Digital Convergence and ICS SOCs

Omar Sherin

GICSP/CERT-IH/CRISC/CBCP

ISA99/IEC 62443 Voting member

EY

Building a better working world

IT

- Mature security approach
- Knowledge widely available
- The information is protected (confidentiality first)

Main components

- Application servers
- Database servers
- Workstations

Vendors

Microsoft SAP ORACLE hp

This is an area where **budget is 10 times bigger** than in IT!

OT

- Newly recognized area of concern
- Specific industrial knowledge
- Different approach to security
- The process is protected (Availability first)

Main components

- Control servers
- PHD servers
- Data historians
- Alarm system servers
- HMI (Human Machine Interface)
- Engineering workstations
- RTU (Remote Terminal Unit) stations
- PLC (Programmable Logic Controllers)

Vendors

ABB Yokogawa Schneider Electric Rockwell Automation SIEMENS Honeywell YOKOGAWA ALLEN-BRADLEY

The **process control** systems operate between the business systems requirements for real time access to data about production processes forced Control Systems to interconnect with business networks and other external systems, which generated **major security issues.**

Global OT/IoT Advisory Services Center

EY

GISS 2016 global key findings – Energy Sector

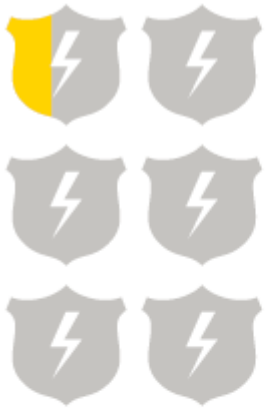
70%

of the most commonly used IoT devices contain vulnerabilities.

HP study reveals 70% of Internet of Things devices vulnerable to attack. (n.d.). Retrieved from http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VHMpw4uUfVc

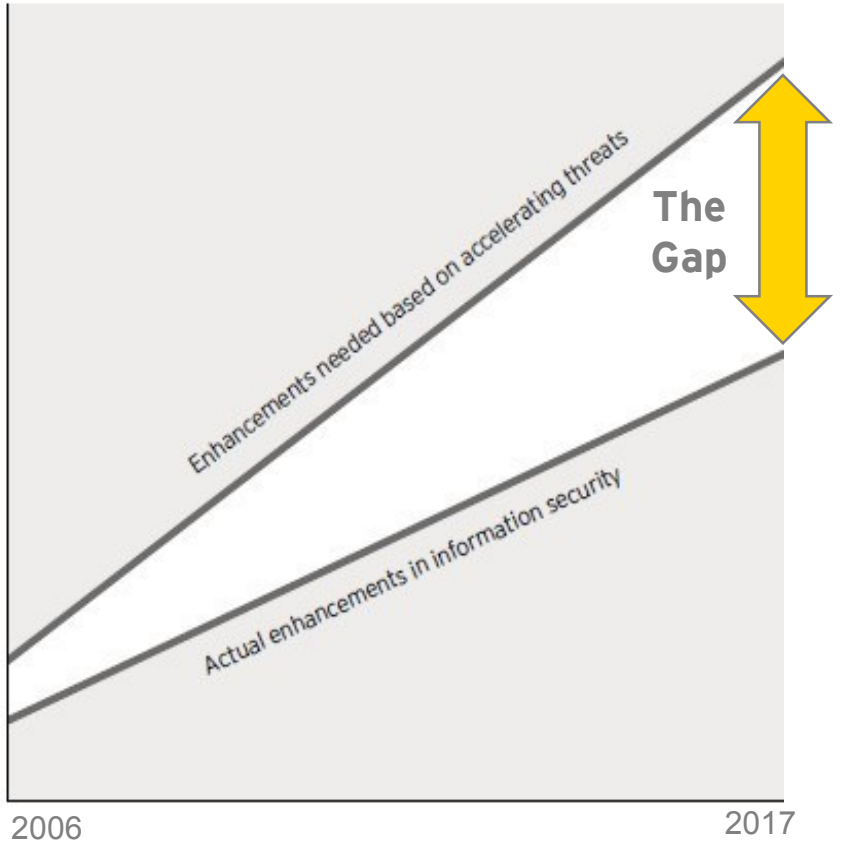
56%

of respondents say that it is "unlikely or highly unlikely" that their organization would be able to detect a sophisticated attack.**

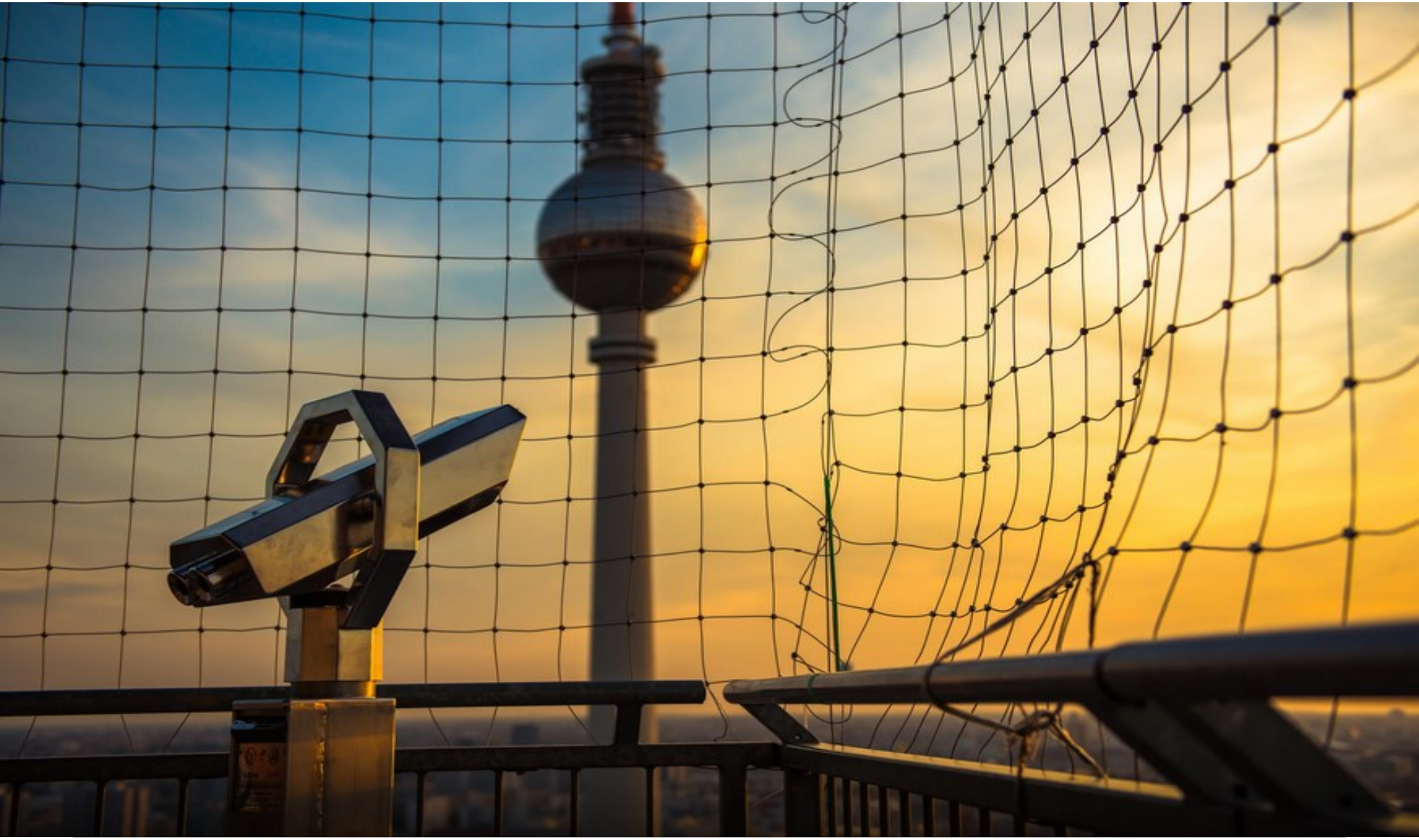


6%

of organizations claim to have a robust incident response program that includes third parties and law enforcement and is integrated with their broader threat and vulnerabilit management function.**



70% of incidents are detected by a third party



You can not detect what you can not see

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials			Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration
Accessibility Features		Binary Padding	Credentials in Files	File system enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data compressed
AddMonitor		DLL Side-Loading	Network Sniffing	Group permission enumeration	Logon scripts	PowerShell	Custom application layer protocol	Data encrypted
DLL Search Order Hijack		Disabling Security Tools	User Interaction	Local network connection enumeration	Pass the hash	Process Hollowing	Custom encryption cipher	Data size limits
Edit Default File Handlers		File System Logical Offsets		Local networking enumeration	Pass the ticket	Registry	Data obfuscation	Data staged
New Service		Process Hollowing		Operating system enumeration	Peer connections	Rundll32	Fallback channels	Exfil over C2 channel
Path Interception		Indicator blocking on host		Owner/User enumeration	Remote Desktop Protocol	Scheduled Task	Multiband comm	Exfil over alternate channel to C2 network
Scheduled Task		Indicator removal from tools		Process enumeration	Windows management instrumentation	Service Manipulation	Multilayer encryption	Exfil over other network medium
Service File Permission Weakness		Indicator removal from host		Security software enumeration	Windows remote management	Third Party Software	Peer connections	Exfil over physical medium
Shortcut Modification		Masquerad-ing		Service enumeration	Remote Services		Standard app layer protocol	From local system
BIOS	Bypass UAC	NTFS Extended Attributes		Window enumeration	Replication through removable media		Standard non-app layer protocol	From network resource
Hypervisor Rootkit	DLL Injection	Obfuscated Payload			Shared webroot		Standard encryption cipher	From removable media
Logon Scripts	Exploitation of Vulnerability	Rootkit			Taint shared content		Uncommonly used port	Scheduled transfer
Master Boot Record		Rundll32			Windows admin shares			
Mod. Exist'g Service		Scripting						
Registry Run Keys		Software Packing						
Serv. Reg. Perm. Weakness								
Windows Mgmt Instr. Event Subsc.								
Winlogon Helper DLL								

Approved for Public Release; Distribution Unlimited. Case Number 15-1288

MITRE

Attack Matrix [control, execute, and maintain]

EY

Security Visibility Approaches in MENA

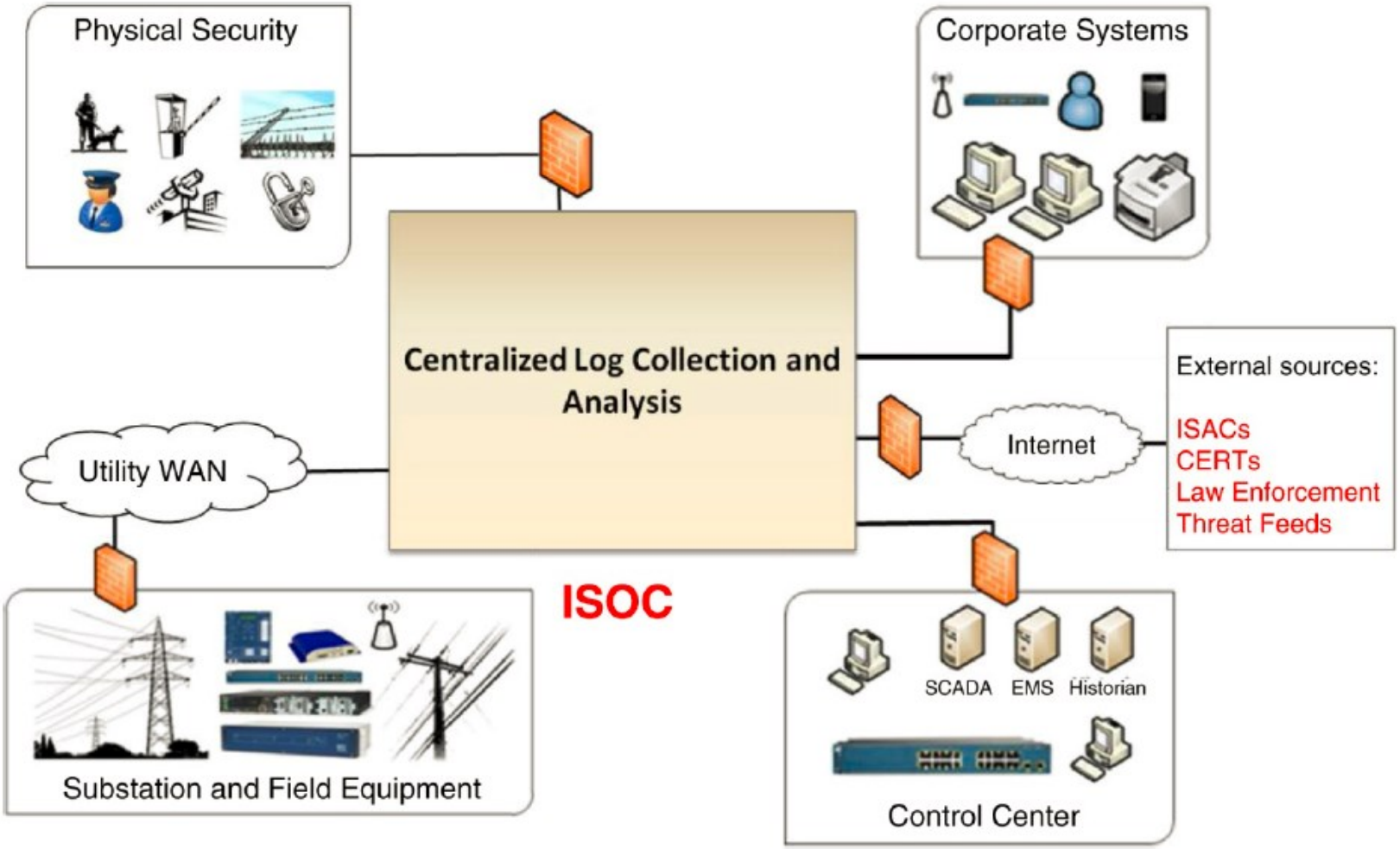
Taking Security Operation Centers (SOCs) as an Example

MENA Organizations opt for:

1. **Integrated SOCs (ISOC) (covering IT/OT/Physical Security)**
2. **Separate SOCs**
3. **Managed SOCs**

Integrated SOCs
A- Full Integration

Architecture Models (Fully Integrated)



Pros vs Cons

Pros:

- ✓ Provides real-time situational awareness across the entire enterprise
- ✓ Easier detection of cross-business unit incidents
- ✓ Develops internal capabilities for true Corporate wide IH
- ✓ Supports an intelligence-driven approach to incident detection
- ✓ Unified view on IH and Patch management..etc

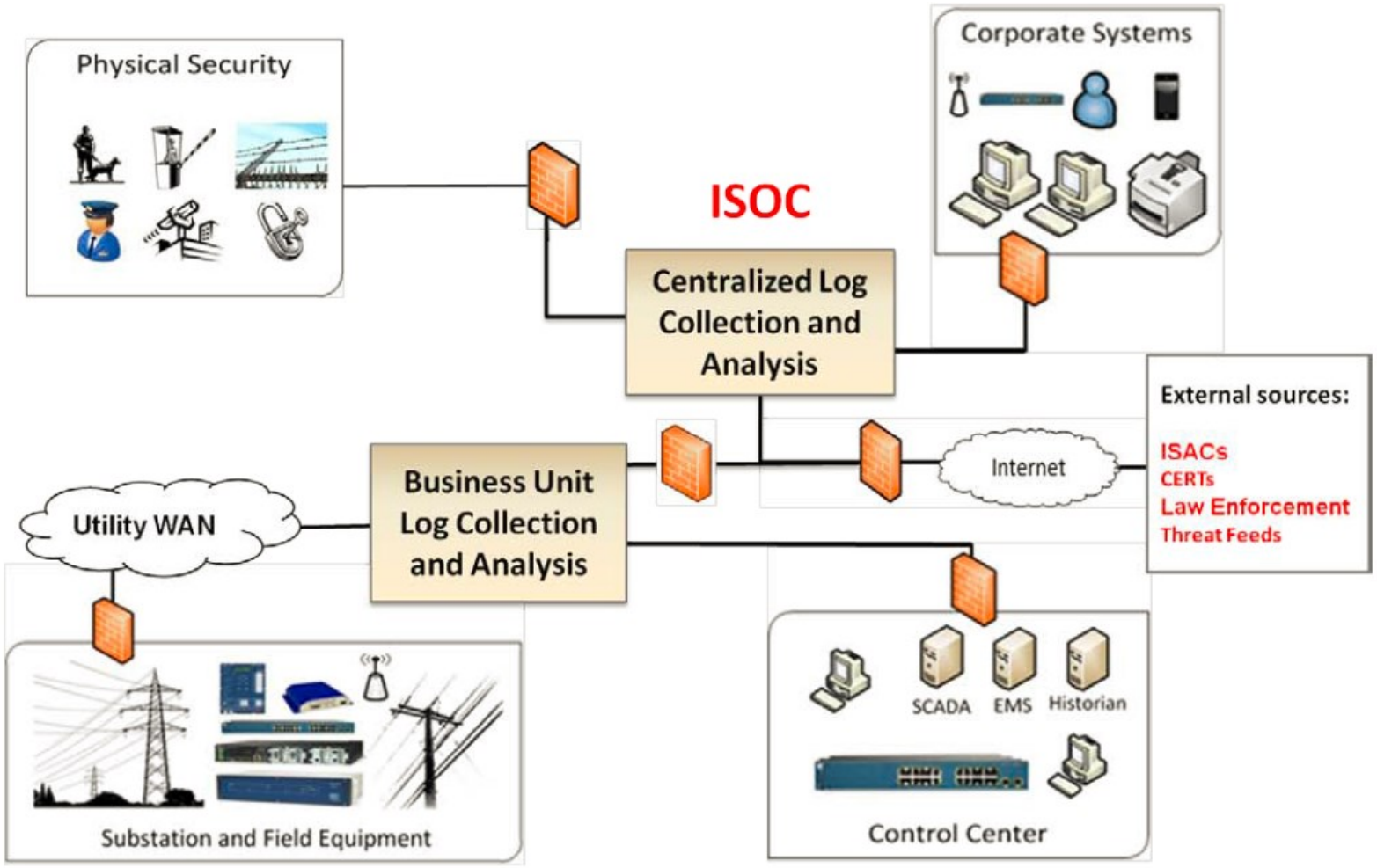
Cons:

- ○ Requires staff to be experts in multiple business units (corporate IT and OT domains)
- ○ Requires staff to be well trained to provide incident response capabilities and forensics support to different business units.
- ○ Corporate Politics and culture can be a challenge

People

Integrated SOCs
B- Distributed Integration

Architecture Models (Distributed Model)



Pros vs Cons

Pros:

- ✓ Reduces likelihood of false positives for ISOC since only critical alarms are brought to their attention
- ✓ Less corporate politics
- ✓ No need for 1 team knows all (Easier to get)

Cons:

- ○ ISOC does not have a real-time view across the enterprise, making it difficult to correlate events and alarms that may appear non-critical
- ○ Staff must develop detailed policies and procedures for each business unit to identify critical alarms that should be brought to the ISOC's attention. (Hand-over)

Process

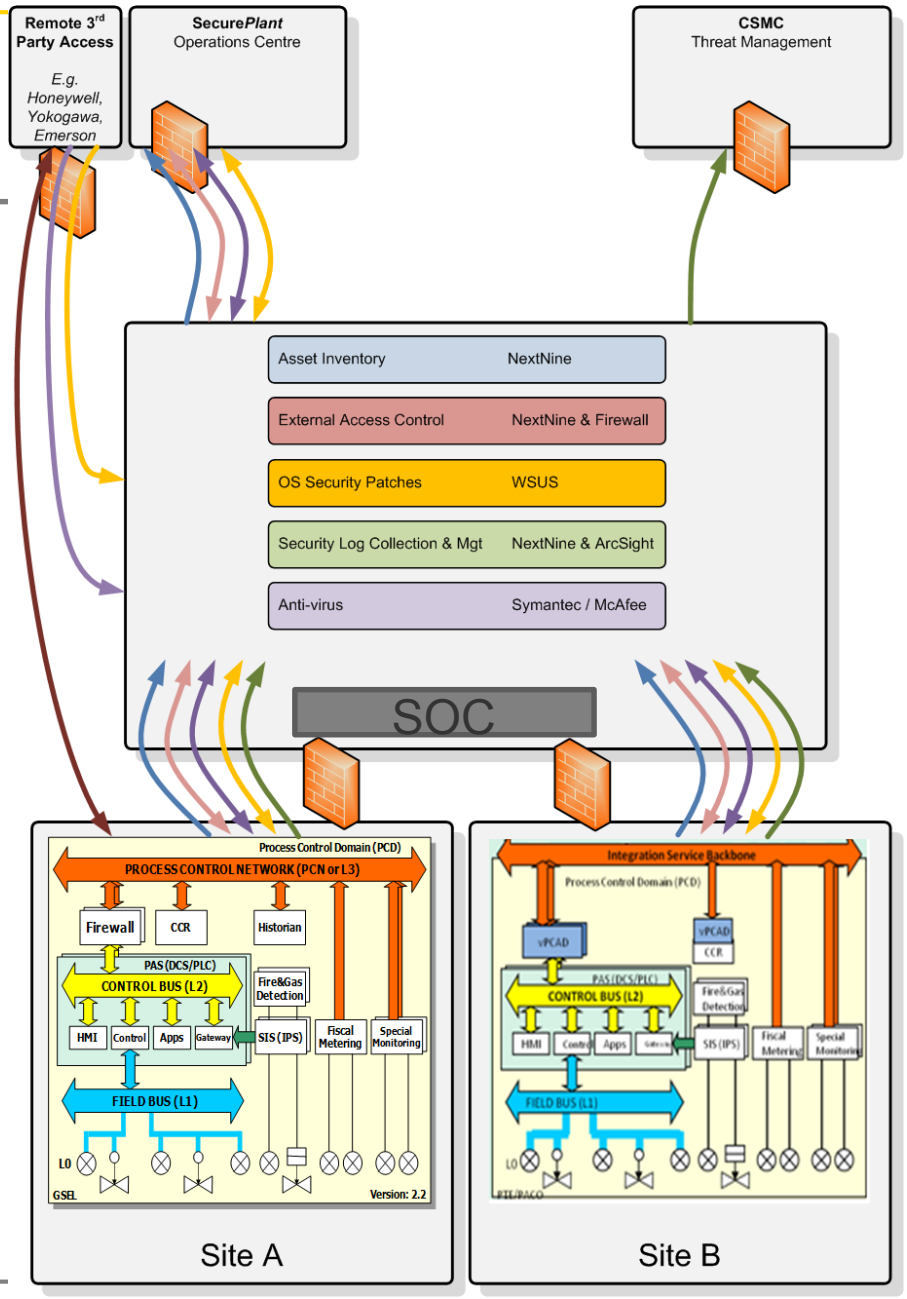
2x CapEx

Separate ICS SOC

OT SOC Services

- Automated Maturity & Compliance Reporting
- Asset Inventory & Configuration Management
- Standardised External Access Control
- Patch Management
- Anti-Virus Management
- Log Collection

Treating the IT as an untrusted 3rd party



Pros vs Cons

Pros:

- ✓ Solves the corporate politics
- ✓ Comfort zone for your technical staff (IT/OT)
- ✓ Least false positives

Cons:

- ○ Much Bigger Investment
- ○ No corporate wide visibility
- ○ Different security levels

Various SOC Deployment models analysis

Service Maturity Level: High Medium Low

Service attributes	100% In-house	Traditional MSSP/Outsource	SOC/CSIRT Staff Augmentation	EY Managed OT SOC	EY Build On-Premise (IT and OT)	Managed EY Digital SOC (IT, OT and IoT)
Speed to effectiveness	**Years**	**N/A**	**Months to year**	**Months**	**Months (EY build & handover)**	**Months**
People						
Service team	On-premise	100% remote	On-premise and remote team	On-premise and remote team (International)	Build and handover	On premise and remote team (based in GCC)
Resource competency	Material gaps	High	High	High	Skill gaps (OT)	High
Service availability	Business hours only	24/7/365 "eyes on glass"	24/7/365 = "on call" for "critical" alerts	24/7/365 "eyes on glass"	Business hours	24x7
Incident response	Material skill gaps	Often not included	Optional	Included	Included	Included
Process					**With EY Input**	
Process effectiveness	Low	High	High	High	High (EY IP)	High
Team integration	Material gaps exist	Low	High	High	Medium	High
Business context	High	Low	High	High	High	Strategic
Reports/metrics	Minimal to none or operational focus	Provider SLA focused	Material gaps	Strategic and operational insight	Medium (EY IP)	SLA ensured
Advanced threat	Commodity malware focus	Commodity malware OR APT focused	Commodity malware focused	Cover threat/attack spectrum	Commodity/APT (EY IP)	APT/Covert and bigger attack spectrum
Technology					**IT/ OT convergence**	
Network visibility	Perimeter, traditional IDS	Perimeter, traditional IDS	Perimeter, traditional IDS	Perimeter and internal, content/session inspection	Internal, perimeter & OT EY Architecture)	Internal, perimeter, OT & IoT
Endpoint/server visibility	Minimal to no capability	Often not included	Minimal to no capability	"Always on" monitoring & "on demand" host analysis	High (EY Architecture)	High
Data loss detection	Minimal to no capability	Often not included	Minimal to no capability	Client data exfiltration detection	Optional (not focus for OT)	Optional (not focus for OT / IoT)
Log management/search	Poorly tuned SIEM	"Black box" SIEM	Poorly tuned SIEM	Well tuned SIEM + analytics/efficient search	High	High
Speed to deployment	Months to years	Weeks	Months to years	Weeks to months	Months	Months
Capital investment	High	Low	High	Low to moderate (Hardware)	High (Opex and Capex)	Moderate (Capex)
Your access to *your* data	High	Minimal to no access (portal only)	High	High	High	High

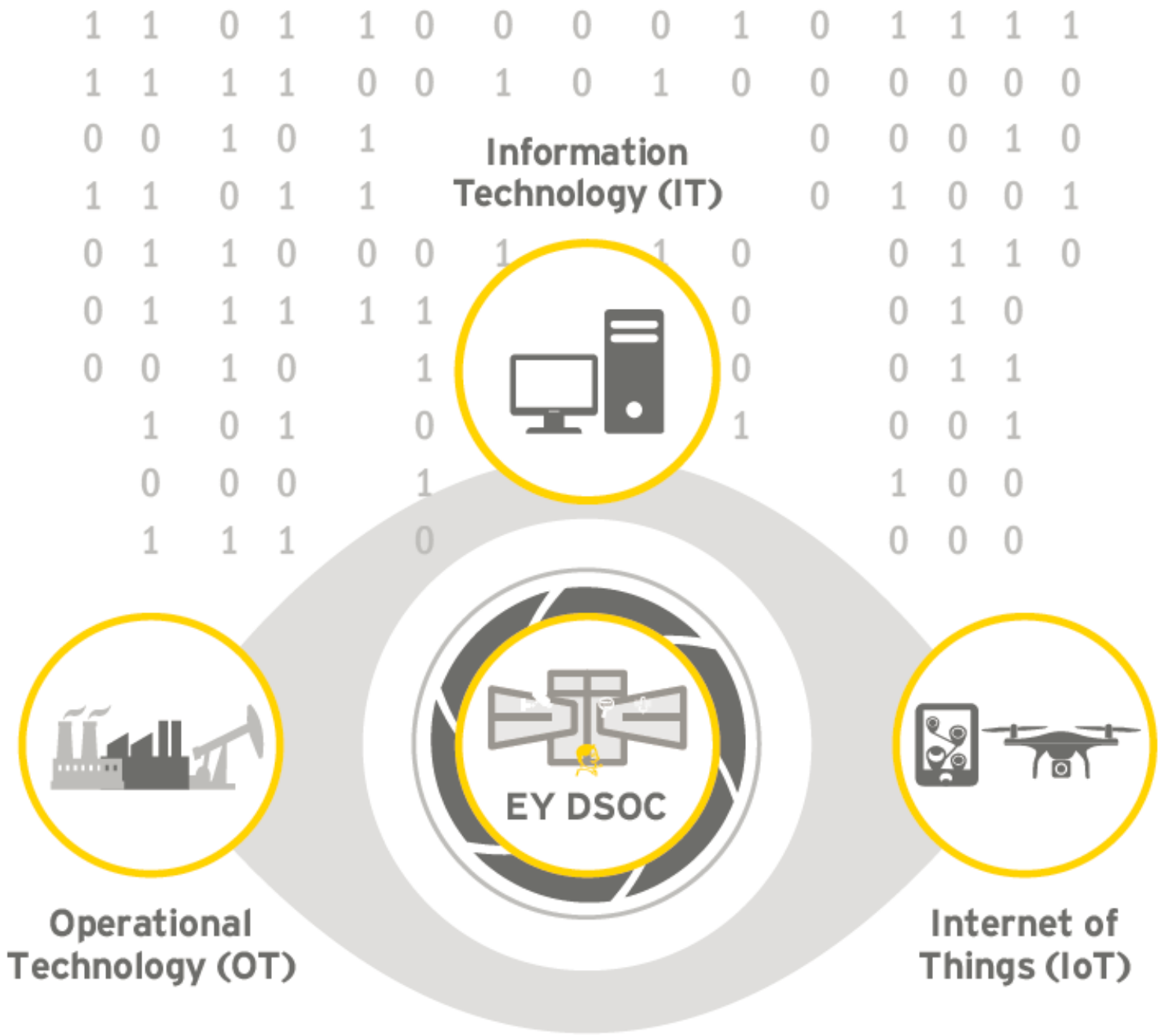
IT: Information Technology

OT: Operational Technology / Industrial Control Systems

IoT: Internet of Things

CSIRT: Computer Security Incident Response Team

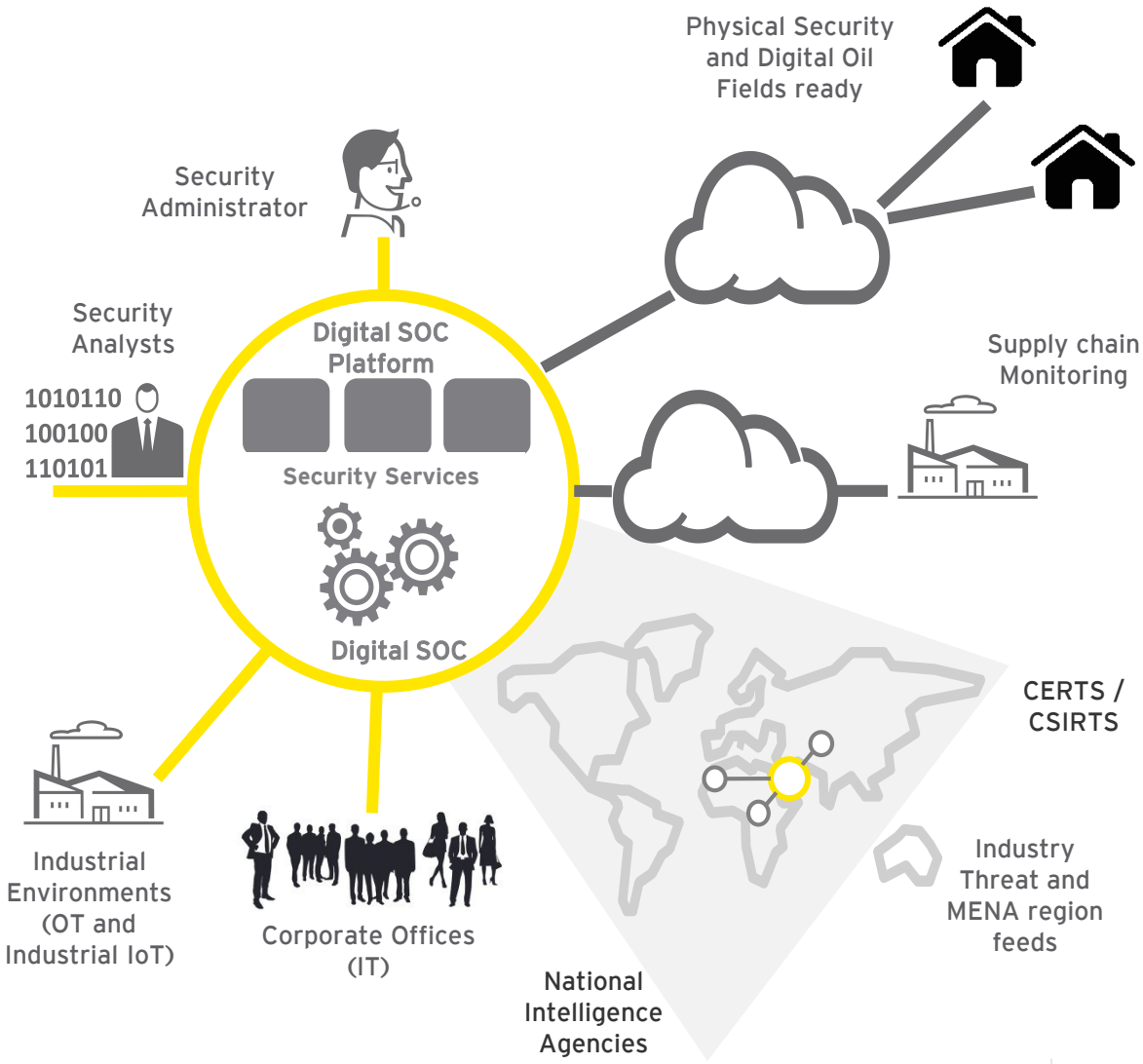
SIEM: Security Incidents & Events Monitoring


Information Technology (IT)
EY DSOC
Operational Technology (OT)
Internet of Things (IoT)

The D-SOC Approach

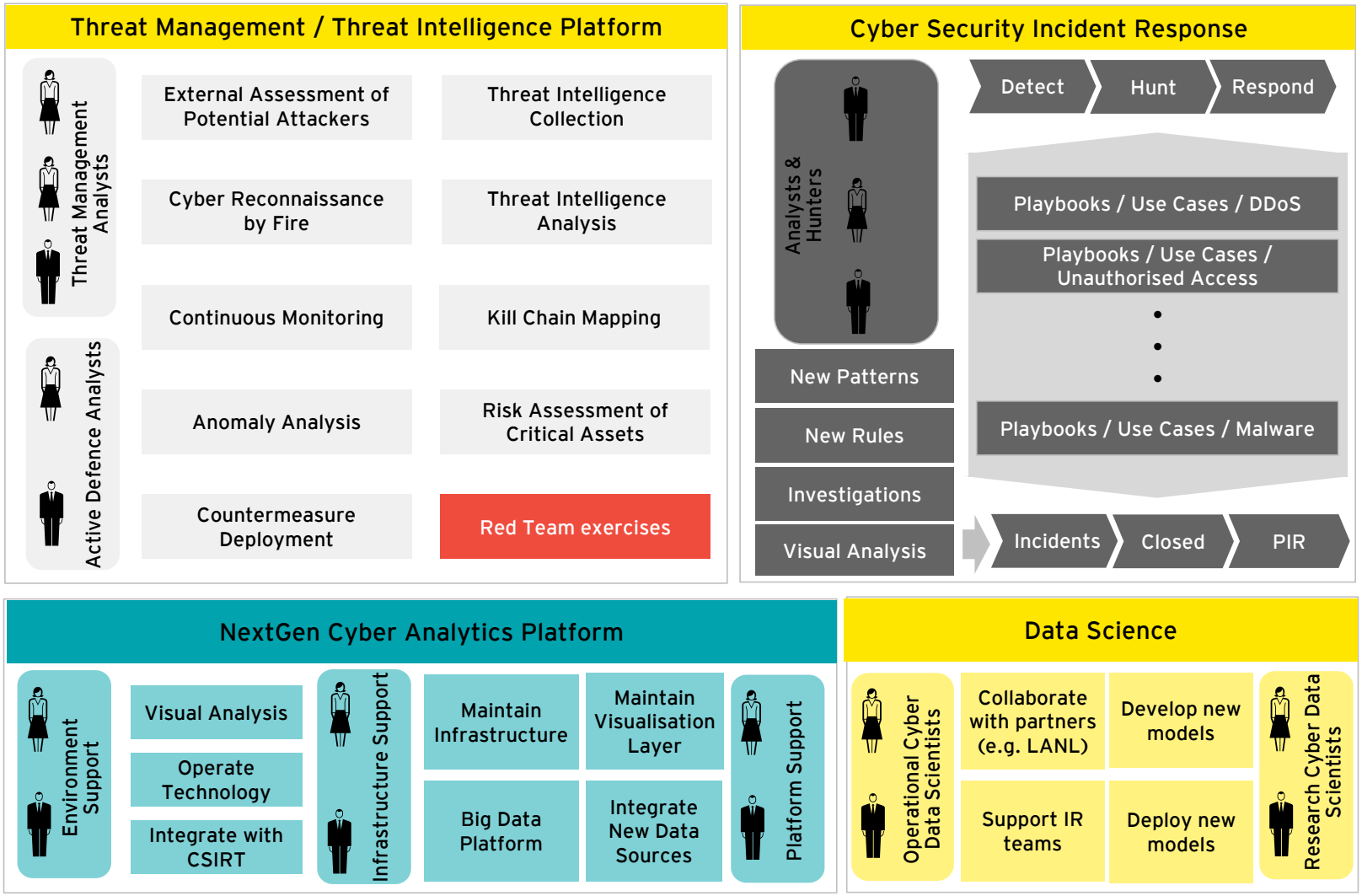
Digital SOCs will enhance the capabilities and value propositions beyond traditional SOCs.

Digital SOCs will provide an end to end threat visibility and awareness, this is essential for today's and tomorrow's hyper connected world.



Next Generation Security Operations

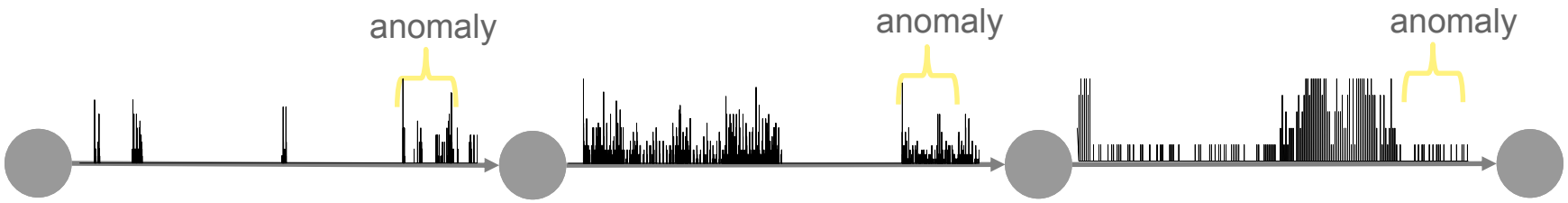
Next Generation security operations operating model



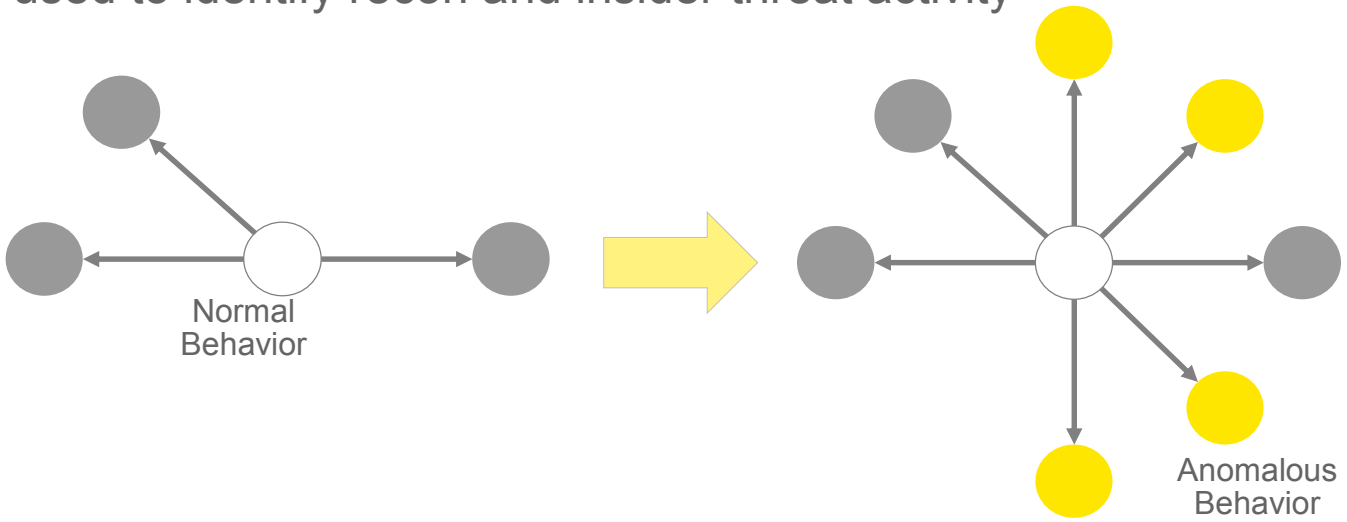
PathScan: A behavioral approach

Identify shapes of anomalous activity in the network in near real time

Paths are used to identify anomalous traversal activity

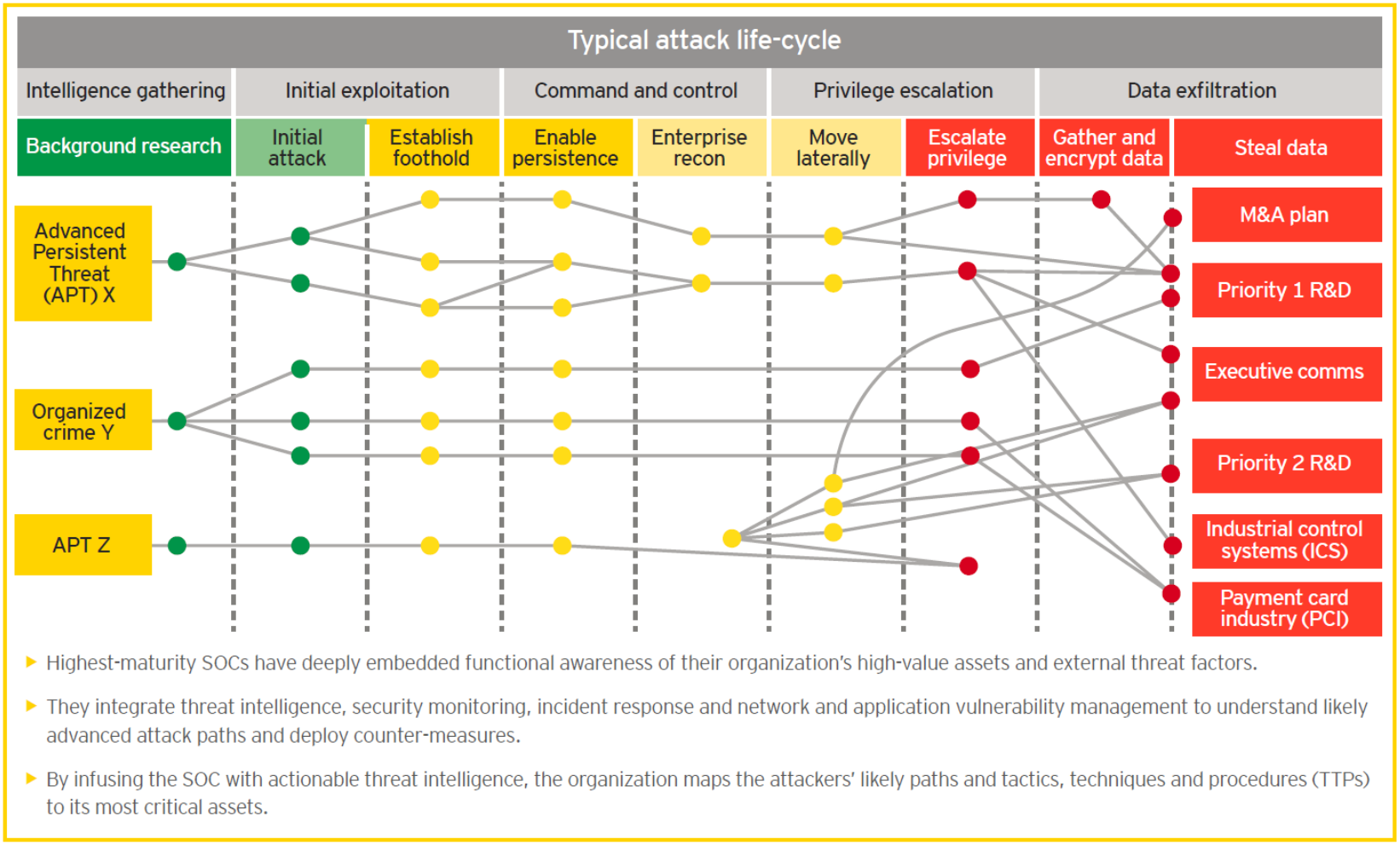


Stars are used to identify recon and insider threat activity



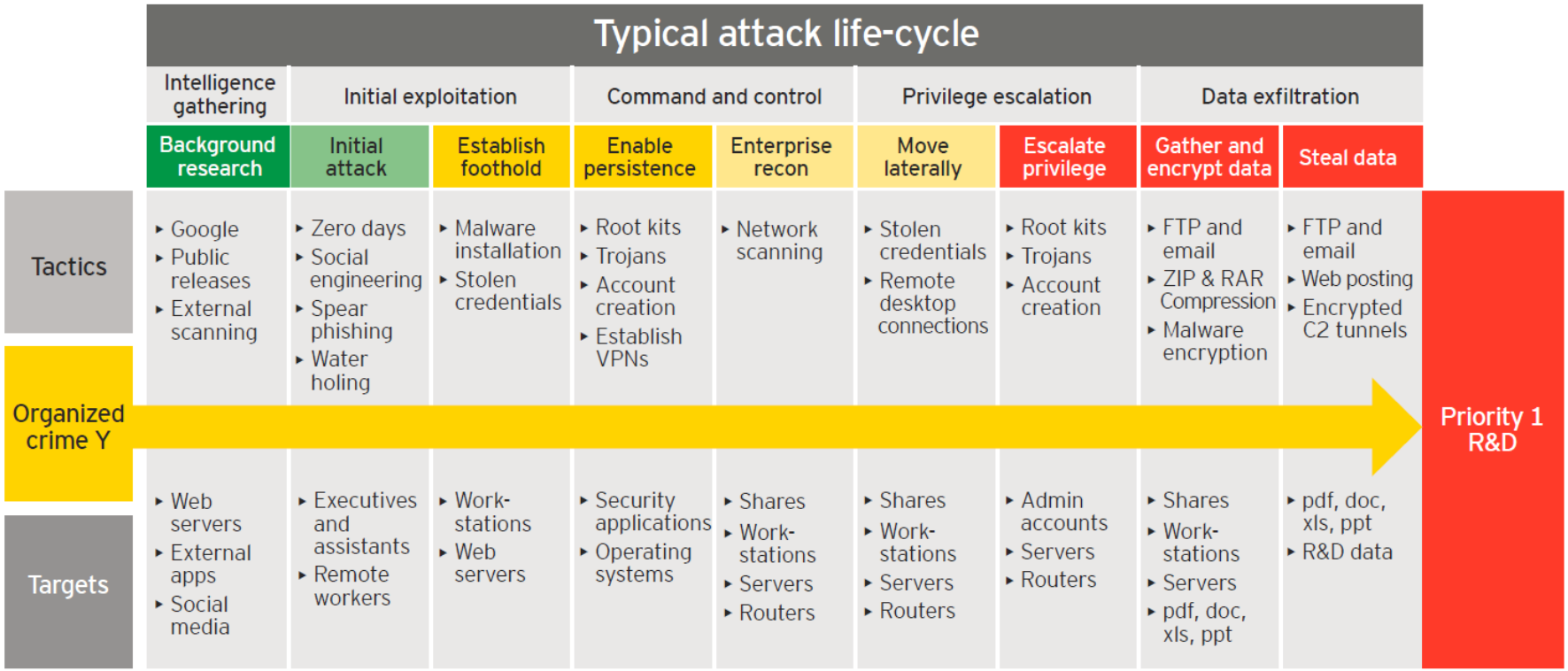
EY

Example: Attack Kill Chain



- Highest-maturity SOCs have deeply embedded functional awareness of their organization's high-value assets and external threat factors.
- They integrate threat intelligence, security monitoring, incident response and network and application vulnerability management to understand likely advanced attack paths and deploy counter-measures.
- By infusing the SOC with actionable threat intelligence, the organization maps the attackers' likely paths and tactics, techniques and procedures (TTPs) to its most critical assets.

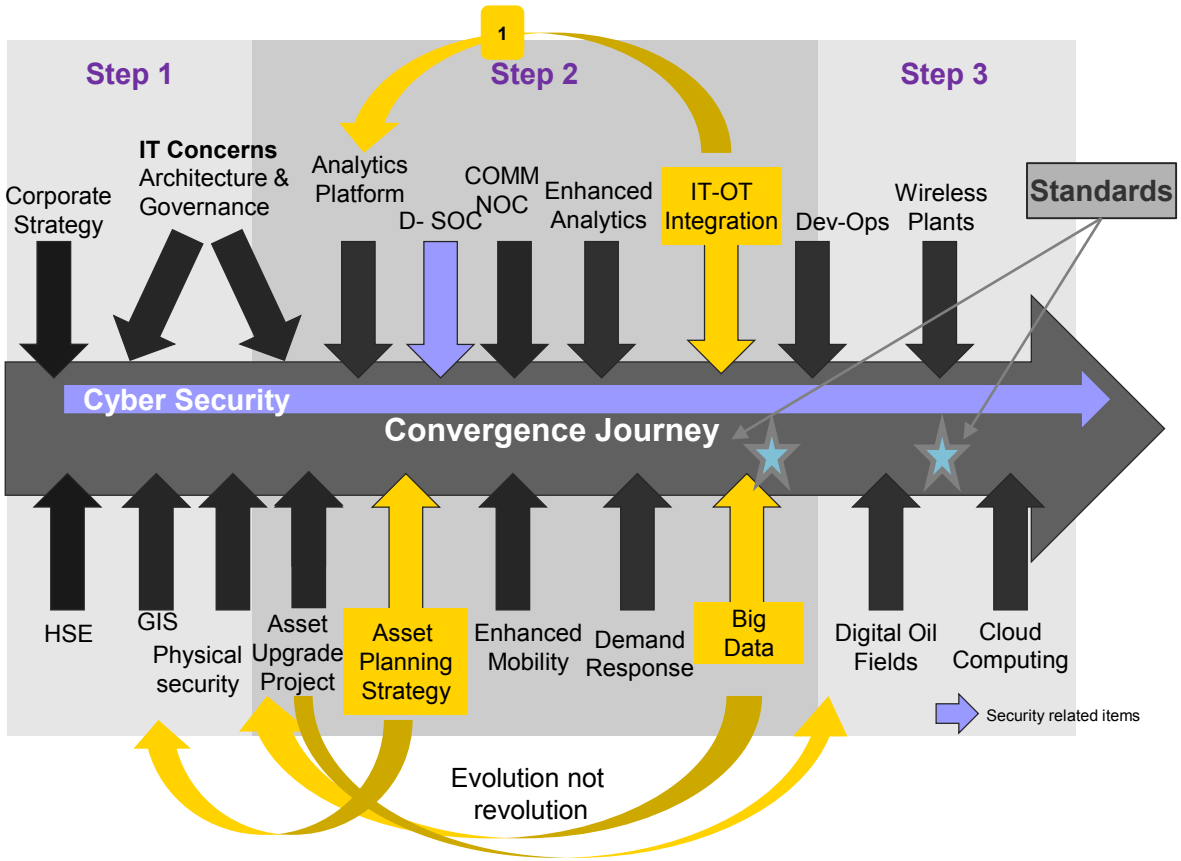
Example: Attack Kill Chain – Attacker Profiling



it's a journey

Convergence Road Map

Charting the path forward



Taking the proper steps towards achieving the Digital convergence security vision requires two timelines: a **long-term strategic roadmap** and an actionable **short-term implementation plan**. Key considerations during this process include:

1. **There are logical dependencies** between initiatives that must be addressed in the roadmap.
2. **Certain initiatives should be considered pre-requisites**. (such as Asset Management Programs)
3. **Convergence plans are complex**, highly intertwined programs. When it's time to execute, strong program management is required.

Thank you

@osherin

EY
Building a better working world