

Symptoms of a Sick SOC

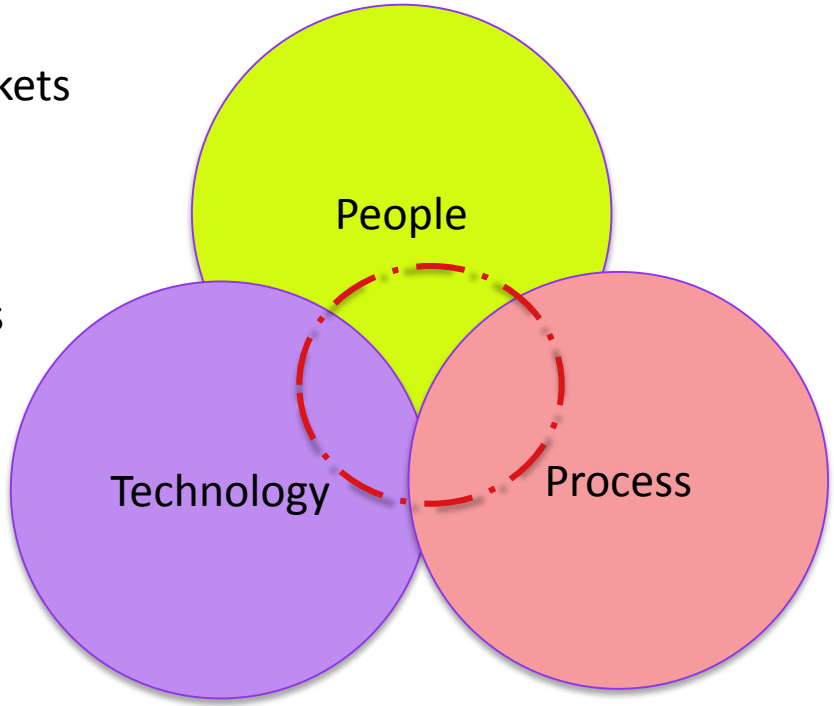
- Alert fatigue for your analysts
  - Causes high staff attrition rates
- Continuously reimaging systems
  - Not identifying the cause of the breach
- No updates to IR plan or associated processes
- Long adversary dwell times
- Limited capability (and typically unaware of it)

SOC Maturity Curve



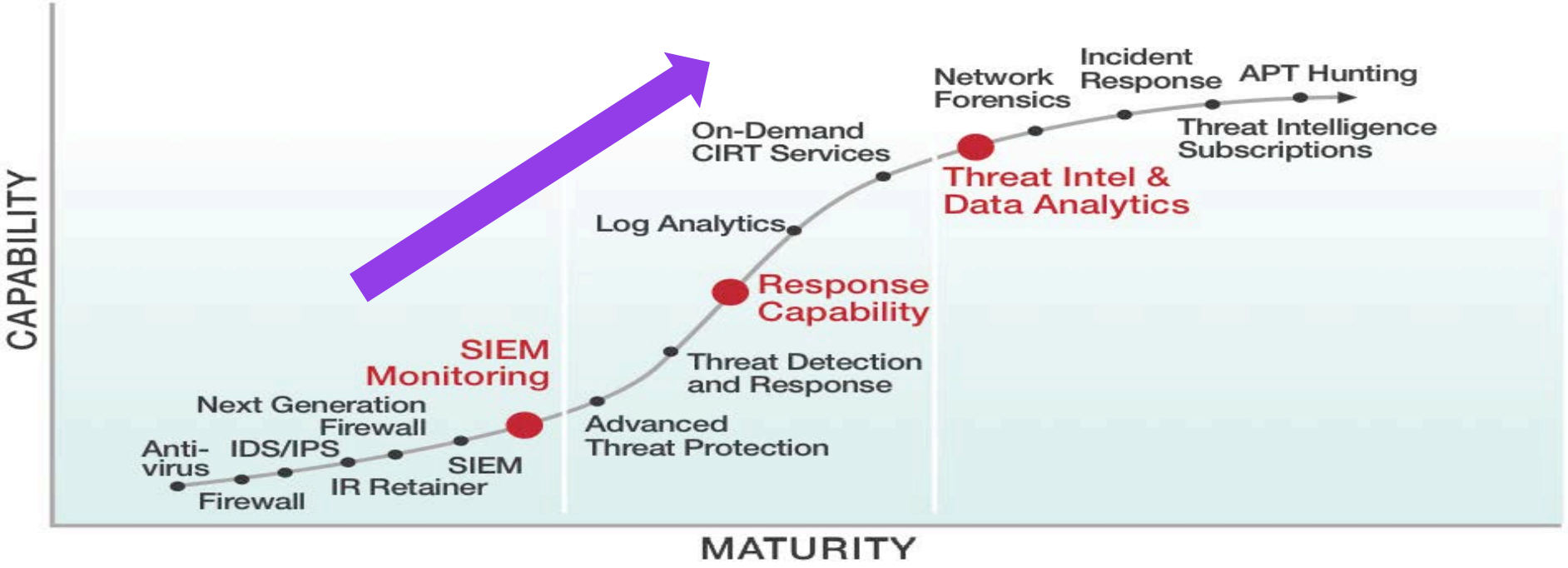
Real-Life Sick SOC Examples

- Reactive to Alerts
- Focus on Closing Tickets
- Resolution without Comprehension
- Alert Centric
- Lengthy Dwell Times

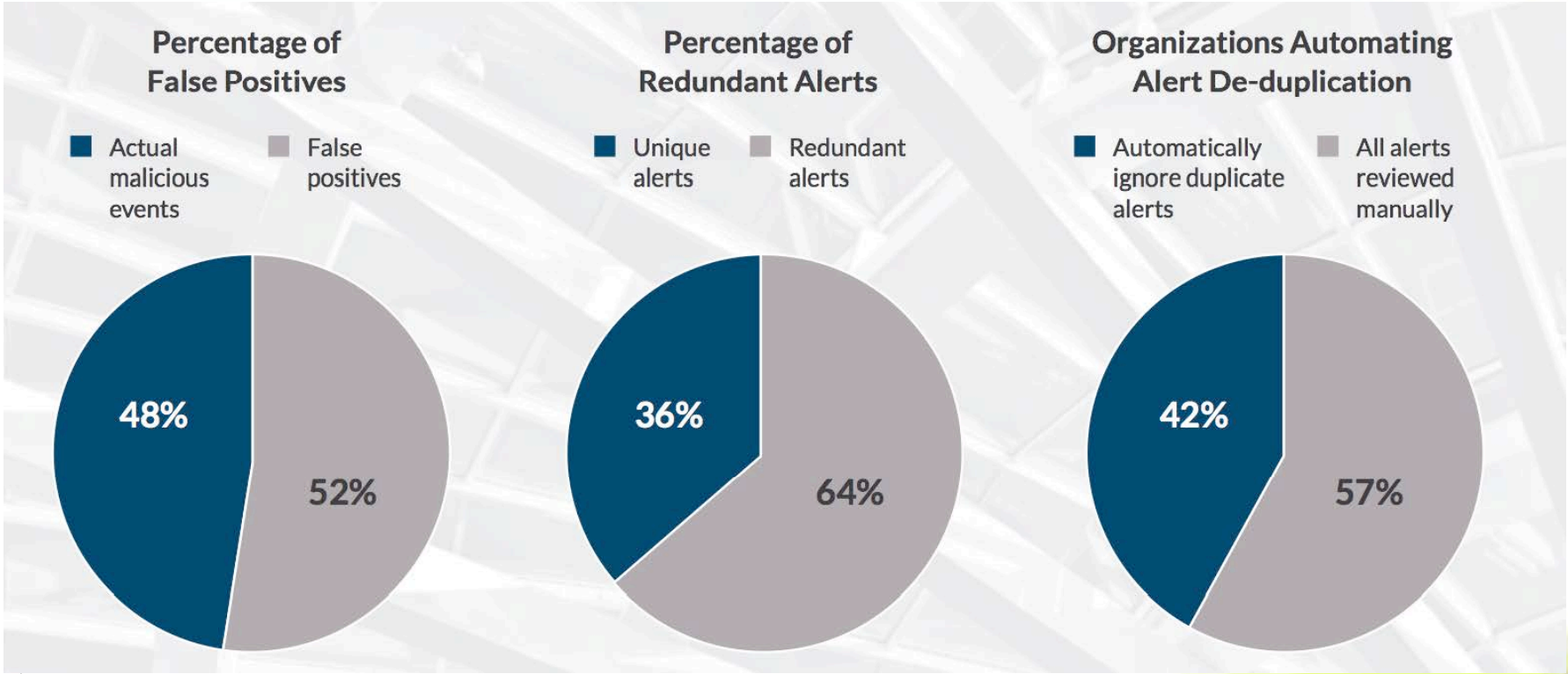


- High turnover
- No Cohesive process
- Little ROI
- No Orchestration
- Little Automation
- No Hunting

How Do We Climb the Maturity Curve?



Eliminate Alert Fatigue



Eliminate Continuously Reimaging Systems

Old Malware Focus

Reimage the machine

New Attacker Focus

Identify the actions of the attacker, the scope of the compromise, the data loss, the steps required to remove the attacker, and the approach required to re-secure the network utilizing threat actor intelligence

Implementing A Living IR Plan

- Clearly defined roles & responsibilities with organizational alignment & training to follow workflow
- Feedback loop to re-evaluate SOC/IR processes, use-cases on an on-going basis
- Monitoring and operational framework is documented, updated and easy to access

Implementing A Living IR Plan

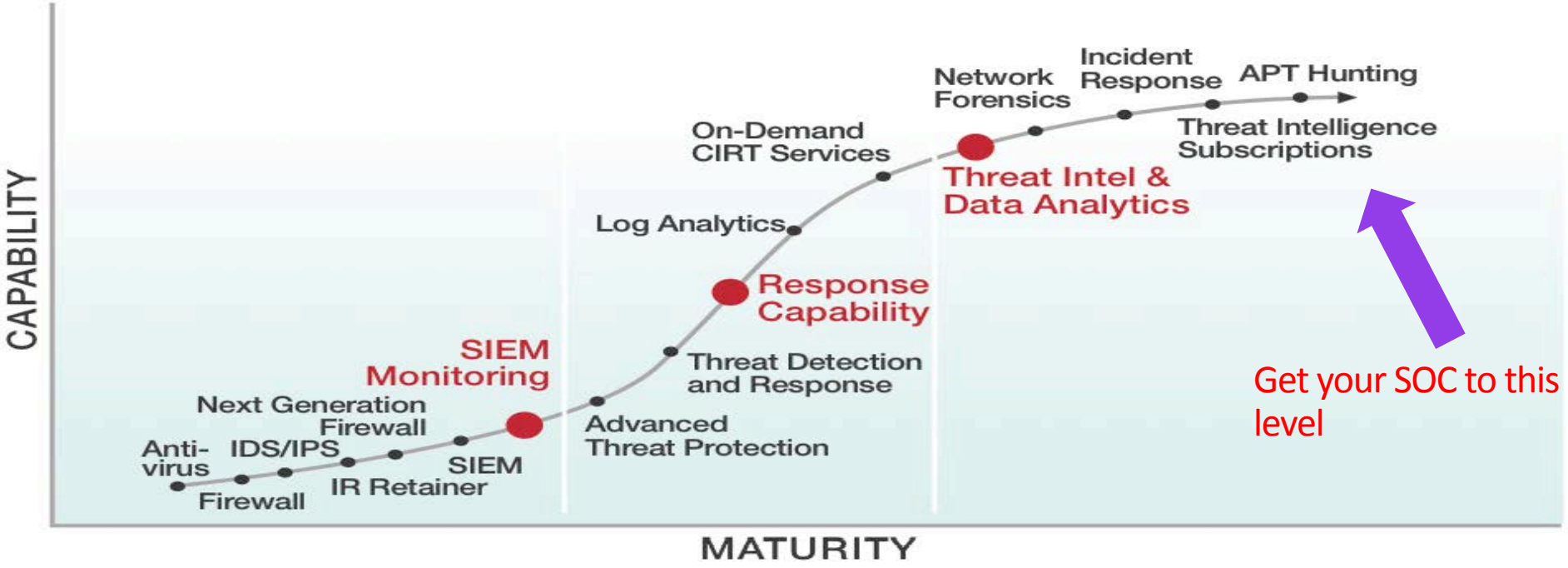
- Correlates internal threat data with threat intelligence from multiple sources
- Cooperation across all orgs and effective communication at all levels
- Has executive support and sponsorship from the very top
- Support for Hunting in the environment at the Network and Endpoint level to warrant out all beachheads established during compromise

Eliminate Adversary Dwell Times

- Update your detection methods with an adversary intelligence led focus
- Create partnerships with law enforcement, vendors, CERT organizations
- Share threat data, analyze and consume threat data
- Continuously learn and implement new processes

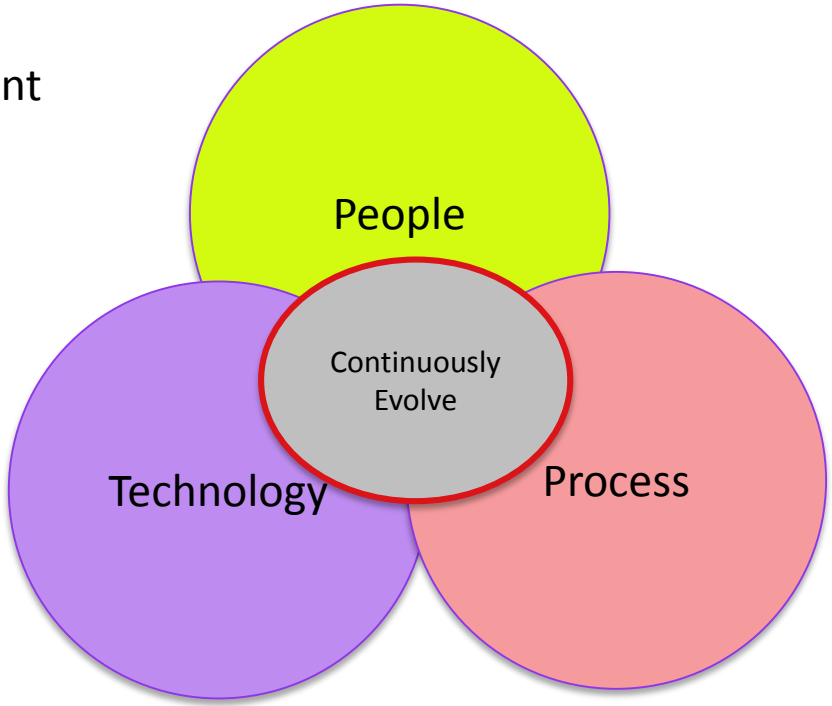
*Dwell Time is the amount of time an adversary spends in your enterprise after the compromise before being detected

SOC Maturity Curve



Healthy SOC Examples

- Hunting for IOCs
- Network and Endpoint IOC Focus
- Intelligence Led Approach
- Threat Containment
- Short Dwell Times



- Application Knowledge
- ROI for IT and Business
- Continuous Process Improvement

Apply –Do These Five Things

- Get an independent assessment
- Review and utilize best practices
- Solve analyst fatigue
- Continuous Process Improvement
- Institutionalize the fact that proper cyber security is a marathon

Thanks

@nohackn