

RSA®Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SPO-W07A

Why the Global Cyber Security Landscape Paints a Concerning Picture

Simon Goldsmith

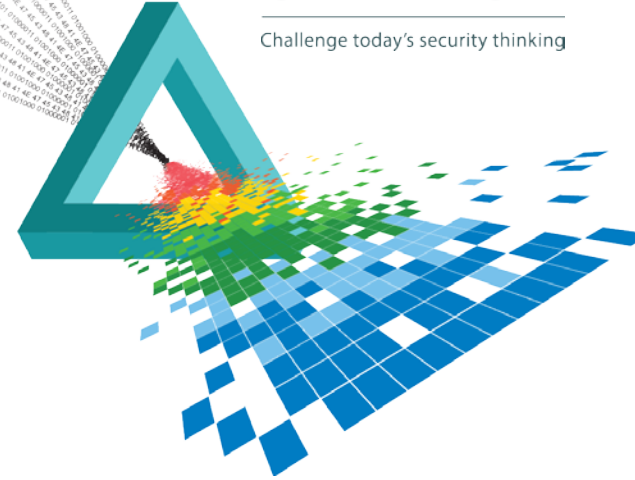
Director of Cyber Security (Commercial Sectors)

BAE Systems

@BAE_AI

CHANGE

Challenge today's security thinking



Today's Discussion

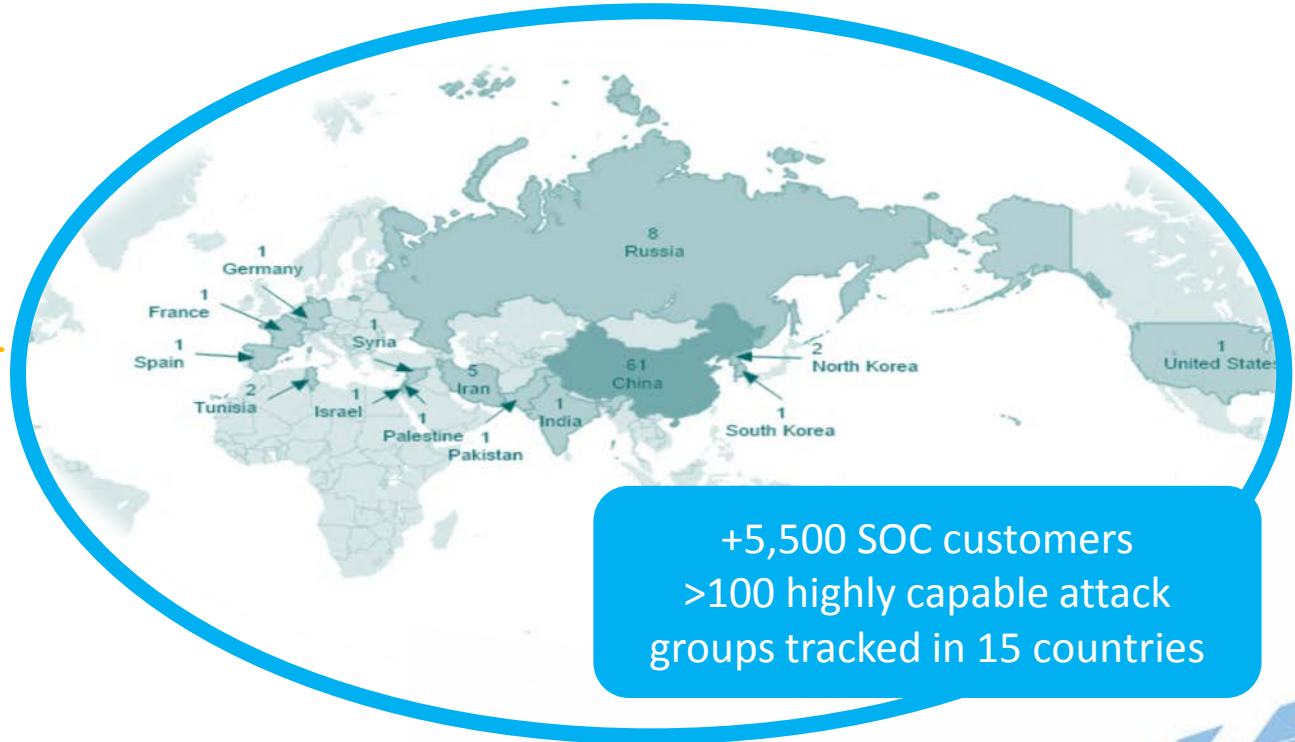


PART 1 THE CYBER THREAT LANDSCAPE

PART 2 MANAGING CYBER THREATS

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

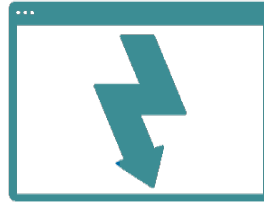
Criminals

As much money as quickly as possible



Activists

Sensational Headlines



Spies

National Advantage
(Economic or political)



Terrorists

Propaganda, Financing
but....

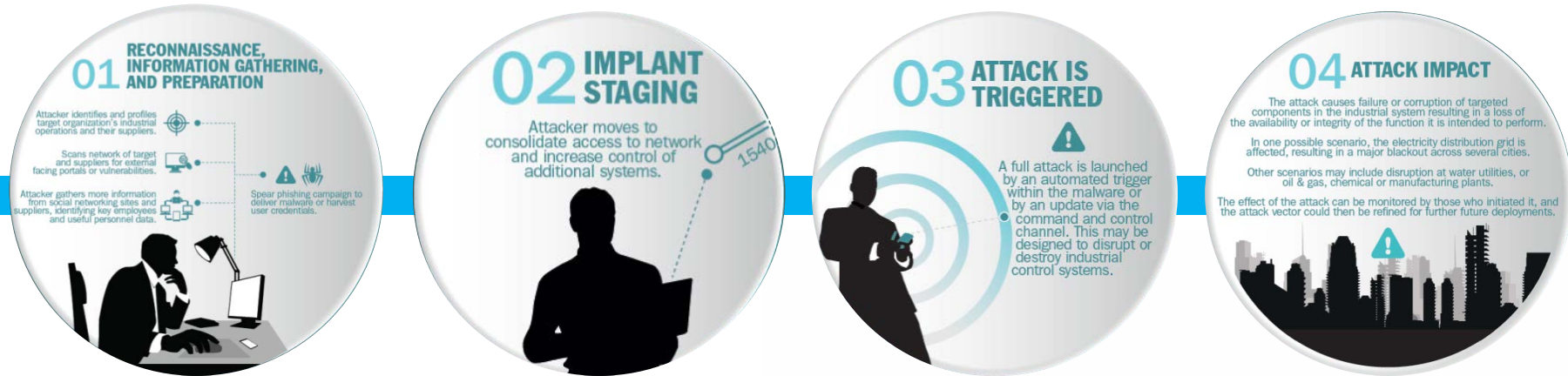


- Cyber- criminality:
- Cyber- activism:
- Cyber- espionage:
- Cyber- terrorism/sabotage: ...

EMERGING
HEAVY ACTIVITY
HEAVY ACTIVITY

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

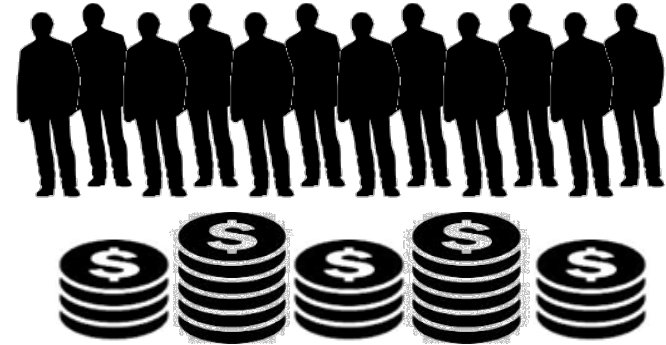
Targeting Strategies

A few targets, large funds



Effort on reconnaissance,
targeting and social engineering
Simple (but low volume) malware
used

Many targets, small funds

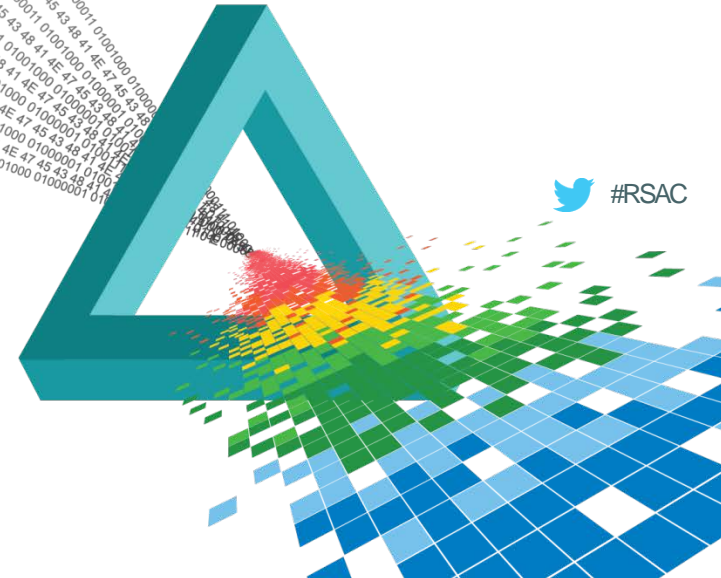


Effort on increasing scale,
distribution and success ratio
Complex malware which can
adapt itself to avoid detection

RSA[®]Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

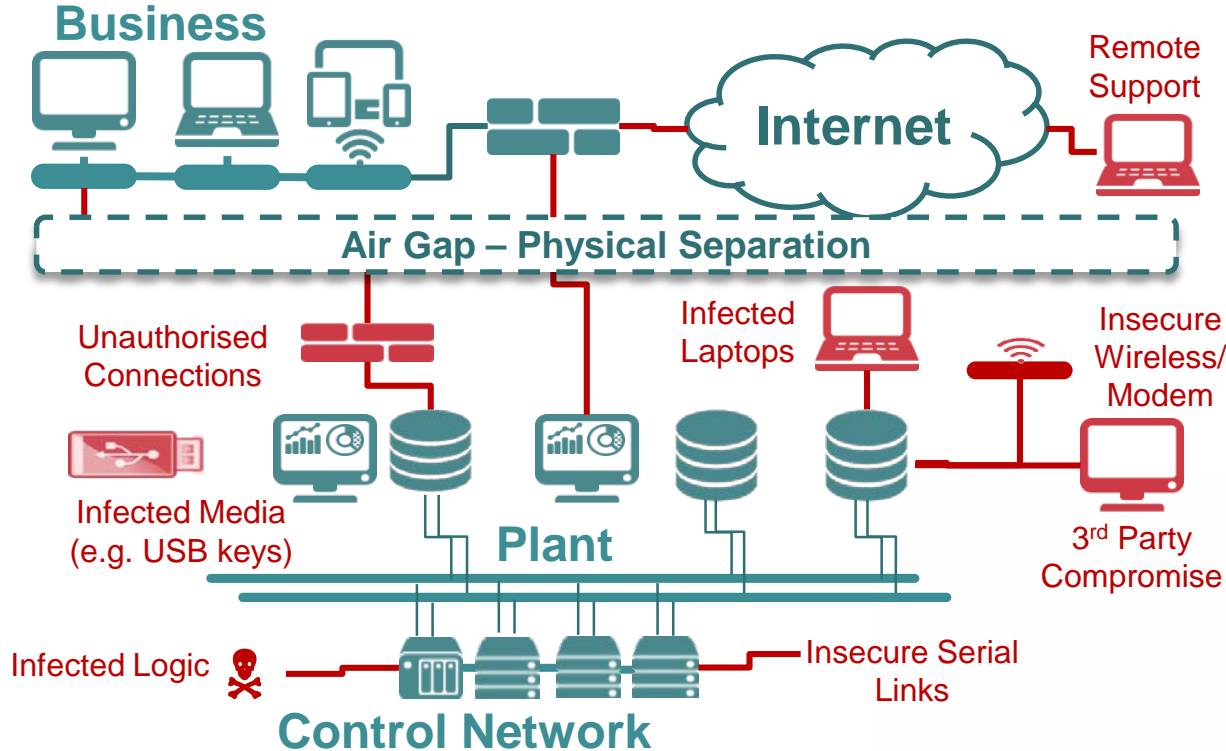
Managing Cyber Threats



Cost and Complexity



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](#)

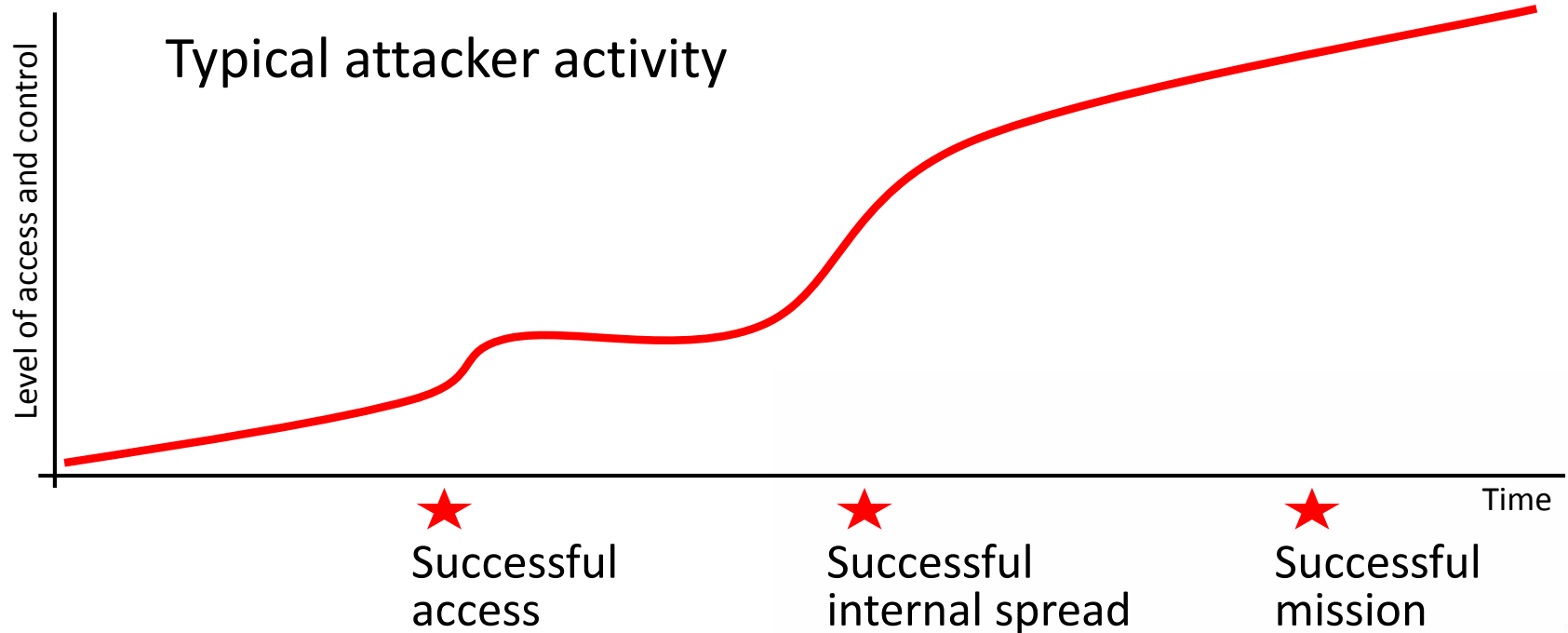
Diverse and Specialist skills



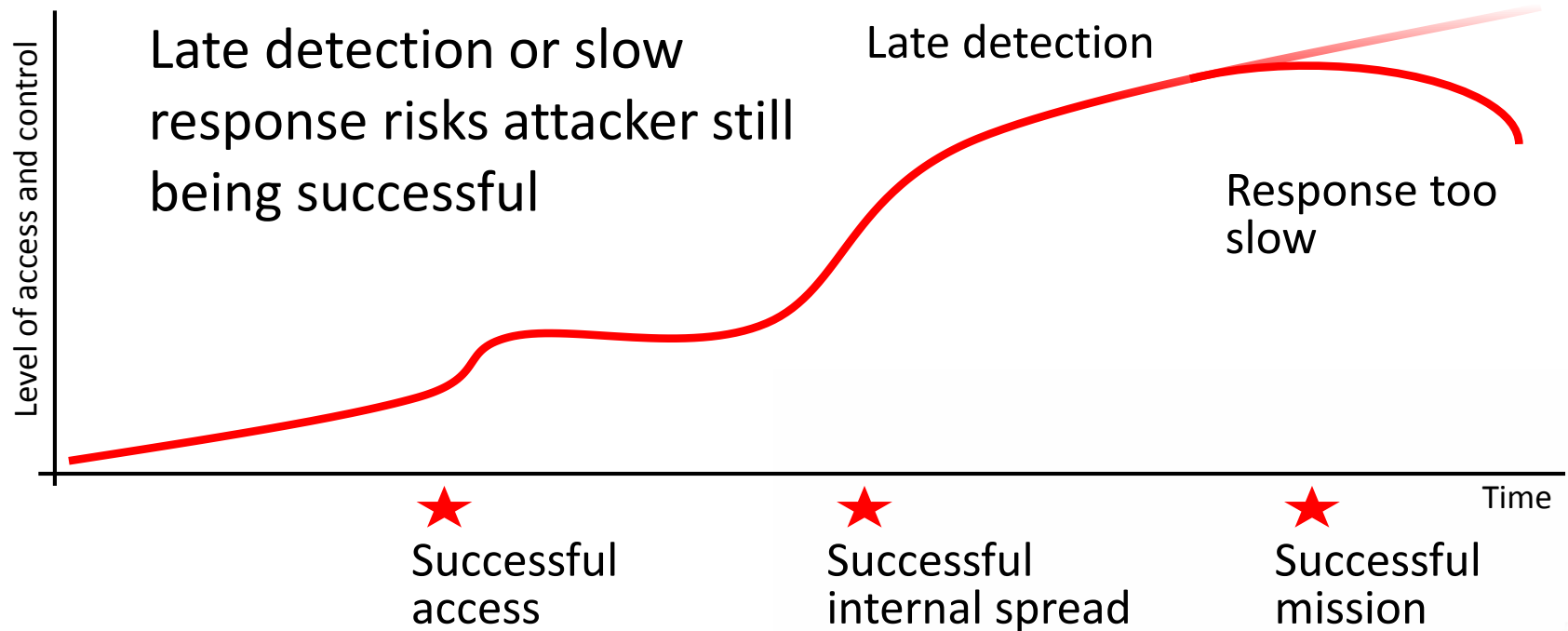
A word cloud centered around the title 'Cyber Investigator'. The words are arranged in a circular pattern around the central text, with varying font sizes and colors (teal and blue) to represent different skill sets. The skills include:

- Public Relations
- Managing Stress
- Technical Writing
- Legal Notification
- Reporting
- Response actions
- Data Collection
- Monitoring Deployment
- Network Architectures
- Data Protection
- Remediation
- Business Knowledge
- Risk Assessment & Mitigation
- Problem Solving & Decision Making
- Prioritisation
- Image Acquisition
- Digital Forensics
- Evidential Processes
- Team Management
- Operating Systems
- Programming
- Threat Intelligence
- Reverse Engineering
- Malware Analysis
- Data Science
- Network Analytics
- Disk Analysis
- Log Data Processing
- Cryptography
- File Formats
- Network Protocols

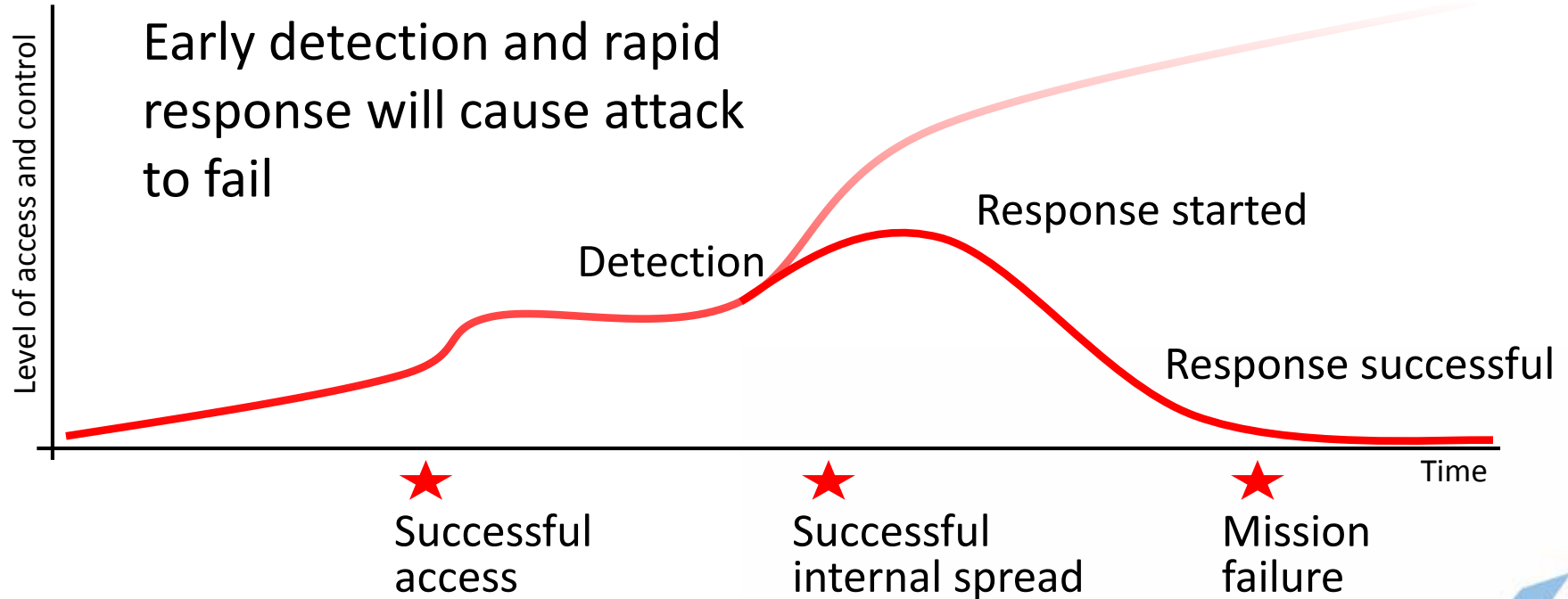
The Difference a Day Makes



The Difference a Day Makes



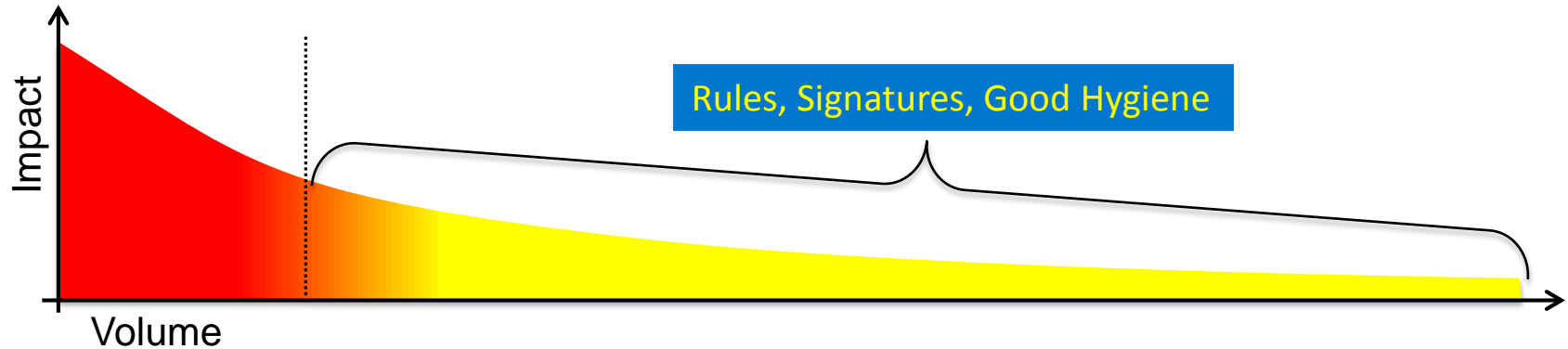
The Difference a Day Makes



Intelligence-led Security Operations



Monitoring Key Components

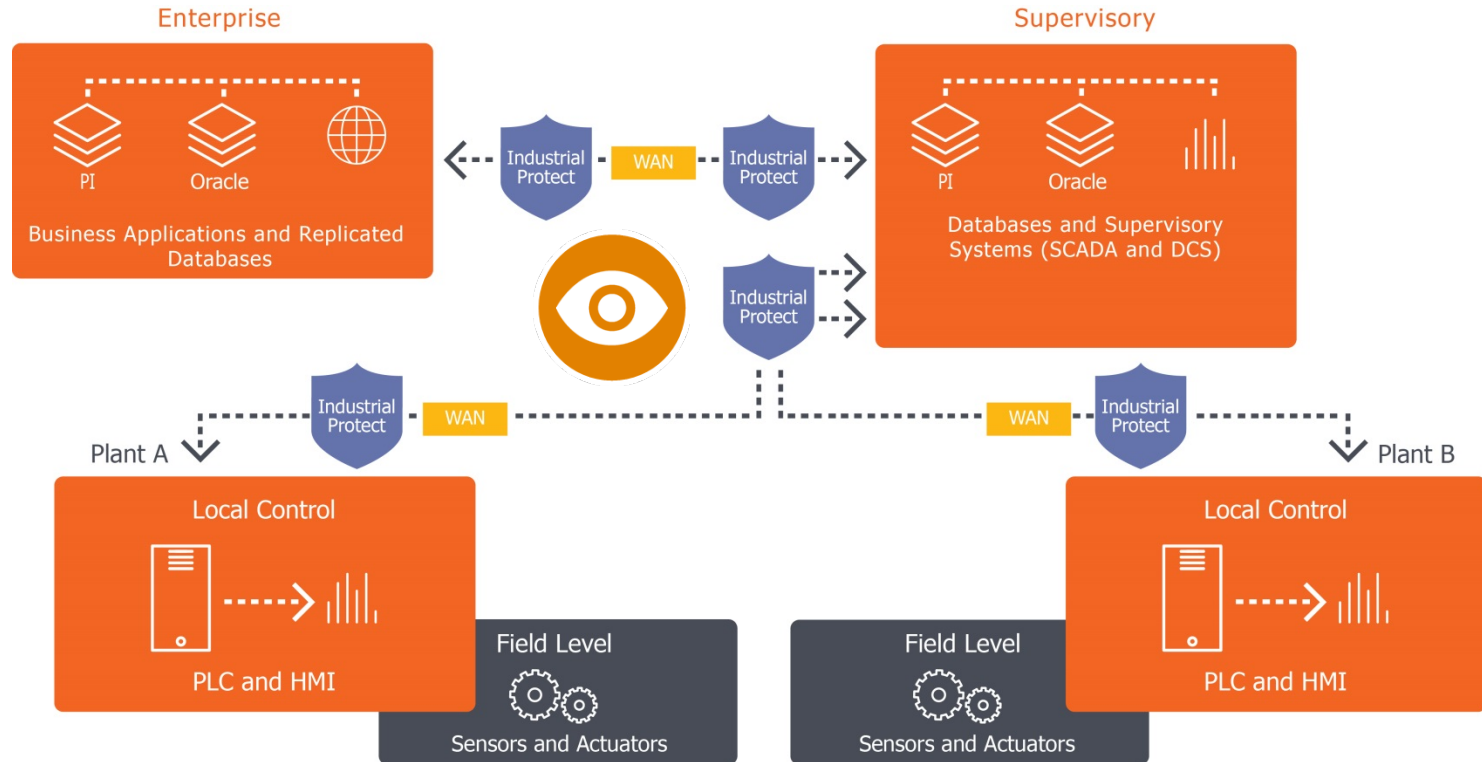


SOC capabilities

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

Service all security functions and other users

Maximise automation from raw data to incident management

Store single copy of organisation data

Enable integration across estate

MONITOR

Monitor whole estate

Correlate across all security information

Employ effective security analytics

Sweep the highest fidelity threat indicators

MAXIMISE THREAT DETECTION

Focus on Integrity and Availability

Assurance for the integrity of message flow across networks

Checks messages for valid contents, format, source and destination

Complete protocol breaks to ensure carrier based attacks are eliminated

Security implemented in hardware (reduced attack surface)

PROTECT ICS

Bi-directional communication – air gaps don't survive!

Simple to install

Simple to manage remotely from a central location

Assured message delivery and support latest operational infrastructure features

FOCUS ON EASE OF USE AND PERFORMANCE

BAE SYSTEMS

INSPIRED WORK

RSA
Conference
2015

Abu Dhabi

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

Q&A