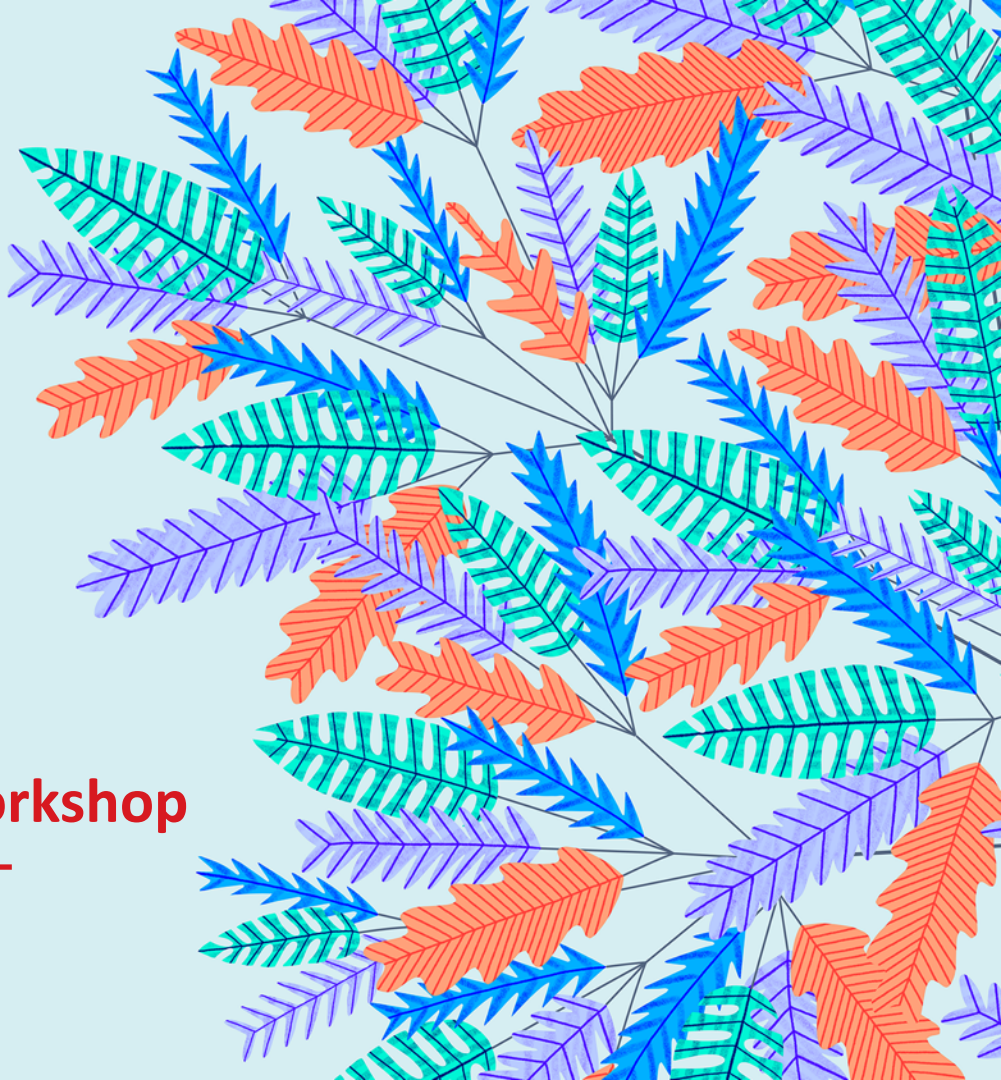
Evolving Your SOCs with Trend Micro OpenSOC XDR

France-Japan Cybersecurity Workshop



Vision: A World Safe for Exchanging Digital Information

1988

Peace of mind computing

1998

Your Internet Virus Wall

2008

Securing Your Journey to the Cloud

2018

Securing Your Connected World

Strategy: Continually Adapt Protection

$$x = i + u - t$$

Anticipate shifts in infrastructure

Embrace changes in user behavior

Adapt protection for full range of threats

The Hardest Job in Tech

On the Minds of Global CSOs

Increasingly active regulatory environment

Endless shortage of skill sets

Vendor consolidation

Rise of the SOC and incident response

Shadow IT becomes real IT

Evolution of CISO and SOC/IR activities

- Compliance CISO = 50%
  - Auditing, reporting, governance, and controls
- “Sweepers” - Integrator CISO = 25 %
  - IOC platform, Open/API driven, SOAR, eDR/MDR
- “Hunters” – Anomaly CISO - 25 %
  - Analytics, Behavioral and account ML/AI, baseline & anomaly detection

50-90,000

250,000

2,000,000

The Reality

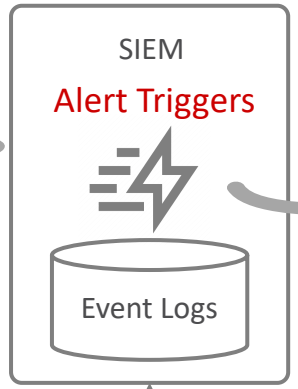
- That average fortune 1000 company SOC has 50-90,000 events per SECURITY events per second into their SIEM
- We have a customer with 250,000 events per second (government)
- We have a TippingPoint customer with 2M events per day JUST from TippingPoint

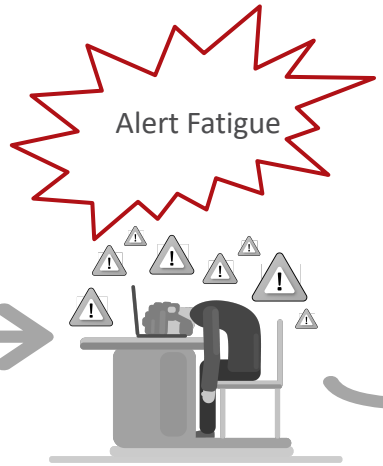
- Most customers deal with manually by having a SOC tier1 analyst (Triage) look at these events and try to determine what is important
- We love our SIEM partners and we do not do SIEM, but the math-based approach of SIEM is not working and customers are asking Trend Micro how we can help because we have a lot more context on threat behavior than just math-based correlation

SOC with only SIEM

Security Architect
Hunters

Writing detection rules and define alert trigger conditions on top of SIEM based on the collected data. Once matched, trigger an alert for analysts to follow up the triage.





Triage Team

IR Team/Senior Analysts

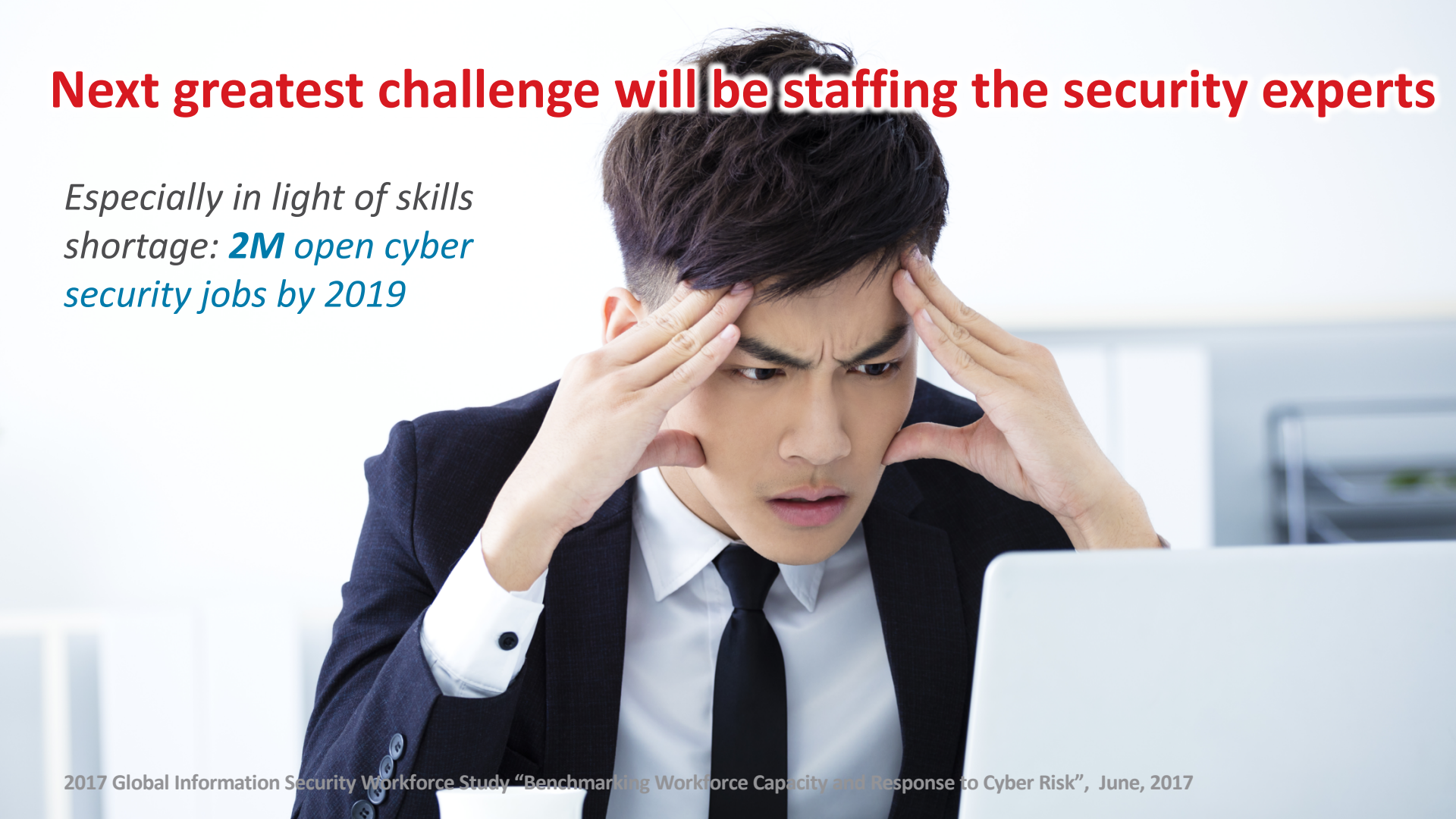
Security Event Logs

SMS | DDD | DSM | Apex One | CAS

TREND MICRO

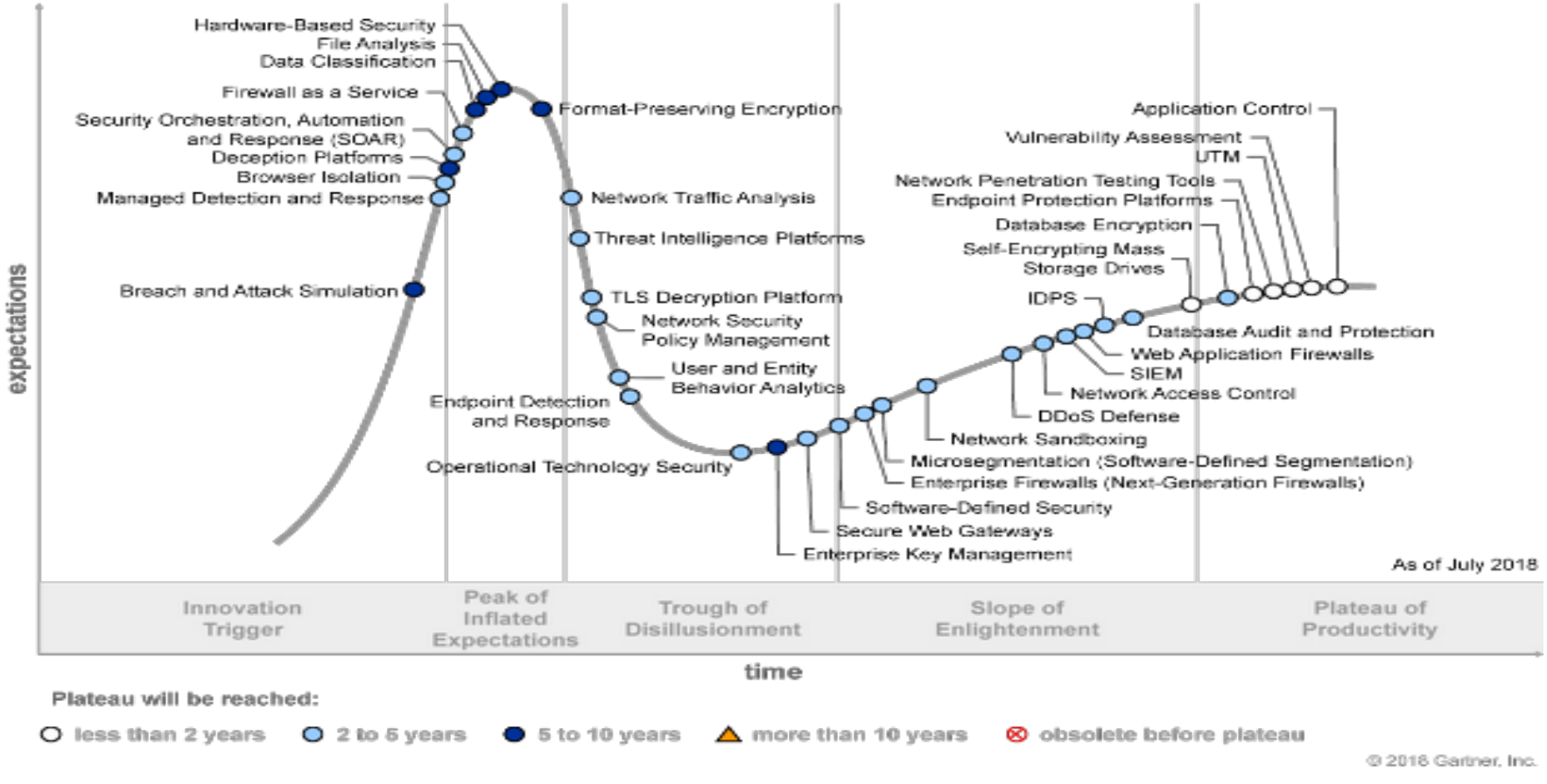
Next greatest challenge will be staffing the security experts

*Especially in light of skills shortage: **2M** open cyber security jobs by 2019*

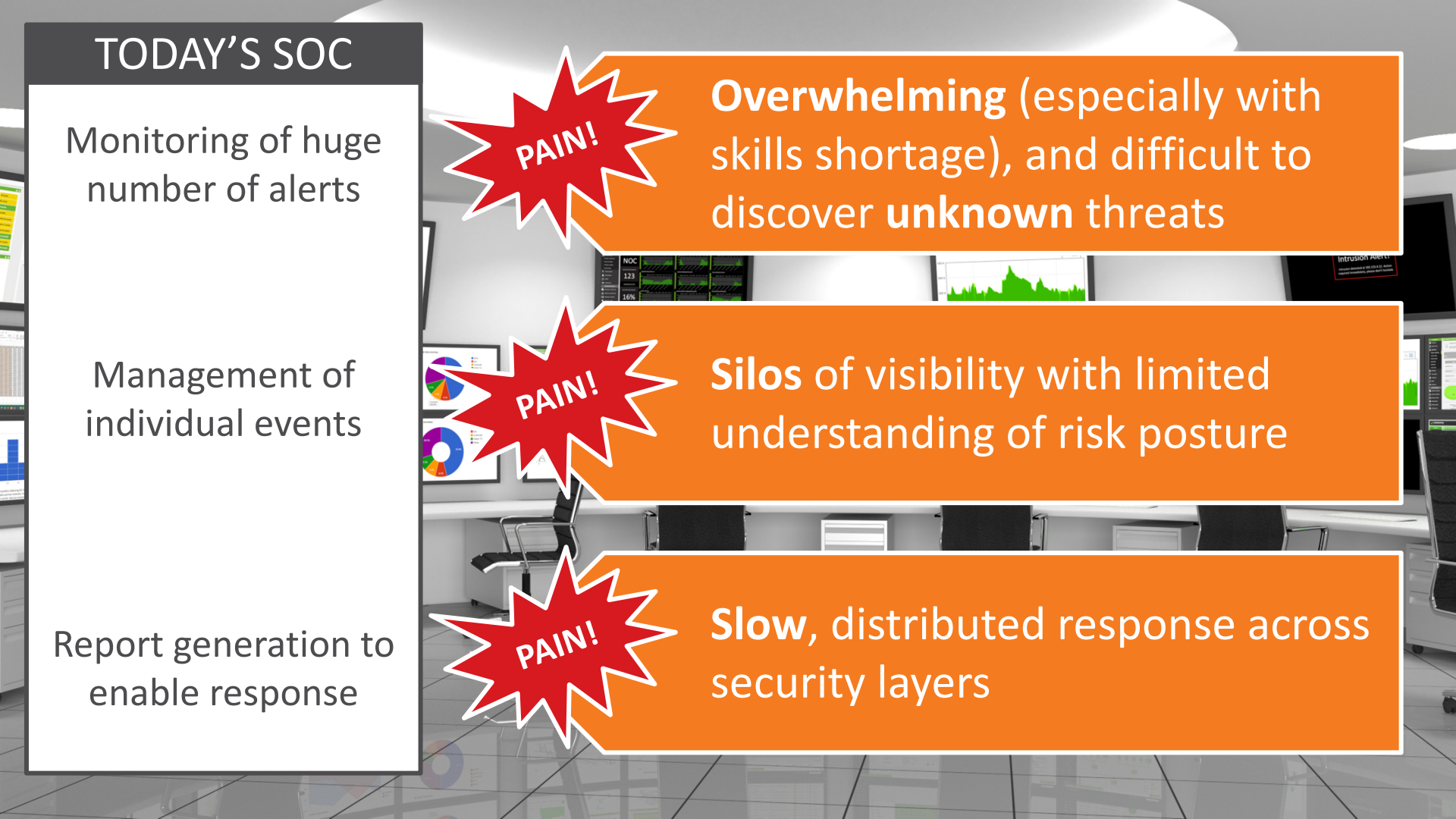


2017 Global Information Security Workforce Study "Benchmarking Workforce Capacity and Response to Cyber Risk", June, 2017

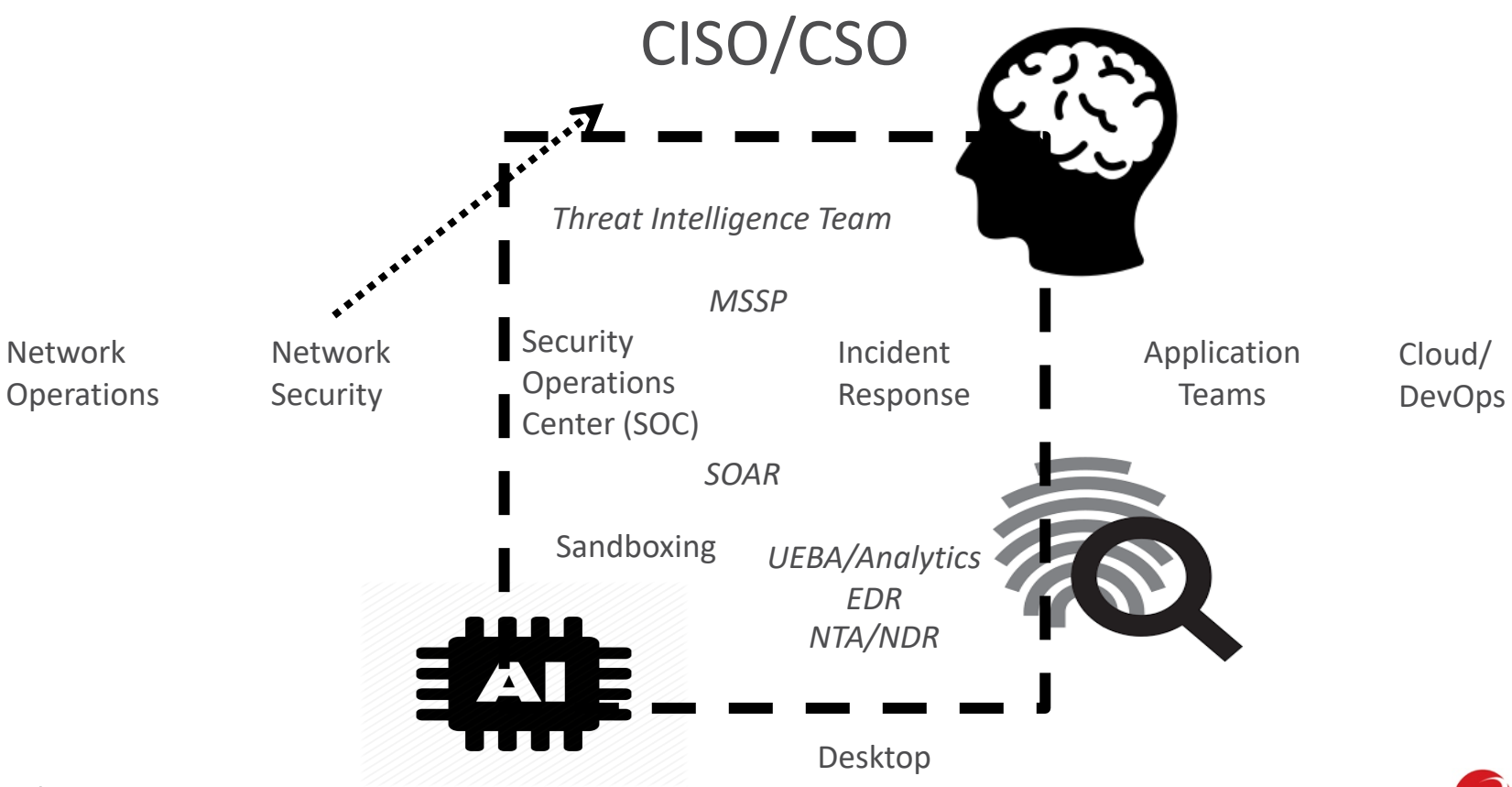
When Your Staff is Bored…….



55


TODAY'S SOC
Monitoring of huge number of alerts
Management of individual events
Report generation to enable response
PAIN!
Overwhelming (especially with skills shortage), and difficult to discover unknown threats
PAIN!
Silos of visibility with limited understanding of risk posture
PAIN!
Slow, distributed response across security layers

All of the “NEXT-GEN SOC” Technologies Promise Automation



Do I need a SOAR platform ?

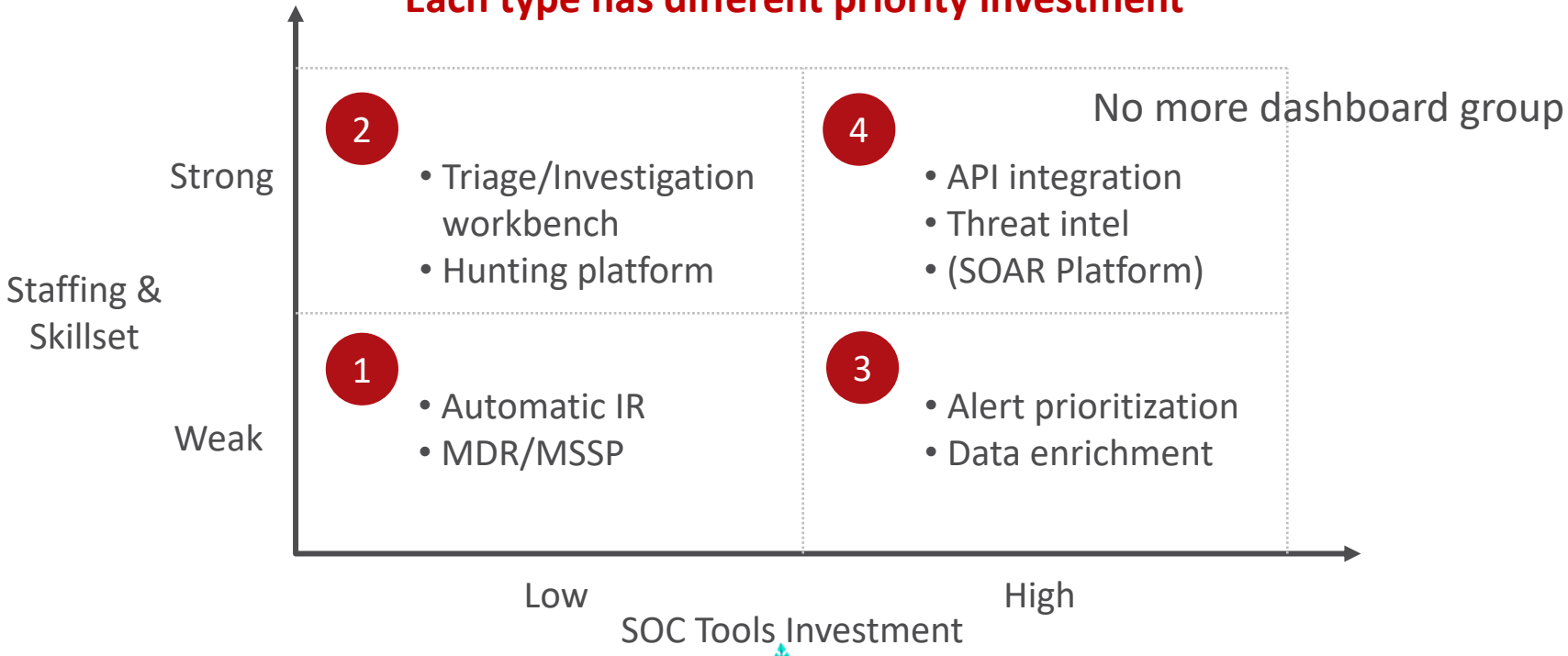
By end of 2020, 15% of organizations with > 5 people in security operations will leverage a SOAR

-- RedScan

What about the other 85 % ?
Is my goal really automation
or is it prioritization ?

SOC Maturity Level

Each type has different priority investment

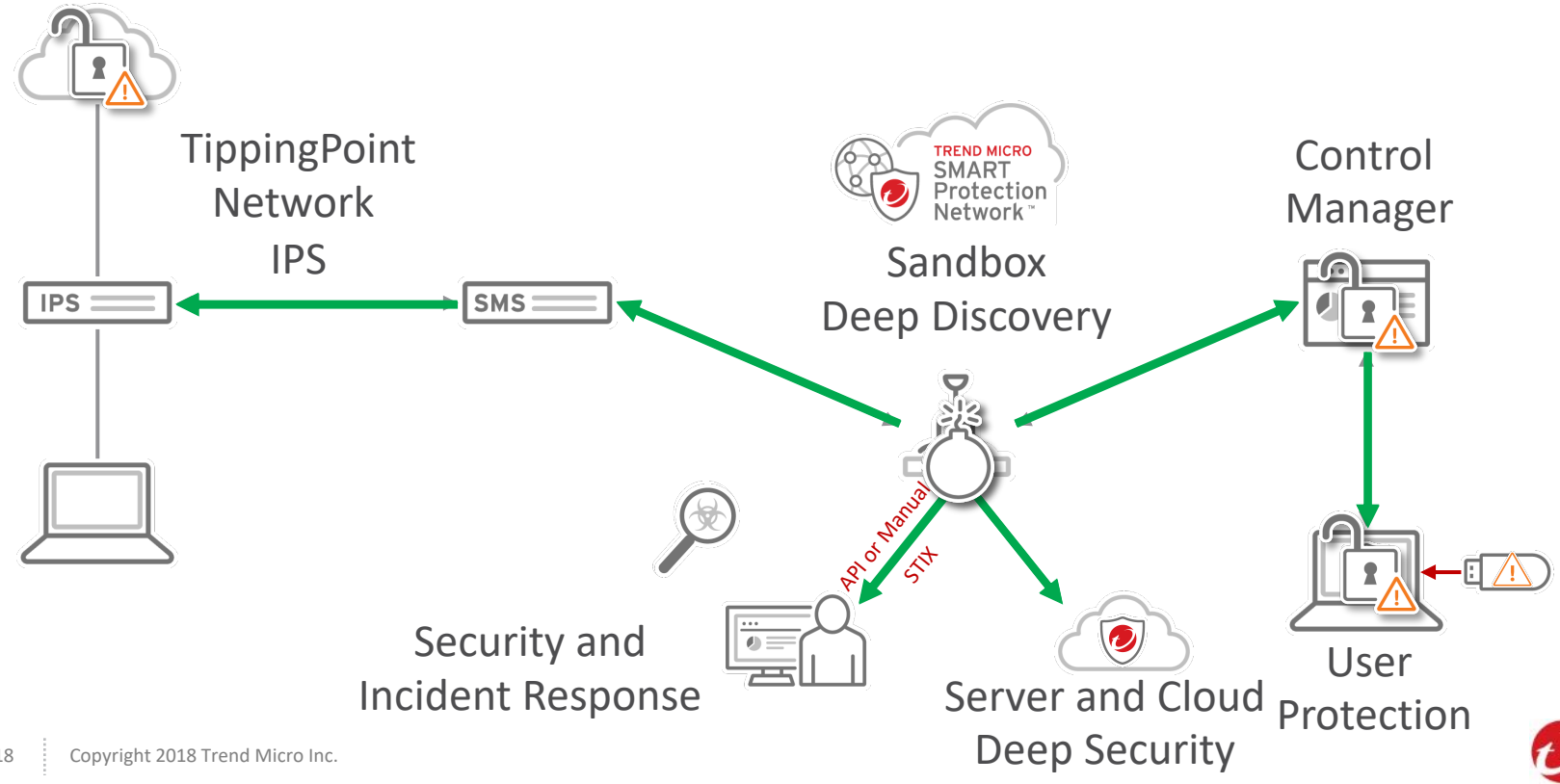


Our Approach
Automation is NOT just another product

Some recent technologies/methodologies help:

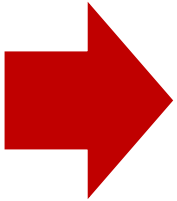
- Workflow automation across traditionally siloed product lines
- APIs and industry standards across the industry
- Job-focused AI and ML technologies (vs. horizontal AI applications)

Connected Threat Defense: Automated Faster Time to Protection



High Level Value of what we are trying to do

- Can’t find people
- Too many products
- What to prioritize
- Which events move to Prevention + Investigation and Response ?



- **Less** Events - **Less** vendors - **Less** Interfaces
- Many workflow steps **automated**
- **Enable people to focus on top priority events**

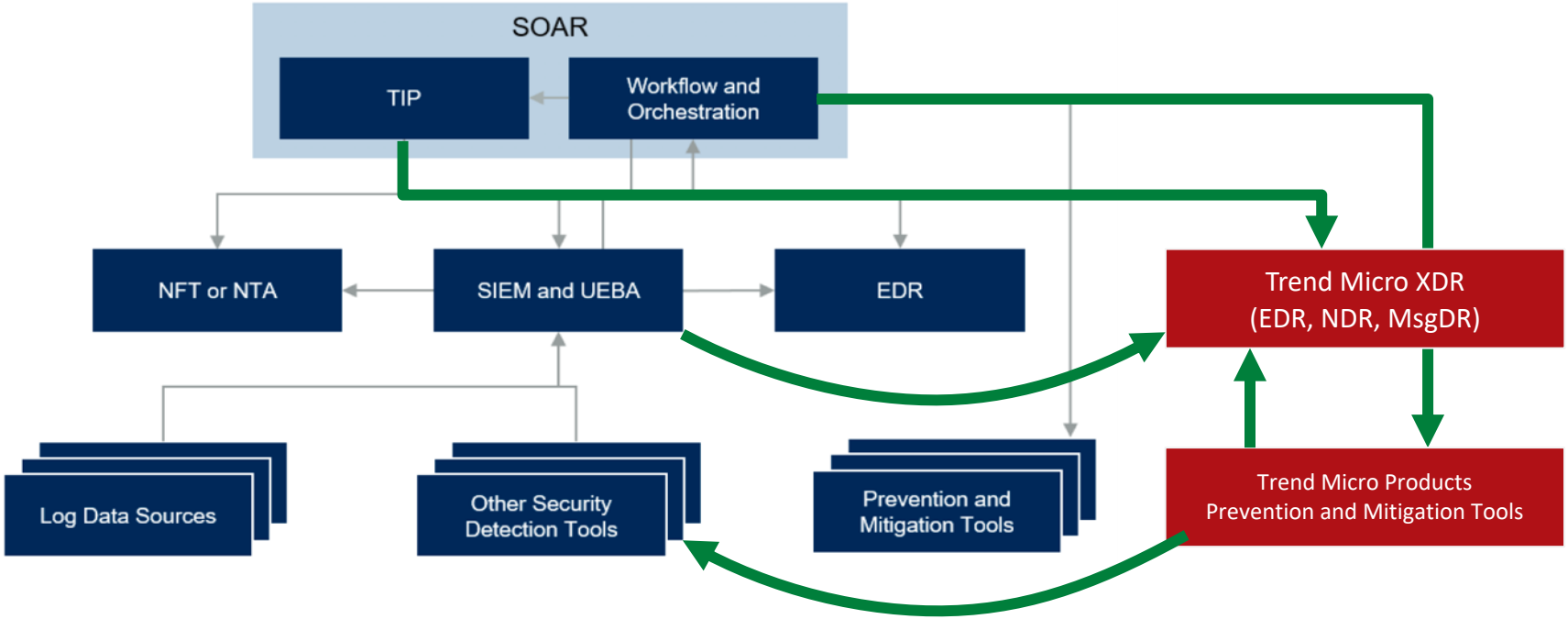
Introducing OpenSOC XDR

- Cloud-base detection and response platform for ENT/VLE customers
  with Trend Micro 3Cs solutions
  to enhance their security operation
  against cyber threats

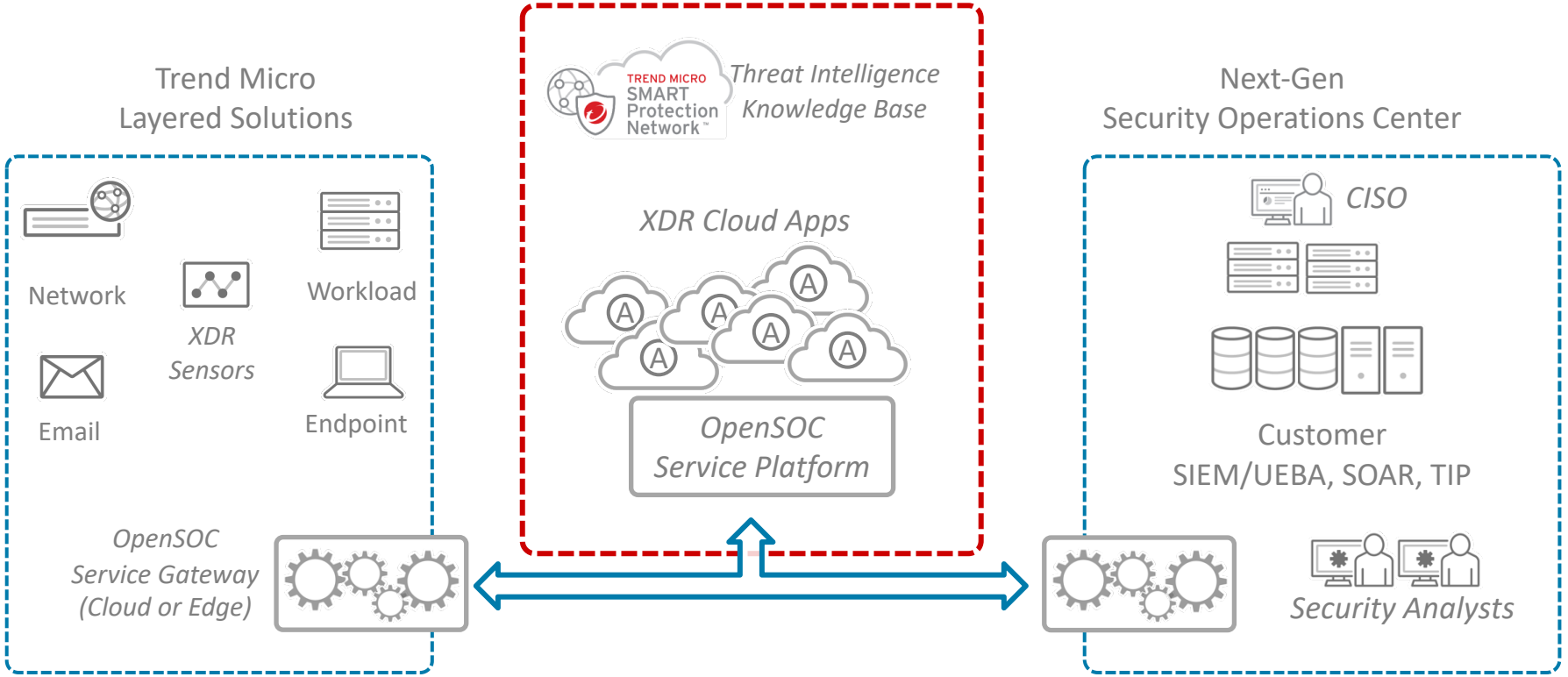
Why XDR

- EDR – narrowly focused, a view of only the endpoint
- XDR – sees everything (X: a far broader set of data)
  - Endpoint, workload, cloud, OT, network
  - Security event log data, host/network/messaging activity data
  - One single visibility into the different stages of attack path and RCA
  - Security teams find more threats faster, and then respond them faster

How OpenSOC XDR and TM Products Fits



OpenSOC XDR Overview



Top 3 Use Cases

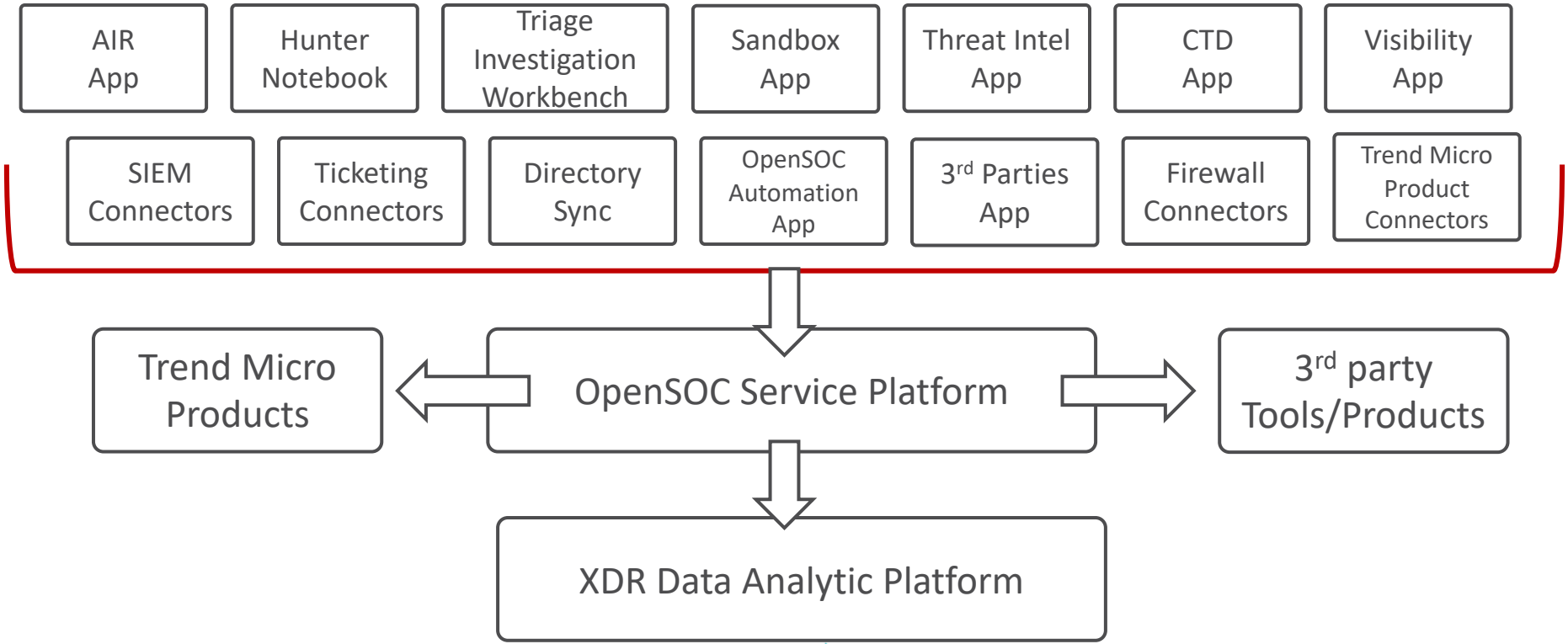
- Effective alert triggers with incident RCA
- STIX/IOC sweeping for compromised hosts
- Automatic threat mitigation

OpenSOC XDR Value Proposition

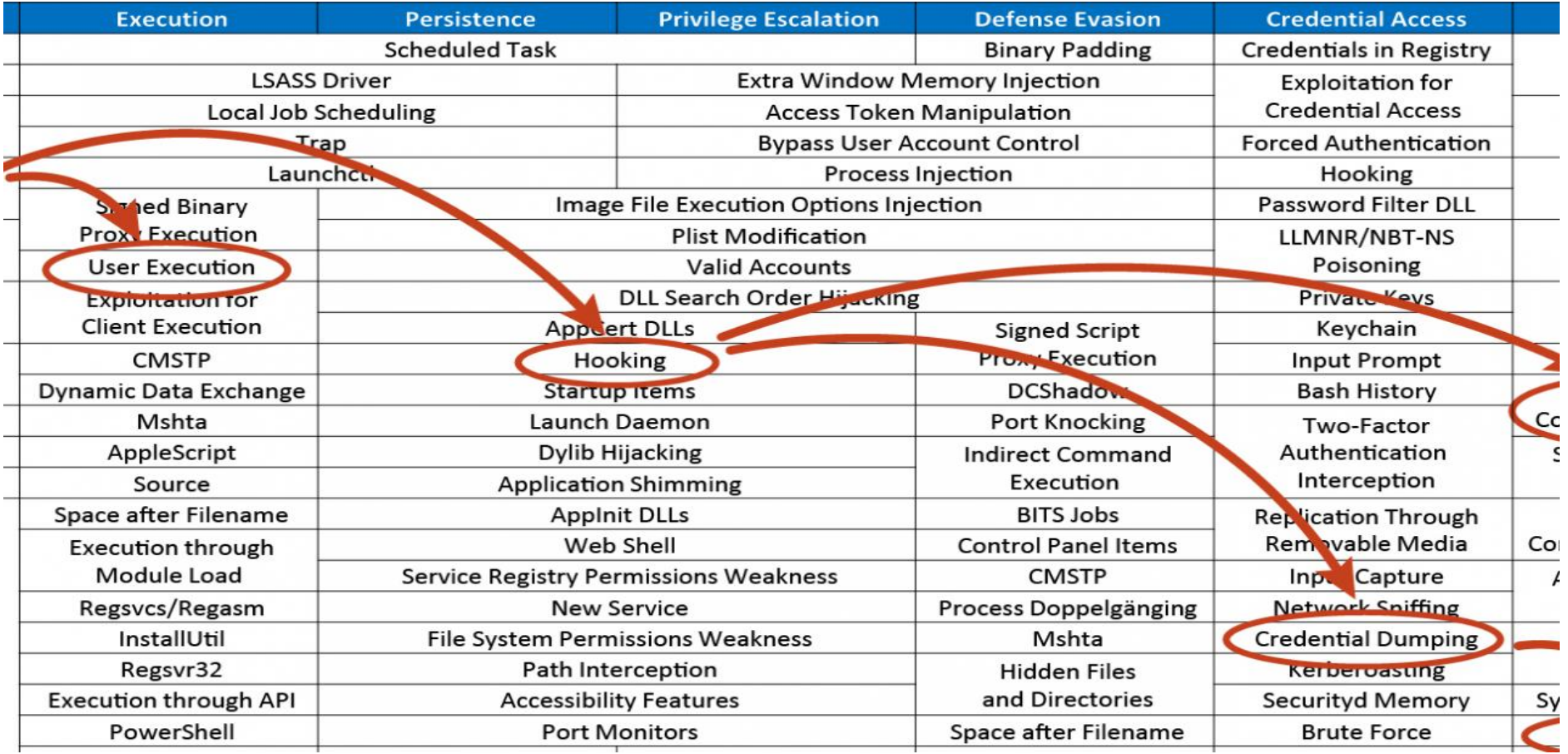
- *Reduce MTTD & MTTR to security incidents*
  - 30 years of Global threat intelligence and 15 years of threat AI/ML analytics
    - Reduce the amount of time it takes on triage to discover a potential security incident (alert prioritization)
  - Global threat expertise and vender guidance
    - Reduce the amount of time it takes on incident response to automatically and collaboratively control, remediate and/or eradicate a threat once it has been discovered (automation)

- *Fit with any security operation designs*
  - An open platform with industry standards ensures that
    - Security architects can satisfy their integration needs,
    - Operation teams can act in their best interests,
    - Partners can add value on top of it.

OpenSOC XDR App Store



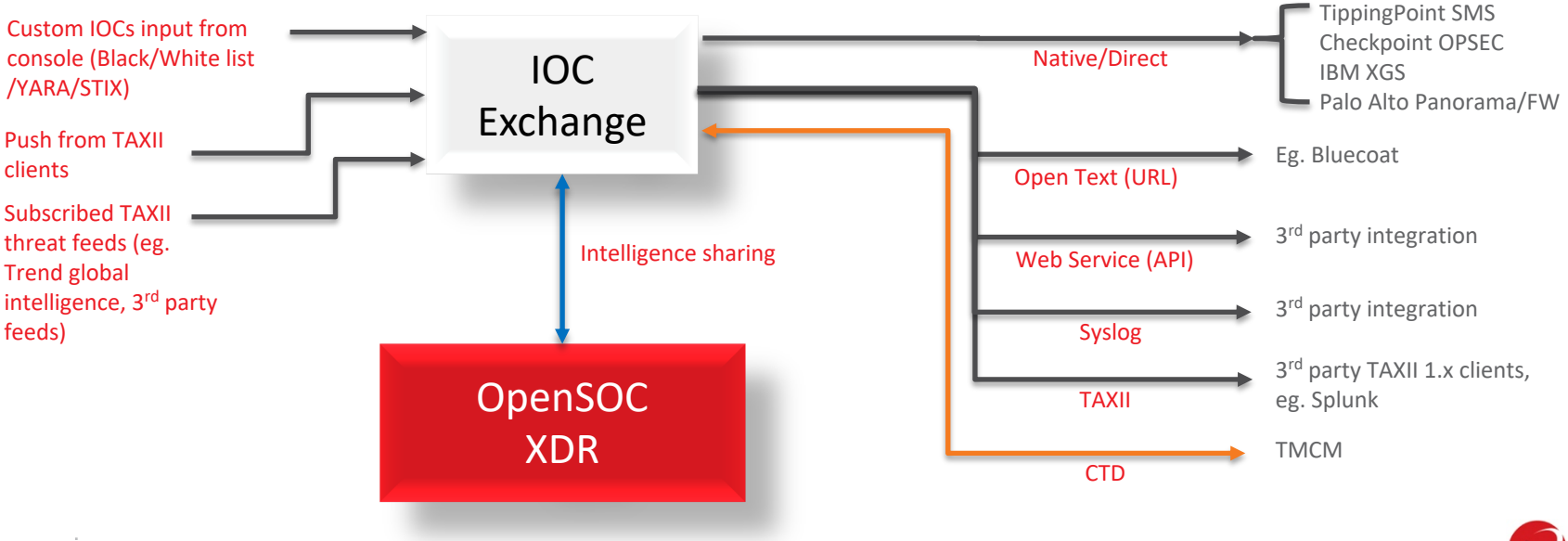
MITRE ATT&CK™ as the Common Language



Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Scheduled Task			Binary Padding	Credentials in Registry
LSASS Driver		Extra Window Memory Injection		Exploitation for Credential Access
Local Job Scheduling		Access Token Manipulation		
Trap		Bypass User Account Control		Forced Authentication
Launchctl		Process Injection		Hooking
Signed Binary Proxy Execution	Image File Execution Options Injection			Password Filter DLL
	Plist Modification			LLMNR/NBT-NS Poisoning
User Execution	Valid Accounts			
Exploitation for Client Execution	DLL Search Order Hijacking			Private Keys
	AppCert DLLs		Signed Script Proxy Execution	Keychain
CMSTP	Hooking			Input Prompt
Dynamic Data Exchange	Startup Items		DCShadow	Bash History
Mshta	Launch Daemon		Port Knocking	Two-Factor Authentication Interception
AppleScript	Dylib Hijacking		Indirect Command Execution	
Source	Application Shimming			
Space after Filename	AppInit DLLs		BITS Jobs	Replication Through Removable Media
Execution through Module Load	Web Shell		Control Panel Items	
	Service Registry Permissions Weakness		CMSTP	Input Capture
Regsvcs/Regasm	New Service		Process Doppelgänging	Network Sniffing
InstallUtil	File System Permissions Weakness		Mshta	Credential Dumping
Regsvr32	Path Interception		Hidden Files and Directories	Kerberoasting
Execution through API	Accessibility Features			Securityd Memory
PowerShell	Port Monitors		Space after Filename	Brute Force

Embracing IOC Standards – STIX and TAXII

- Standard based Advanced Threat Intelligence Sharing
  - Intelligence management, consolidation and sharing with 3rd party products by standard formats and protocols



28

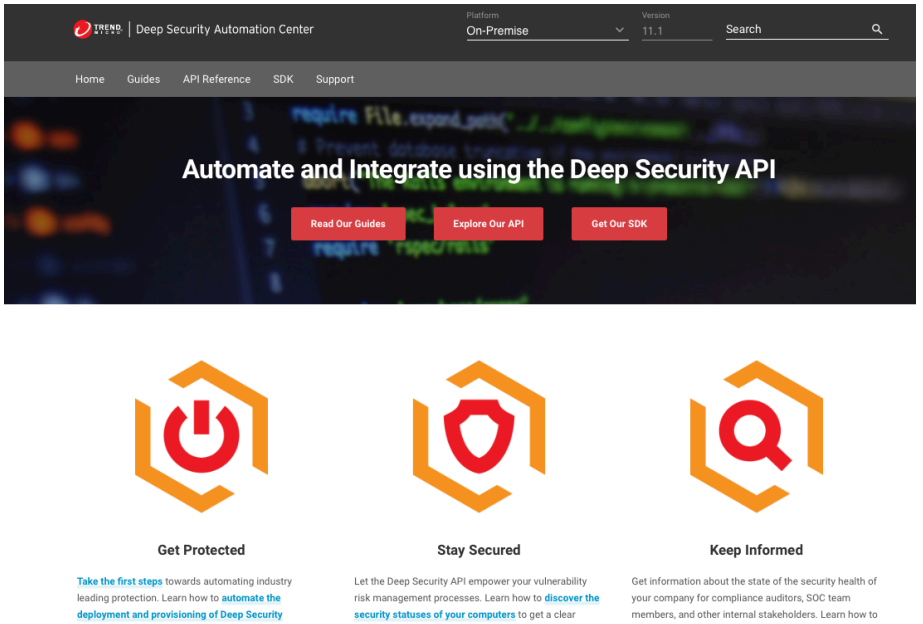
OASIS Open Command & Control

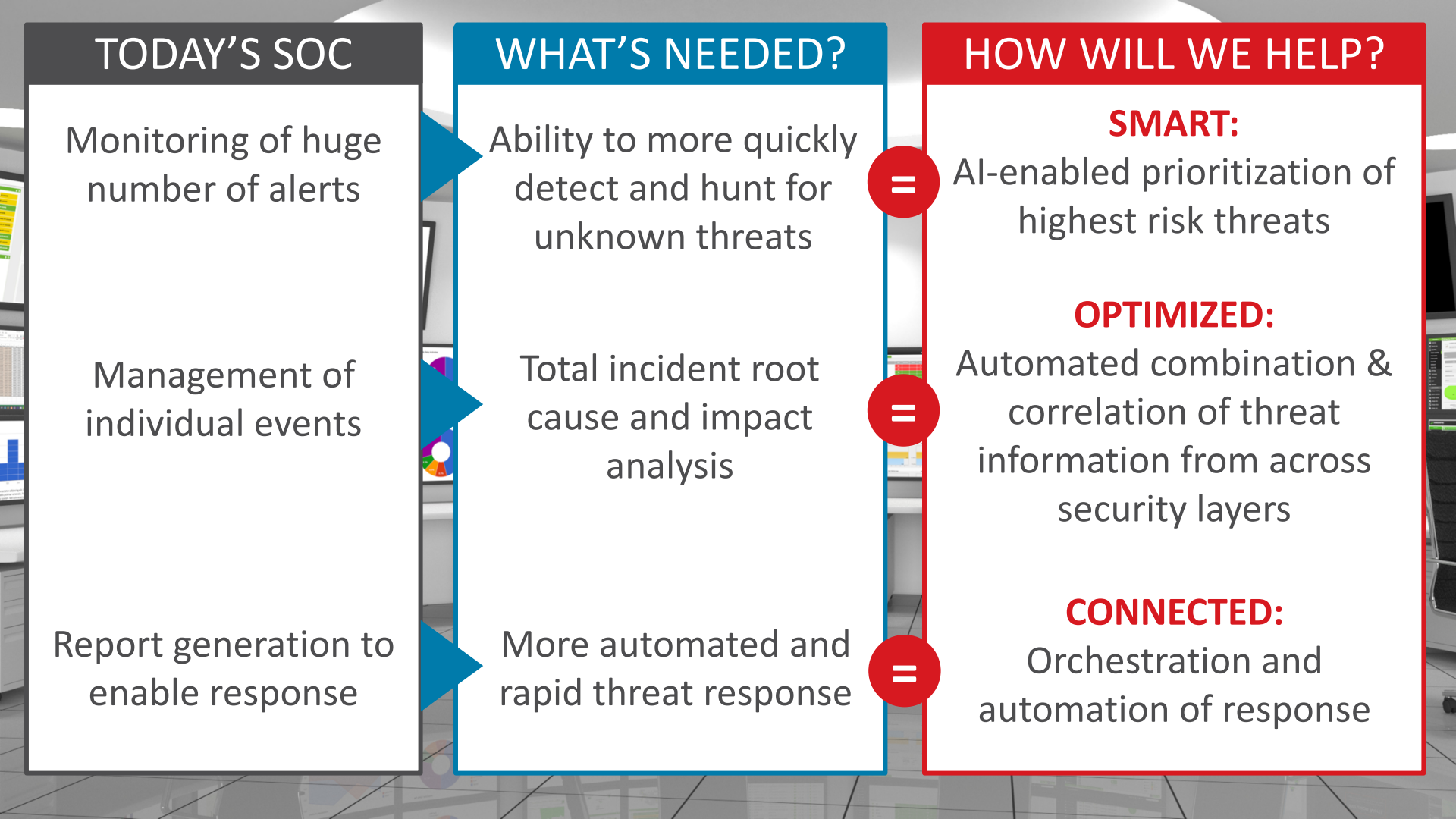
Enable machine-to-machine communications
Common language for SOC to command & control security controls

OpenSOC XDR Automation Center for Security Engineers

- Single entry for customer lookup automation use case, sample code and Product API detail usage.

Automation Center
(Sample code and API Search)




TODAY'S SOC
Monitoring of huge number of alerts
Management of individual events
Report generation to enable response
WHAT'S NEEDED?
Ability to more quickly detect and hunt for unknown threats
Total incident root cause and impact analysis
More automated and rapid threat response
HOW WILL WE HELP?
SMART:
AI-enabled prioritization of highest risk threats
OPTIMIZED:
Automated combination & correlation of threat information from across security layers
CONNECTED:
Orchestration and automation of response


TREND MICRO
THE ART OF CYBERSECURITY