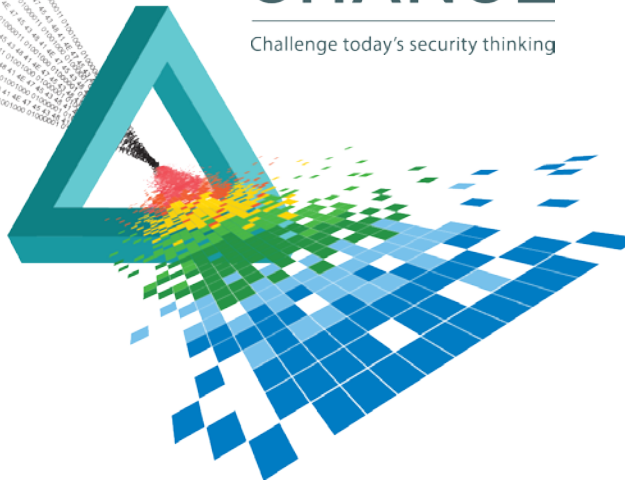
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking



SESSION ID: SPO-W07A

Why the Global Cyber Security Landscape Paints a Concerning Picture

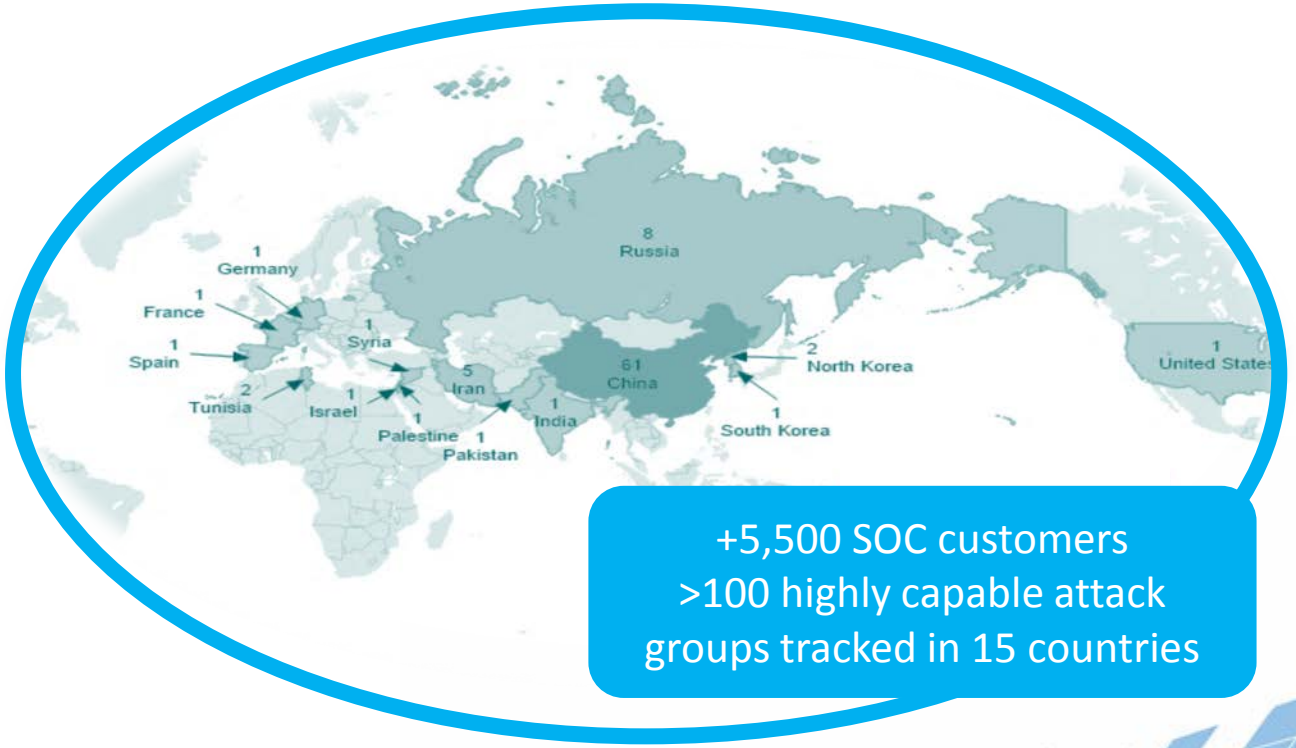
Simon Goldsmith

Director of Cyber Security (Commercial Sectors)
BAE Systems
@BAE_AI

Today's Discussion

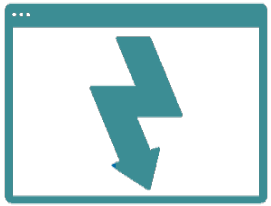
BAE Systems Monitoring the Evolving Threat

- SOC threat intelligence
- Incident Response Team
- Malware feeds
- Open source & security research communities
- Active & passive tracking
- Social media & hacker forums
- Intelligence exchange with trusted partners



Cyber Threat Actor – Recent Activity

Criminals	Activists	Spies	Terrorists
As much money as quickly as possible	Sensational Headlines	National Advantage (Economic or political)	Propaganda, Financing but…..

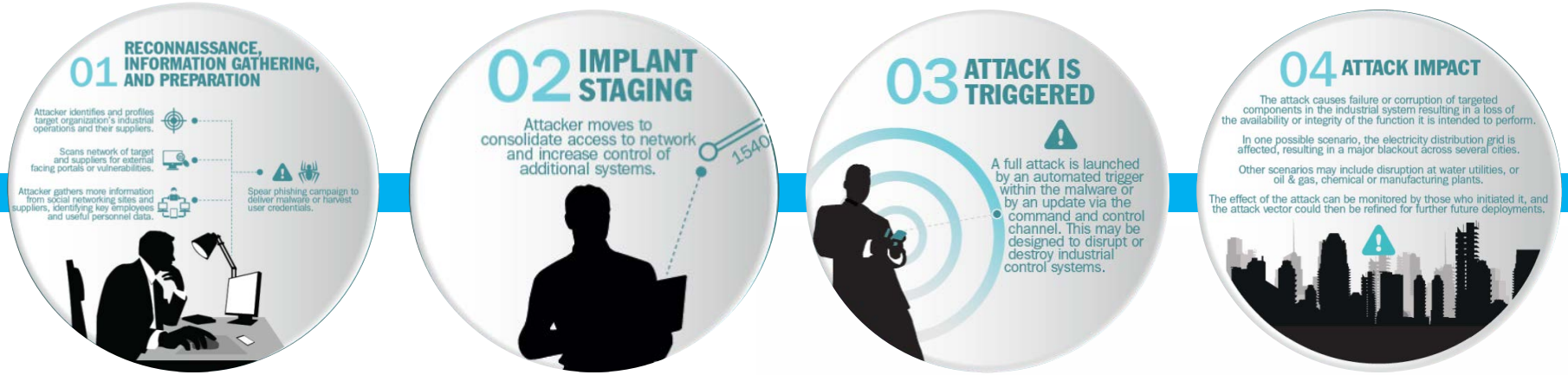


- **Cyber- criminality:** **EMERGING**
- **Cyber- activism:** **HEAVY ACTIVITY**
- **Cyber- espionage:** **HEAVY ACTIVITY**
- **Cyber- terrorism/sabotage:** **…**

BAE SYSTEMS
INSPIRED WORK

Cyber/Physical Convergence

ICS-CERT received and responded to **245** confirmed incidents in 2014. The access vector used in the attack could not be determined in **38%** of cases.



1. **poor detection and monitoring capabilities → lack of cyber incident readiness**
2. **Zero-day exploits for SCADA $8,000 vs $1M for IOS 9**

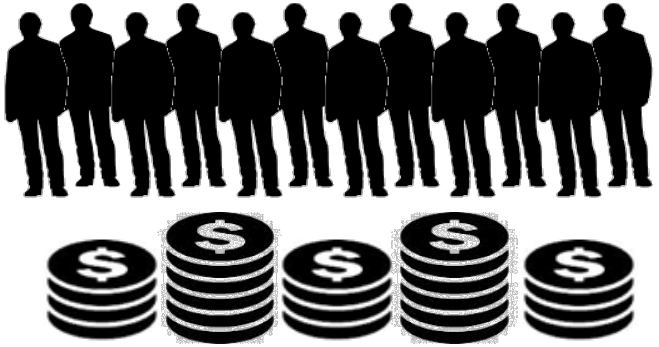
Targeting Strategies

A few targets, large funds

Effort on reconnaissance, targeting and social engineering

Simple (but low volume) malware used

Many targets, small funds



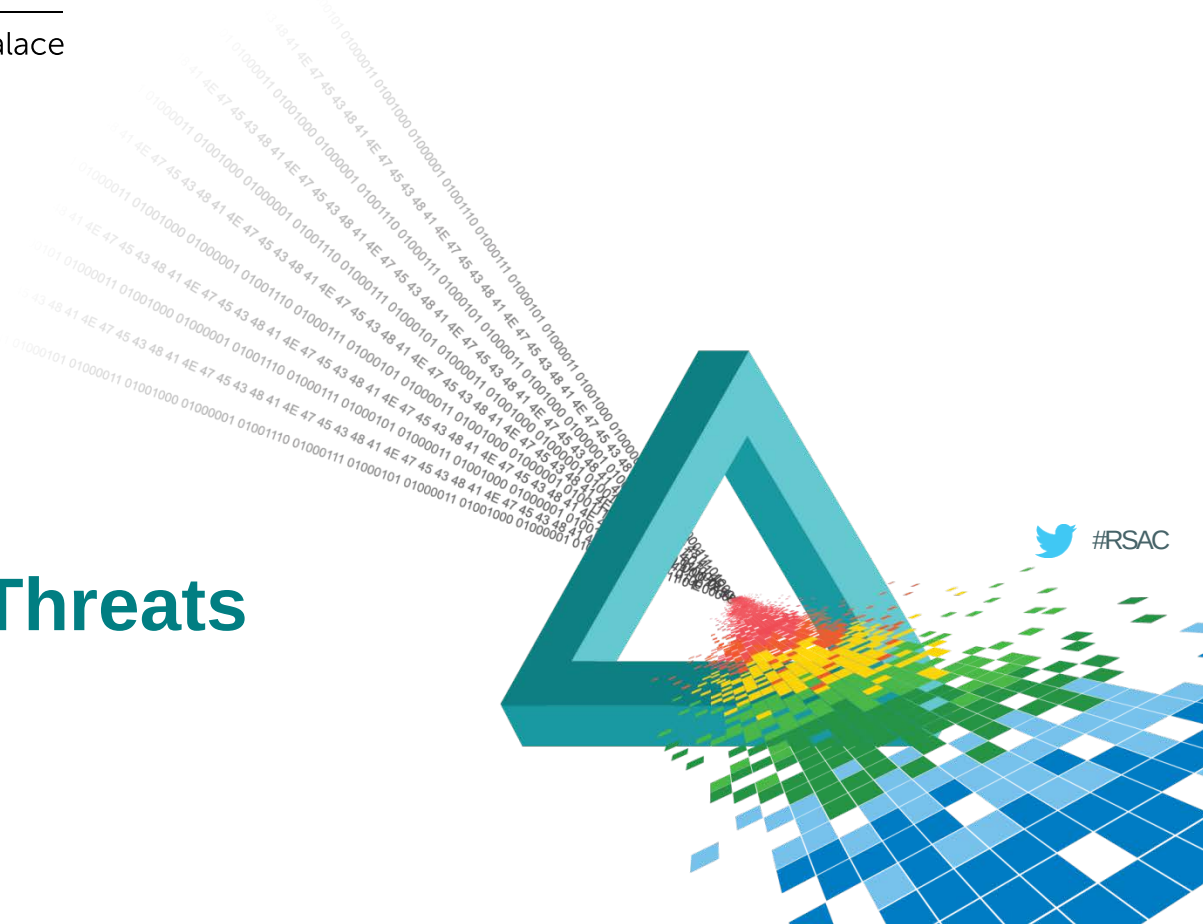
Effort on increasing scale, distribution and success ratio

Complex malware which can adapt itself to avoid detection

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

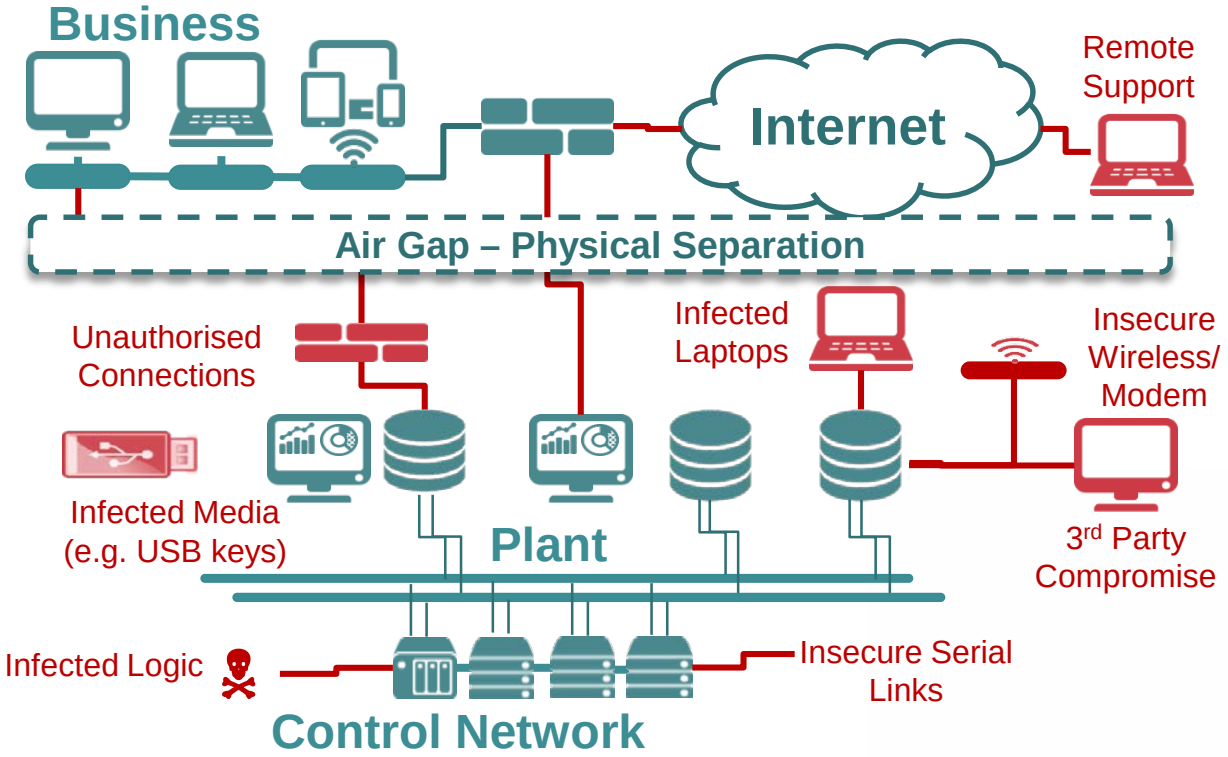
Managing Cyber Threats



Cost and Complexity

Credit: Forrester

Myths and Bad Assumptions



HISTORIC VIEW

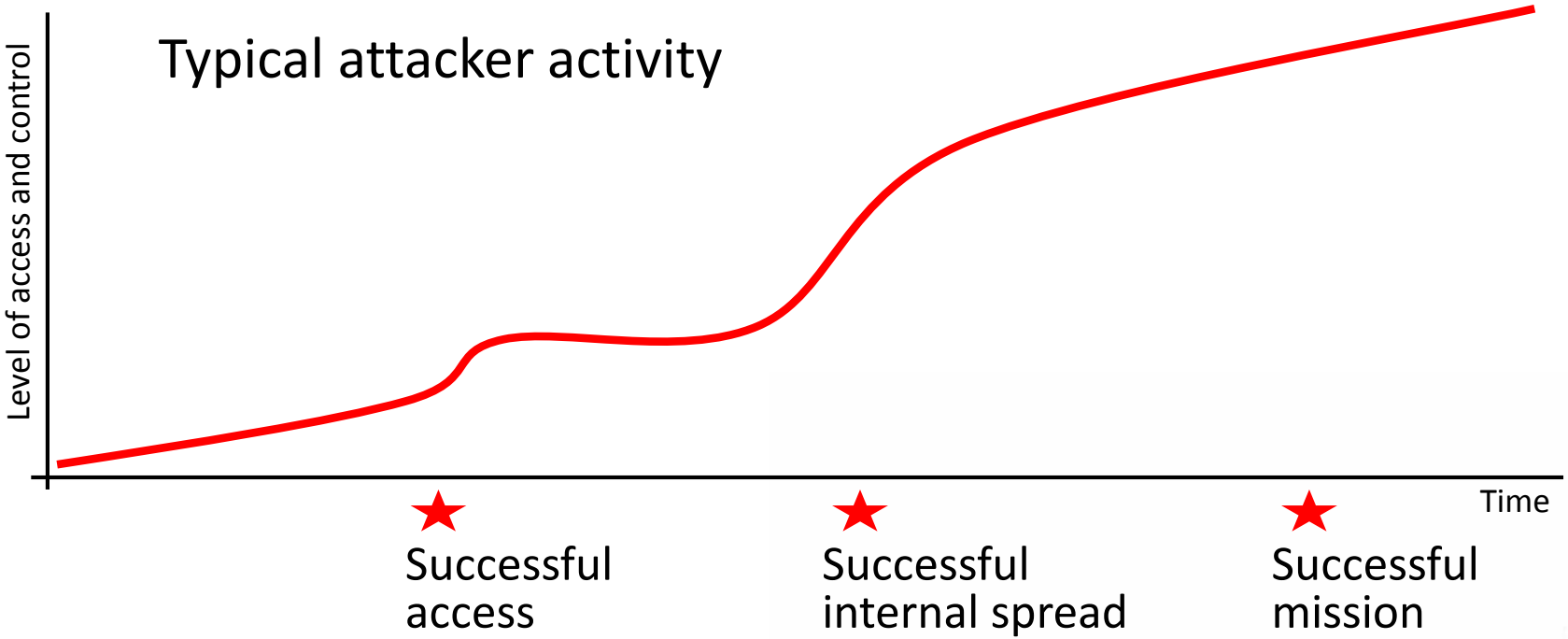
REALITY

"*In our experience … in **no** case have we **ever** found the operations network, the SCADA system or energy management system **separated** from the enterprise network. On average, we see **11 direct connections** between those networks. In some extreme cases, we have identified up to **250 connections** between the actual producing network and the enterprise network.*"
Source: [The Subcommittee on National Security, Homeland Defense, and Foreign Operations May 25, 2011 hearing]

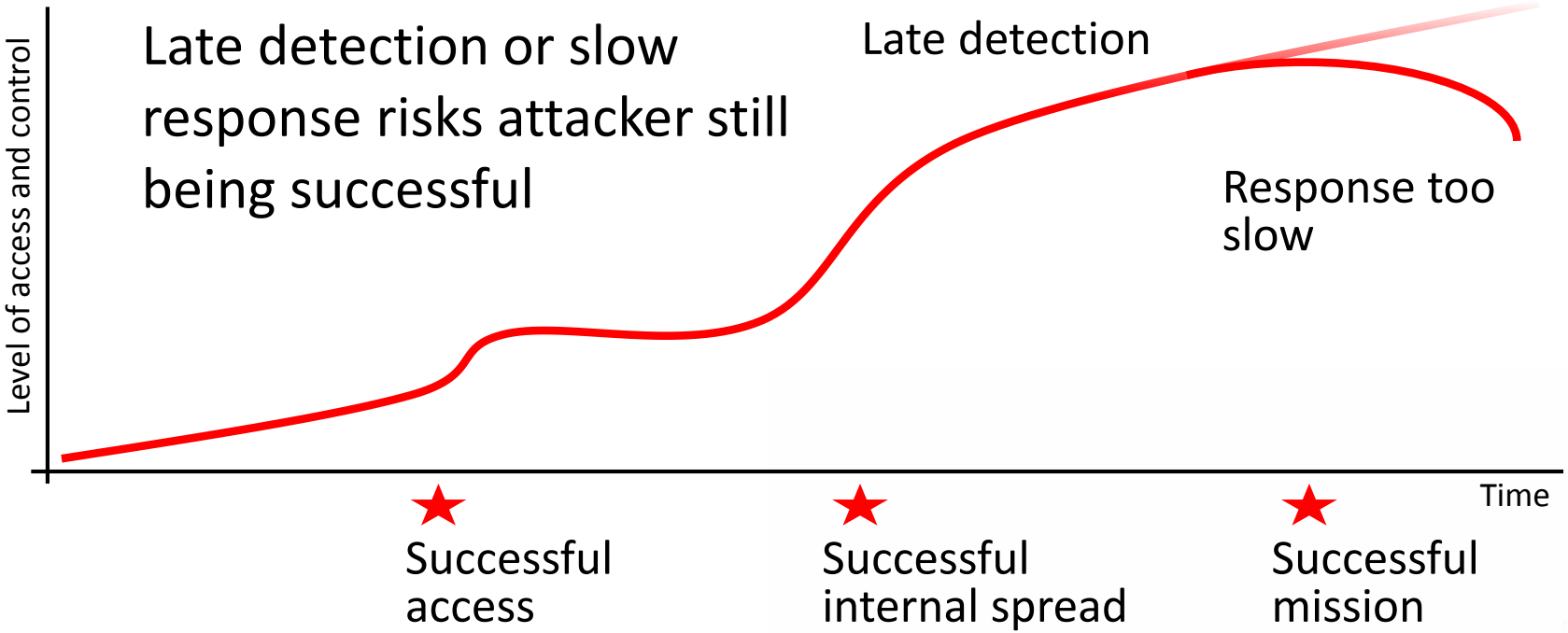
BAE SYSTEMS
INSPIRED WORK

Diverse and Specialist skills

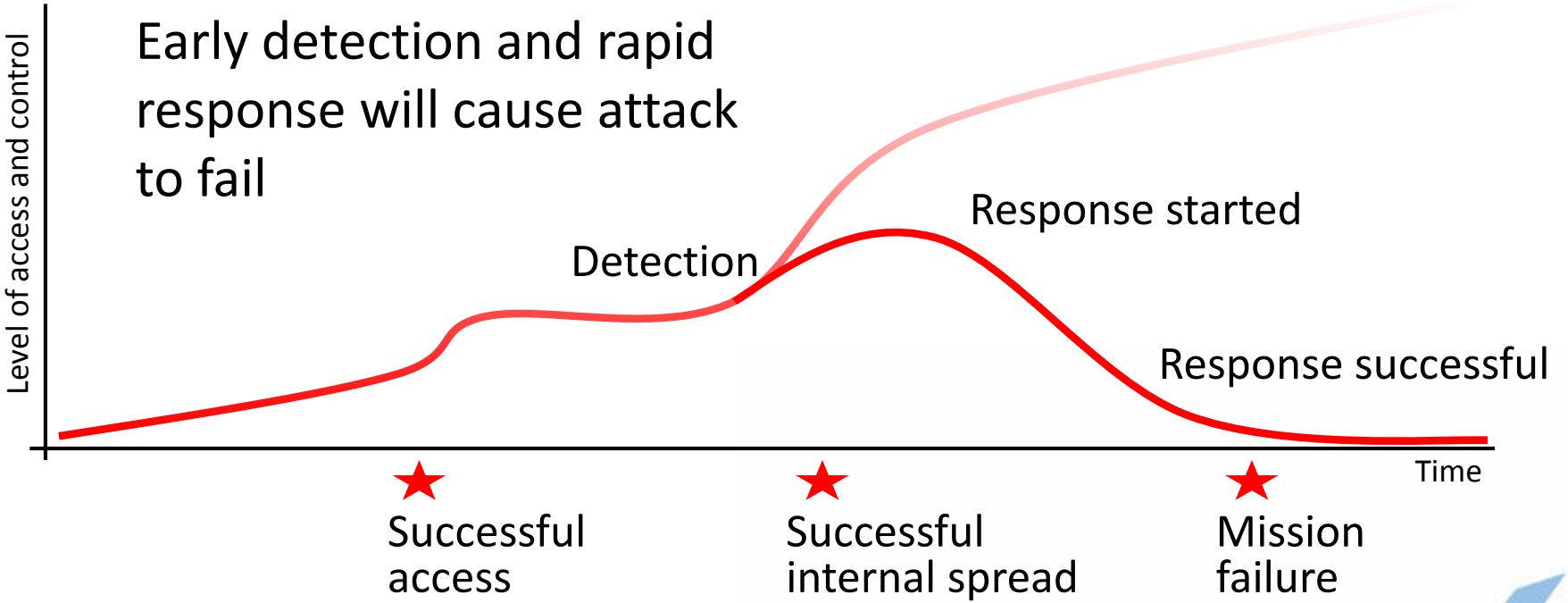
The Difference a Day Makes



The Difference a Day Makes



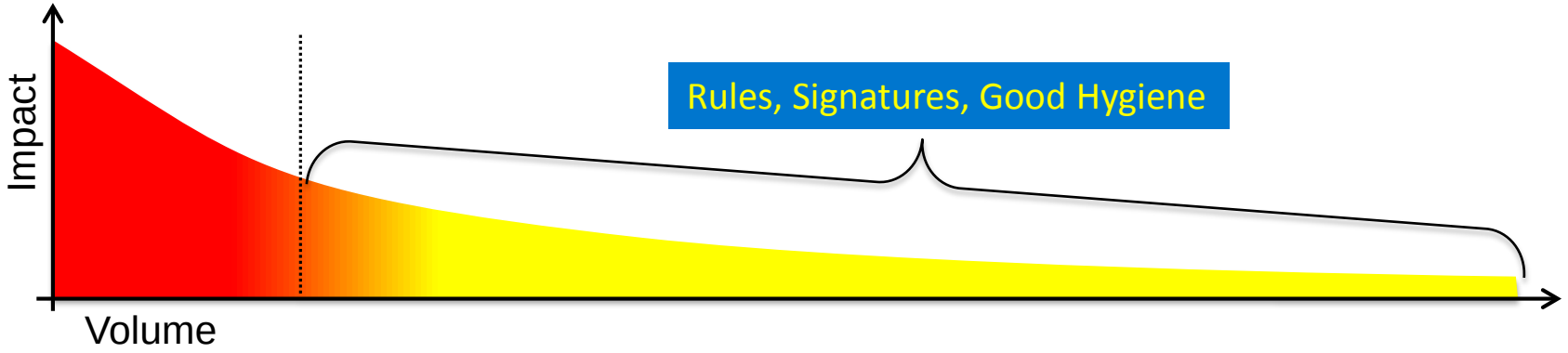
The Difference a Day Makes



Intelligence-led Security Operations

BAE SYSTEMS
INSPIRED WORK

Monitoring Key Components

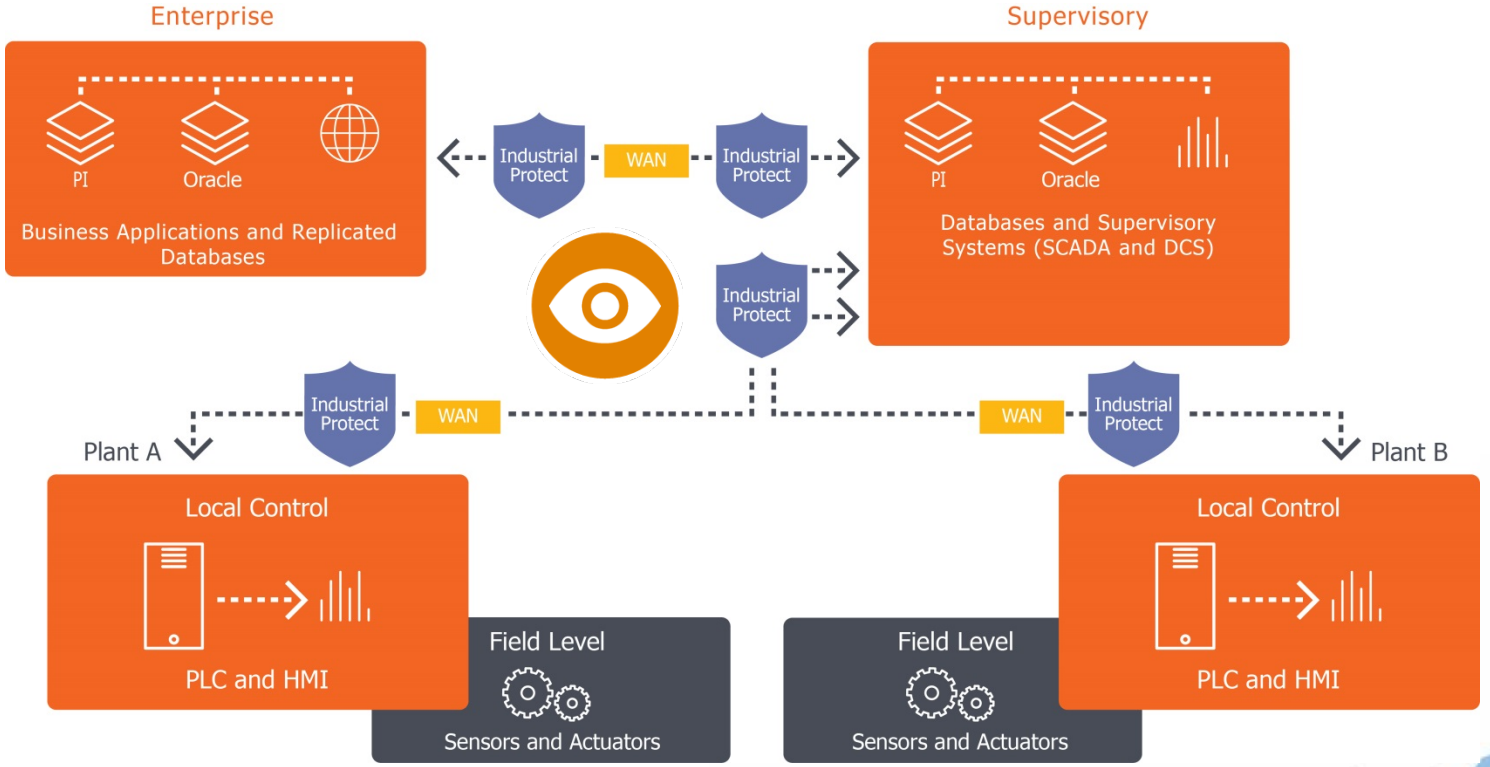


SOC capabilities

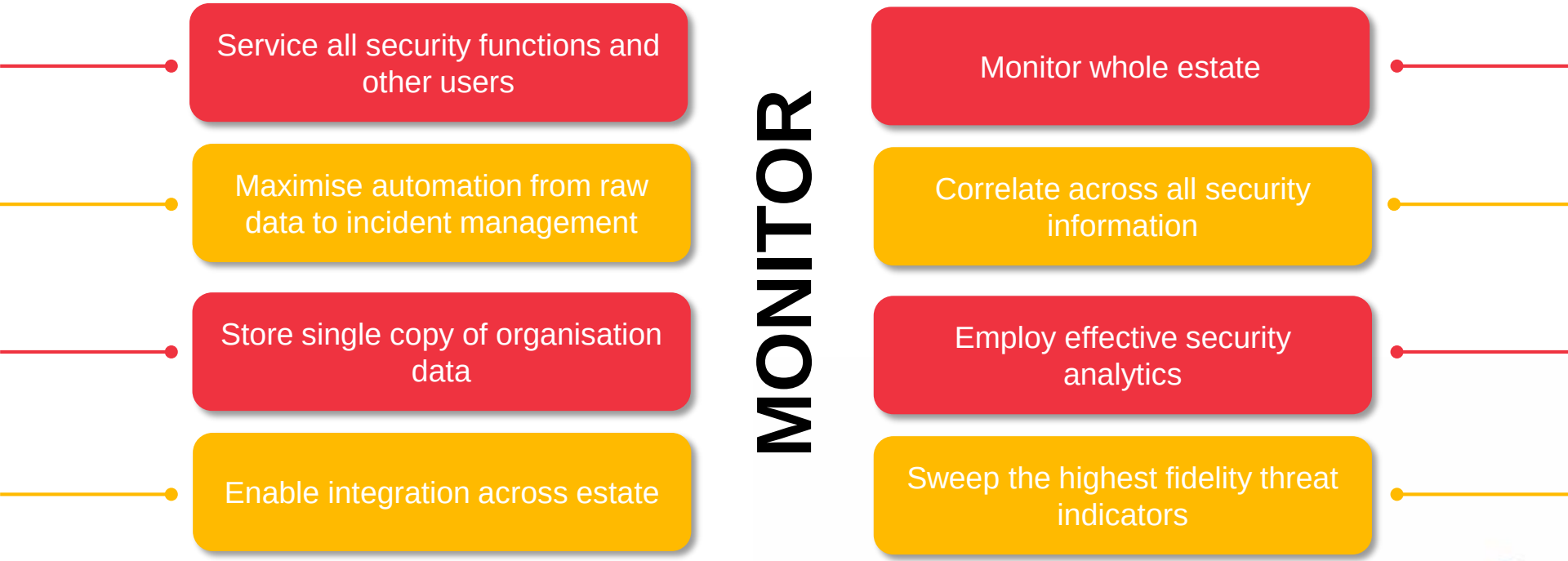
1. Protective Monitoring – Leveraging existing security devices for effective monitoring
2. Security Device Management – Manage security devices to maximise protection
3. Advanced Threat Detection – Detect the most sophisticated attacks
4. Threat Intelligence – Use knowledge of the attackers to improve defences

ADVANCED SECURITY OPERATIONS: AUTOMATE THE MUNDANE AND MAKE THE MOST OF SKILLED SECURITY PERSONNEL

What about SCADA? New Protection Architectures

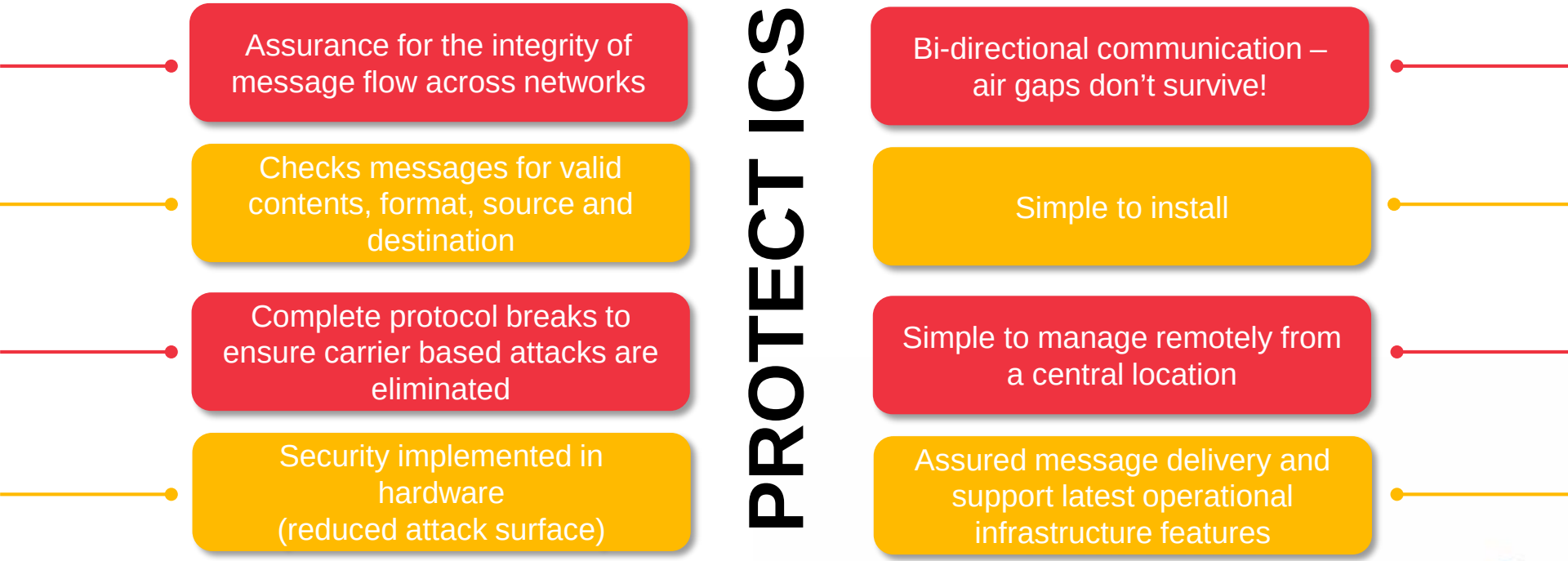


Maximise the Value of People and Data



MAXIMISE THREAT DETECTION

Focus on Integrity and Availability



FOCUS ON EASE OF USE AND PERFORMANCE

RESPOND: INCIDENT READINESS GUIDANCE

- Clear principles and procedures
- Understand the threats and risks
- Technical response
- Legal / HR / PR / Regulatory Compliance

Additional considerations for ICS:

- Safety implications
- Operational continuity
- System diversity

Best Practise

- SANS
- CPNI
- Industry specific

Today's Discussion