BAE SYSTEMS
INSPIRED WORK

CSM-ACE 2014

Cyber Threat Intelligence Driven Environments

Presented by James Calder
Client Services Manager, Singapore

BAE SYSTEMS
INSPIRED WORK

CONTENTS

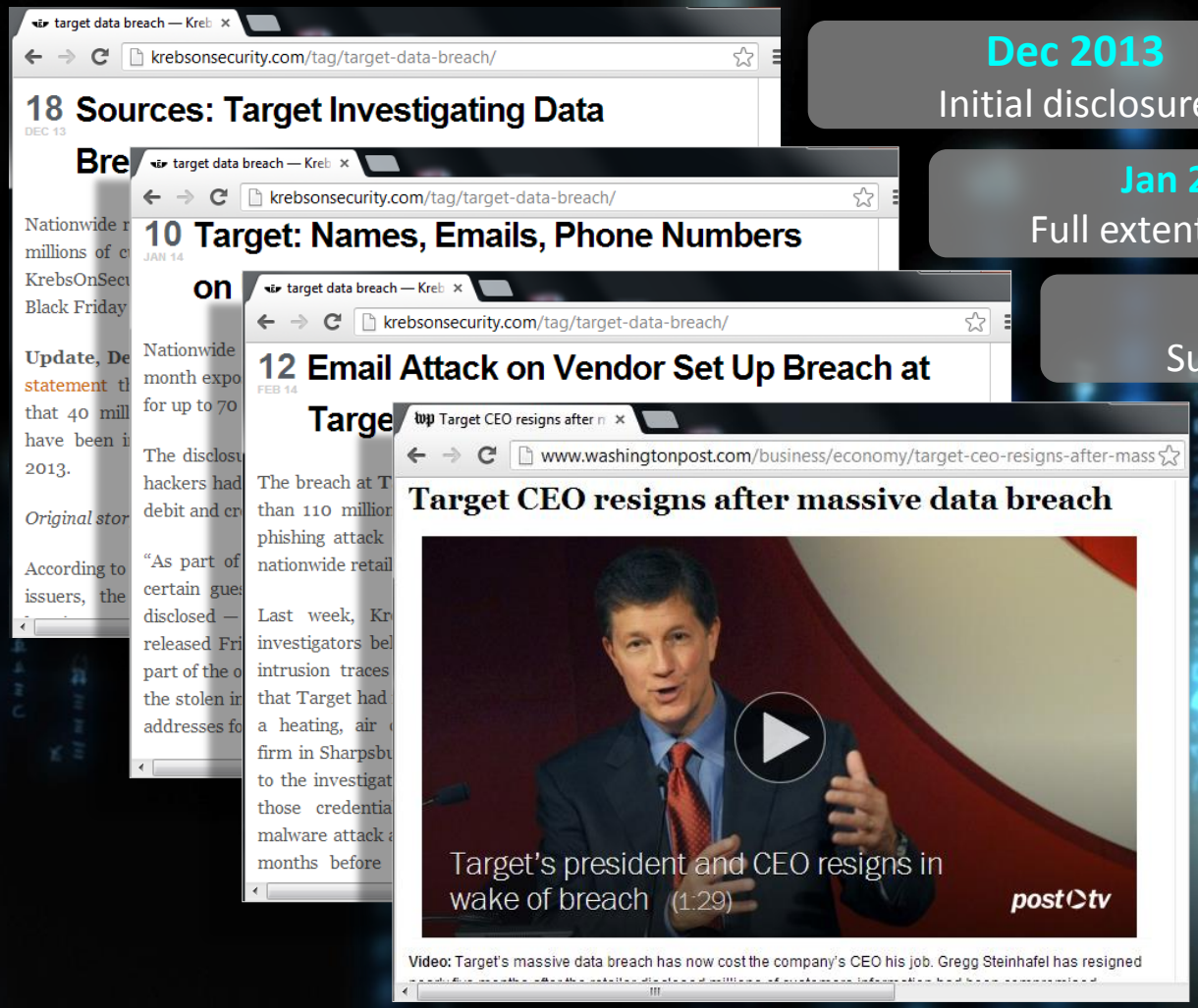
BAE SYSTEMS
INSPIRED WORK

DIGITAL CRIMINALITY

Convergent trends in cyber and financial crime

BAE SYSTEMS
INSPIRED WORK

RISKS IN CYBER SPACE



Dec 2013
Initial disclosure

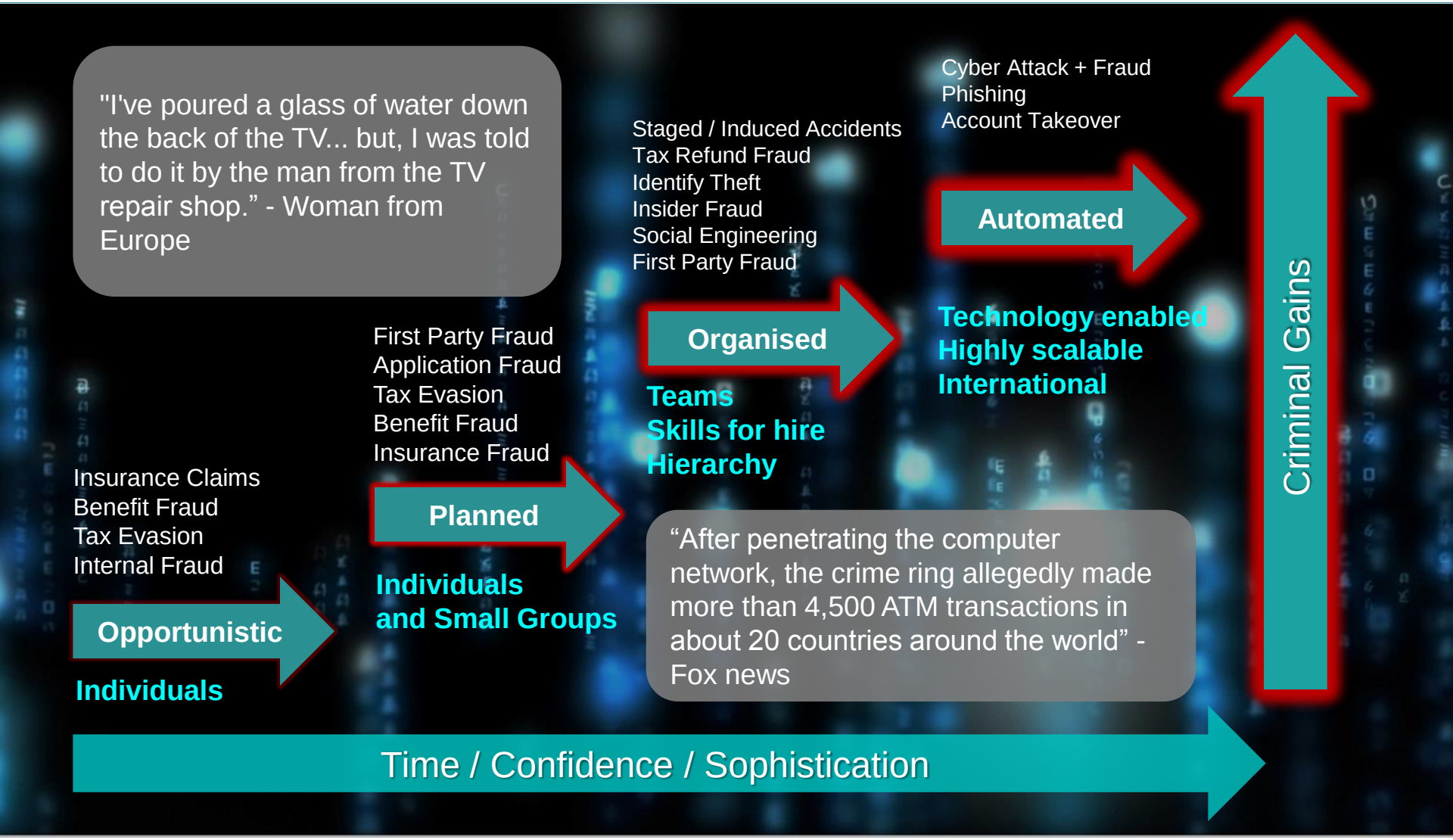
Jan 2014
Full extent revealed

Feb 2014
Supply chain link

May 2014
Target CEO resigns

BAE SYSTEMS
INSPIRED WORK

EVOLUTION OF FRAUD ATTACK METHODOLOGIES



BAE SYSTEMS
INSPIRED WORK

THE ROLE OF CYBER IN ENABLING FRAUD

Definitions

Cyber-crime: Illegal or damaging acts in cyber-space (eg “hacking”, DDoS, information theft)

Cyber-enabled crime: Crimes facilitated or enhanced through use of cyber-space

Digital criminal: Organised criminals who specialise in stealing money using cyber techniques

	Fraud Challenge	Cyber Challenge
Definition	Fraud attacks are attacks against a business process	Cyber attacks are against information technology infrastructure
Method	Criminals seek to create or manipulate transactions.	Criminals seek to steal data or control/disrupt systems.
Threat Actor Goal	Financial Gain	Information Theft System Manipulation Economic Espionage Denial of Service

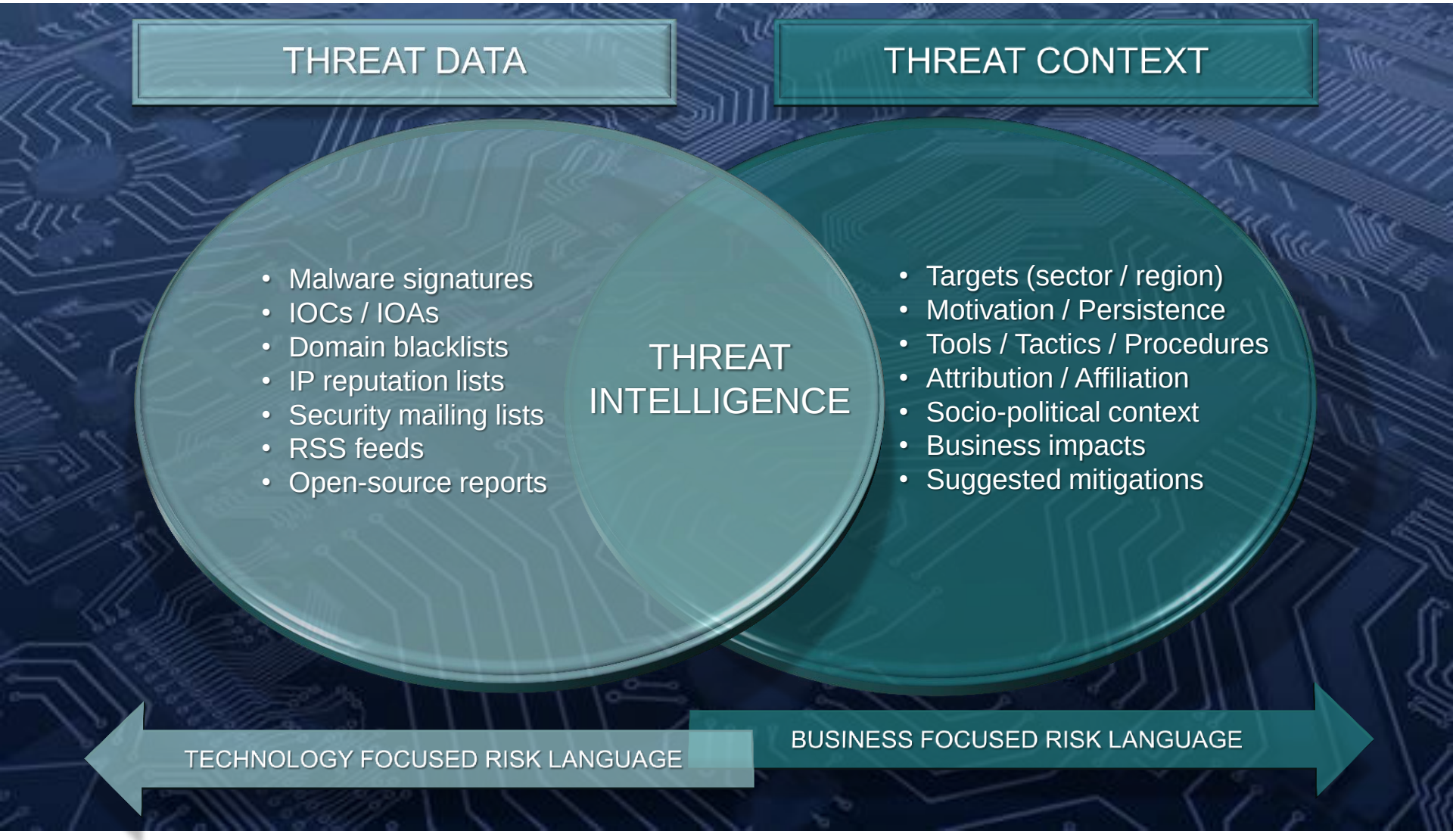
BAE SYSTEMS
INSPIRED WORK

Intelligence-led security

Understanding threat intelligence

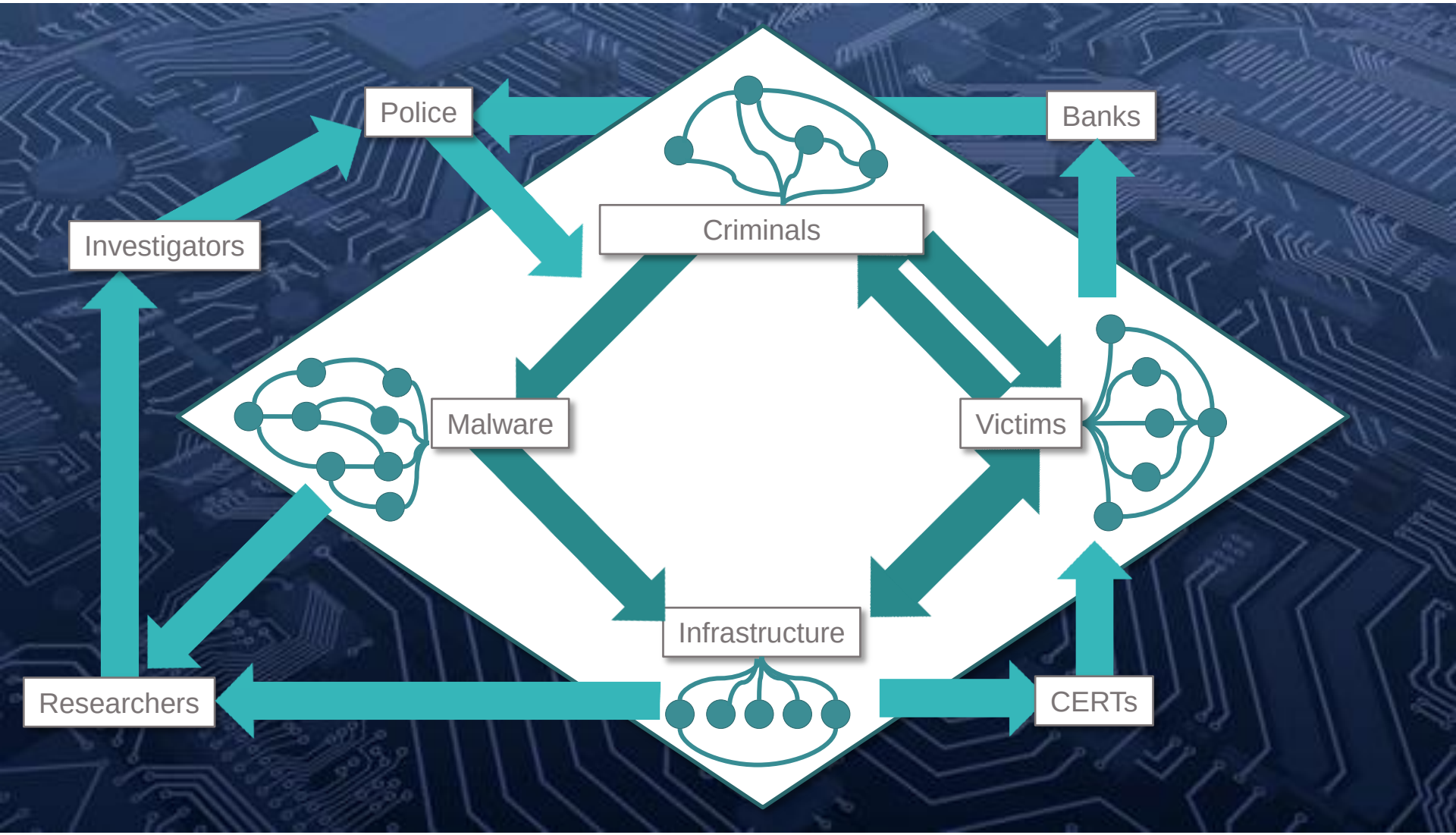
BAE SYSTEMS
INSPIRED WORK

UNDERSTANDING THREAT INTELLIGENCE



BAE SYSTEMS
INSPIRED WORK

DRIVES THE BUILDING OF INTELLIGENCE MODELS



BAE SYSTEMS
INSPIRED WORK

SIX STEPS TO INTELLIGENCE-LED SECURITY

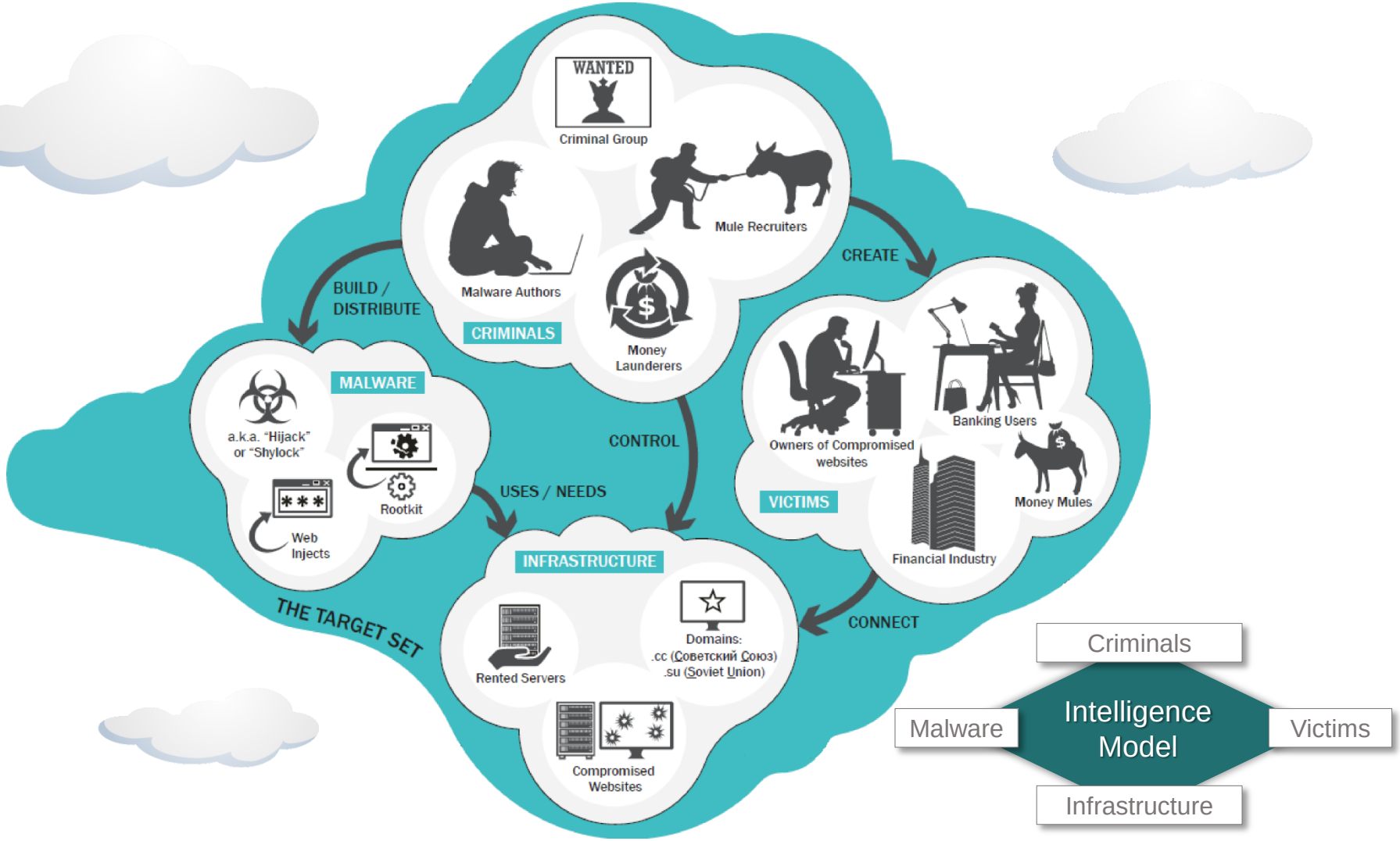
BAE SYSTEMS
INSPIRED WORK

Shylock Case Study

Use of threat intelligence to counter digital crime

BAE SYSTEMS
INSPIRED WORK

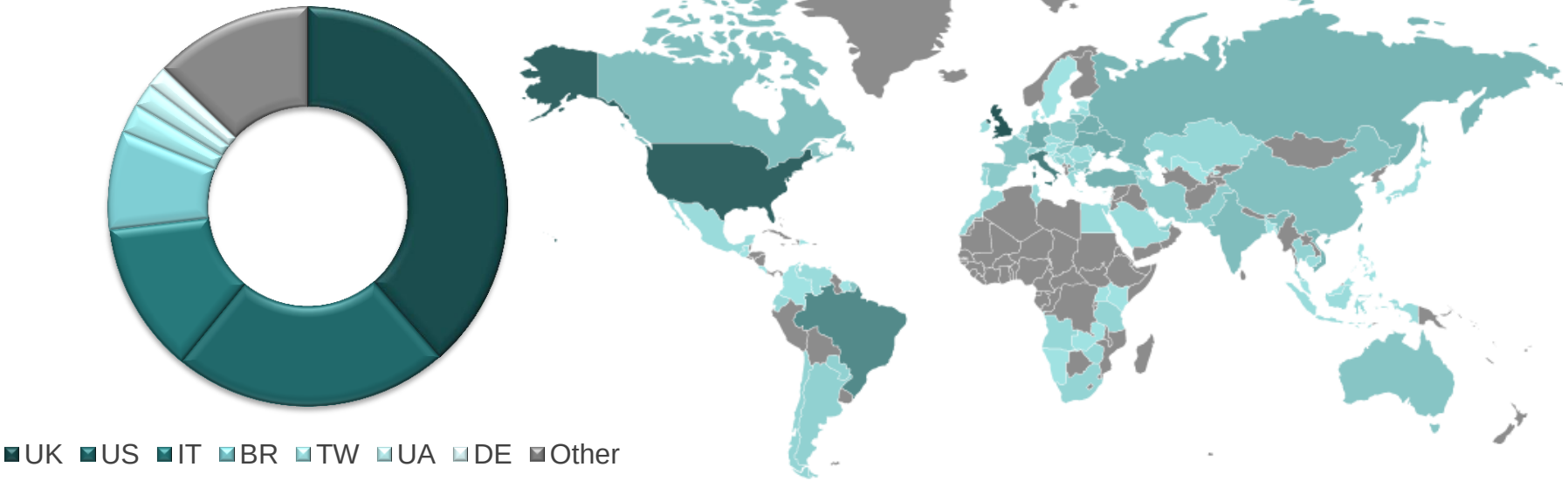
SHYLOCK – A CYBER CRIMINAL INTELLIGENCE PROBLEM



BAE SYSTEMS
INSPIRED WORK

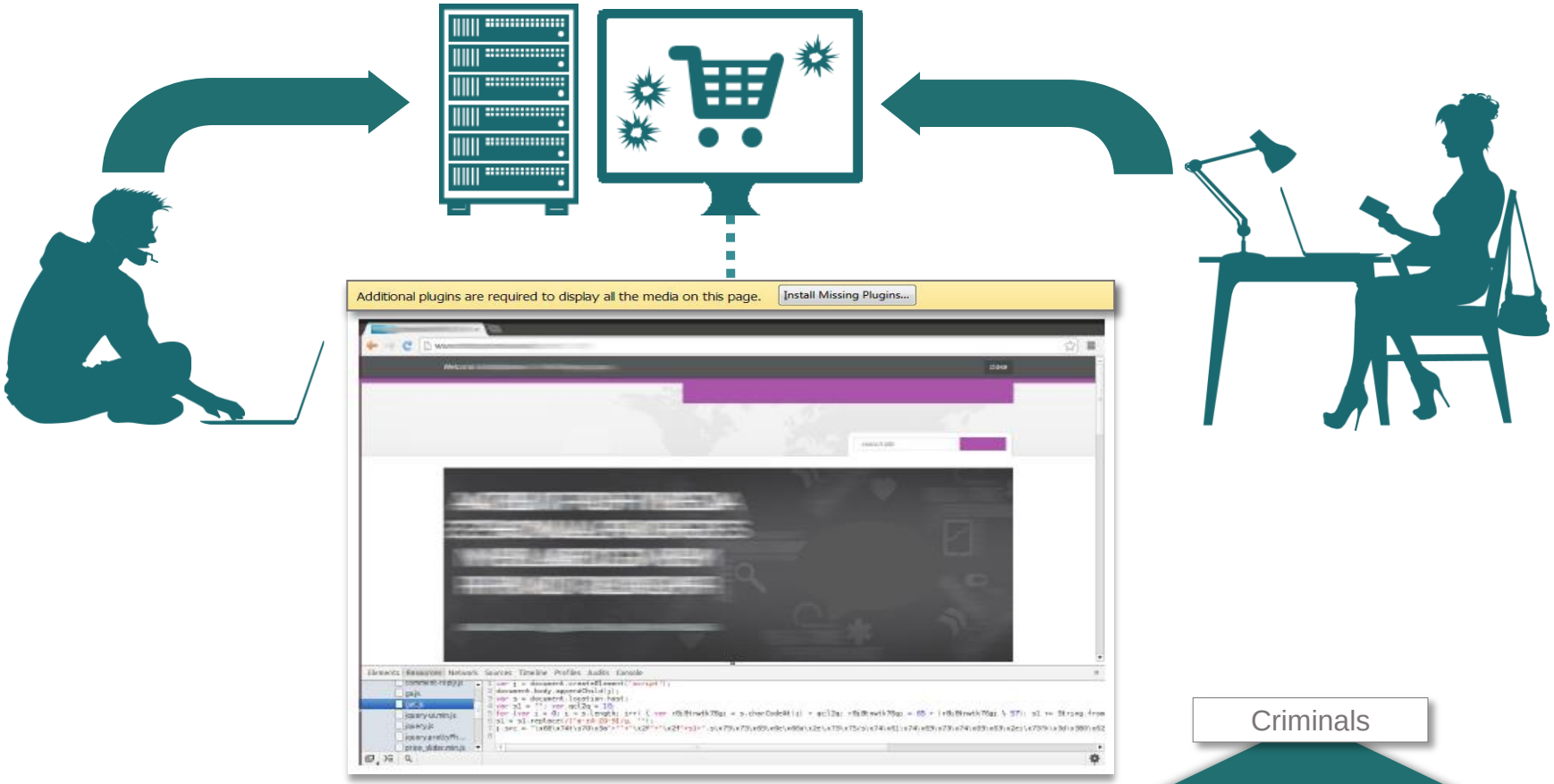
SHYLOCK FINANCIAL CRIME OPERATION

- **Estimated** at over 50K machines compromised
- **Global** victimisation, but with a **preference** for UK, US, and Italy



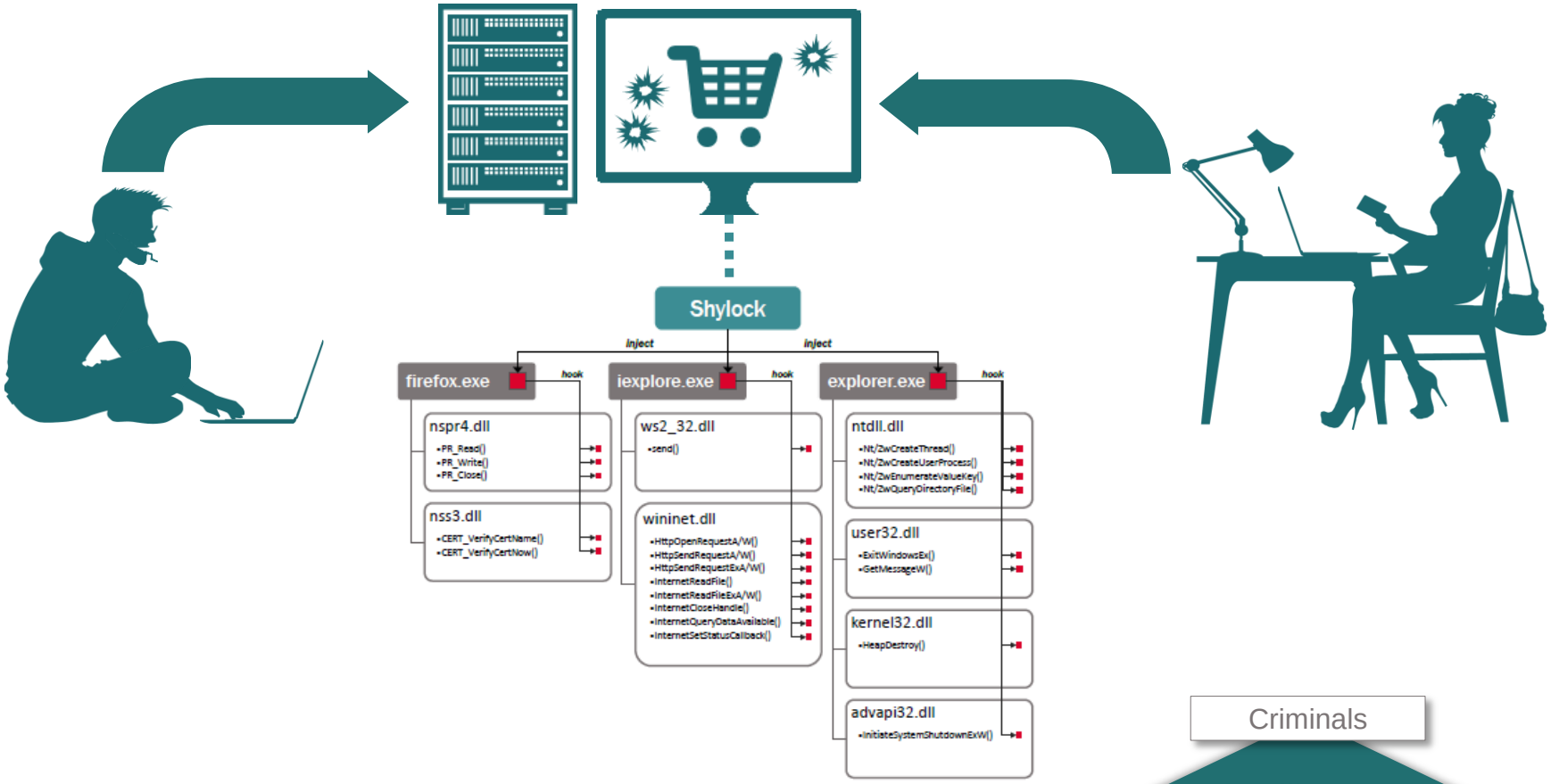
BAE SYSTEMS
INSPIRED WORK

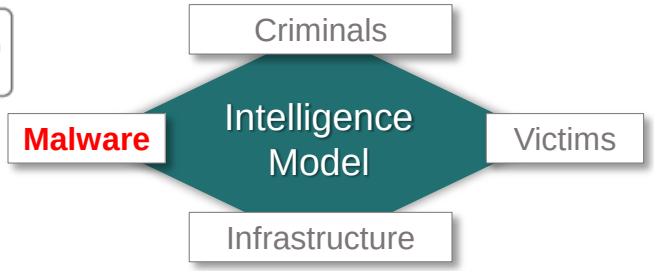
HOW IT WORKS – COMPROMISING THE VICTIM



BAE SYSTEMS
INSPIRED WORK

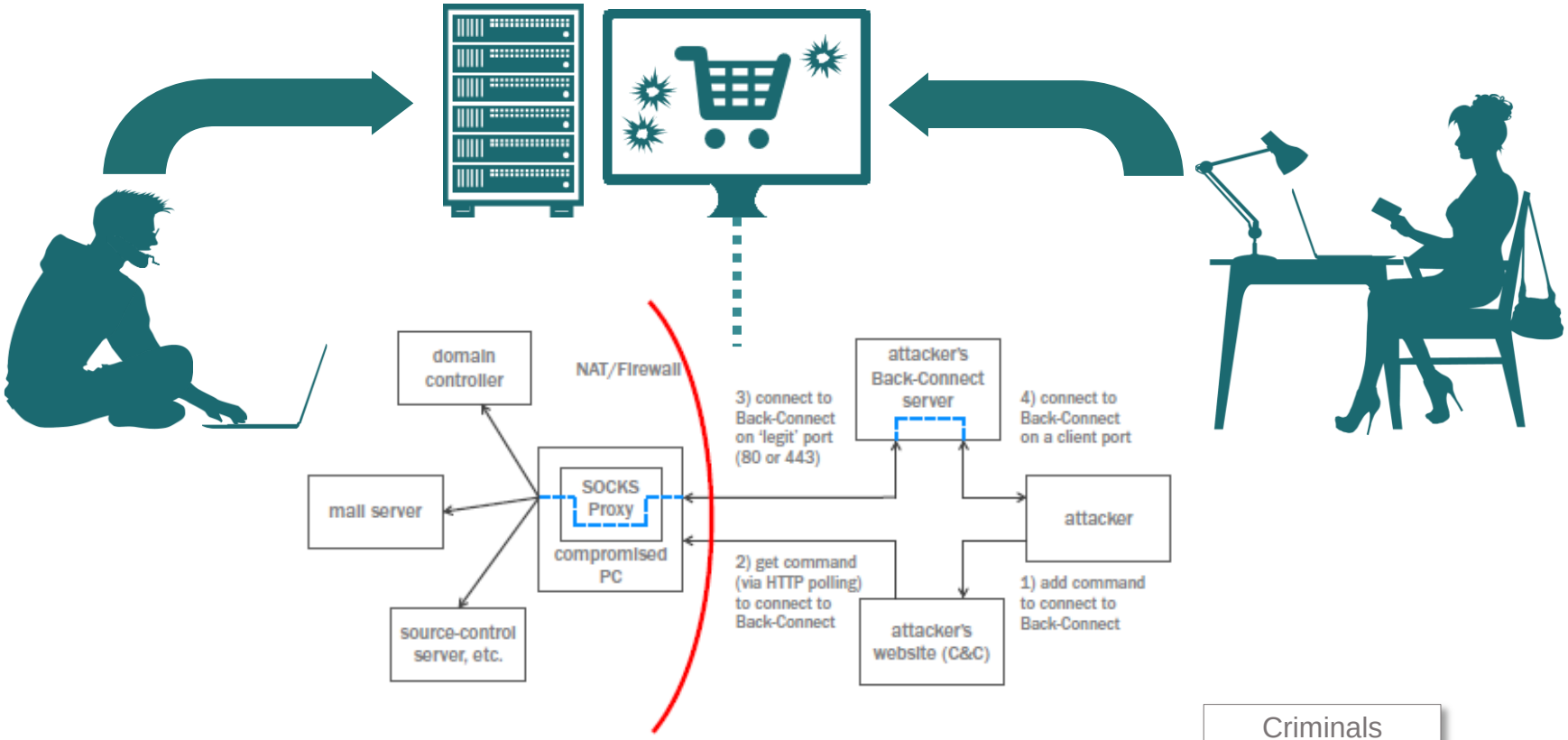
HOW IT WORKS – MALWARE AUTOMATION

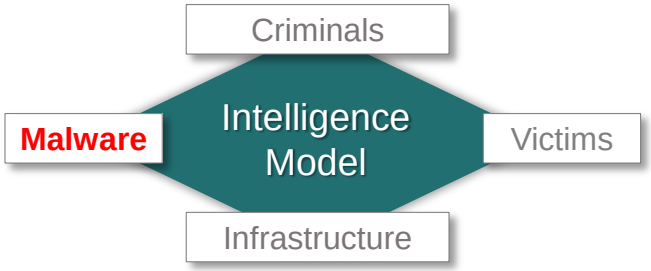




BAE SYSTEMS
INSPIRED WORK

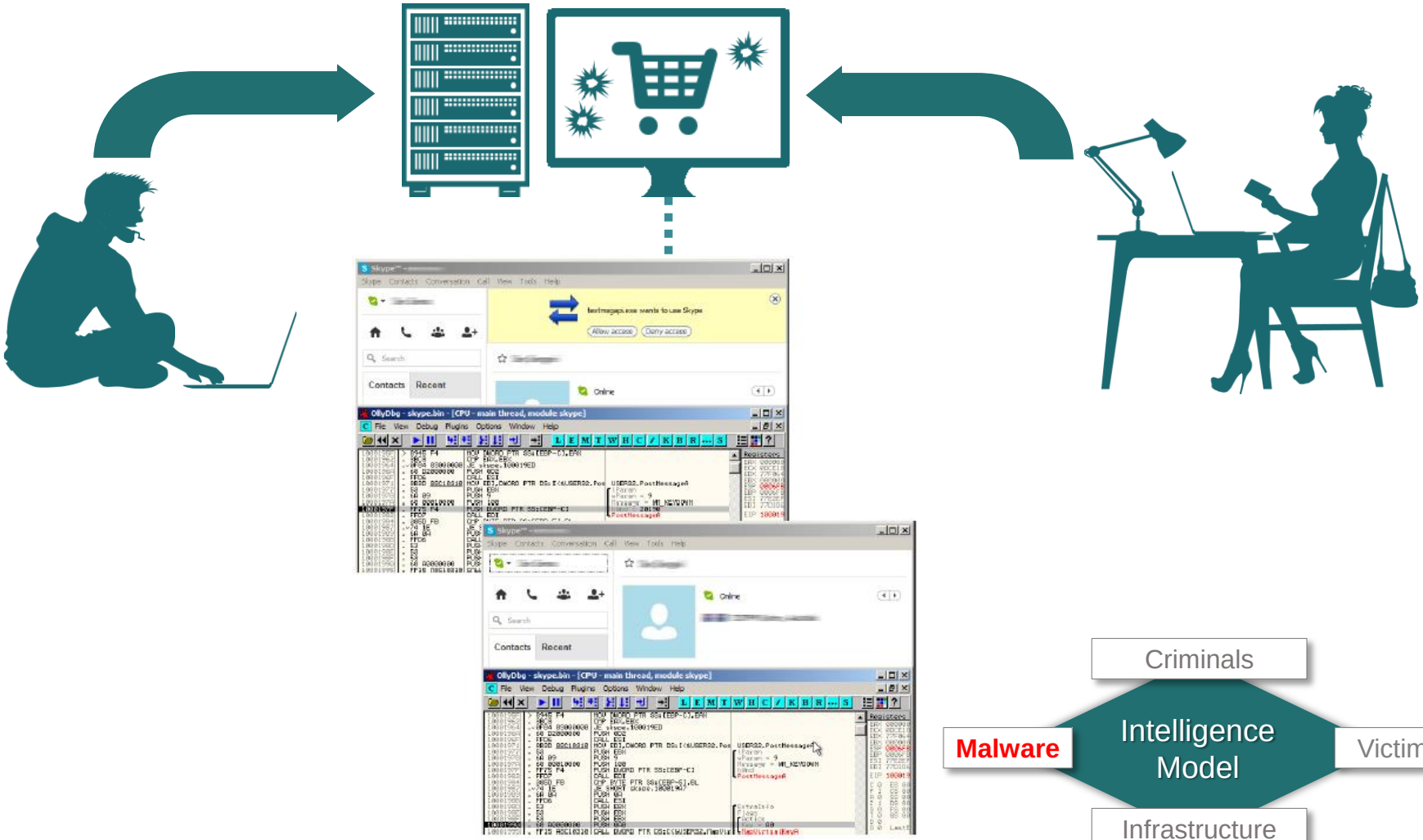
HOW IT WORKS – MALWARE AUTOMATION





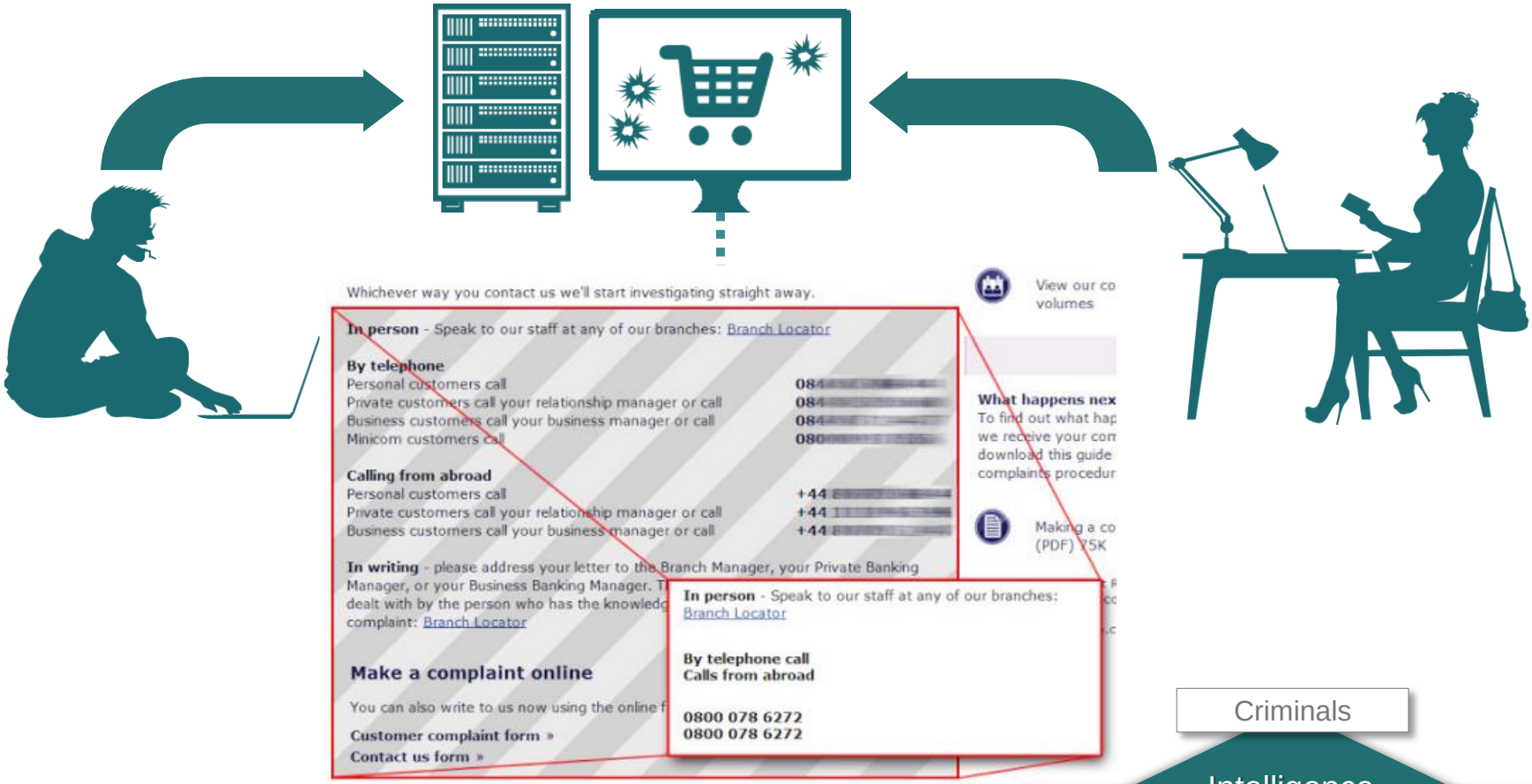
BAE SYSTEMS
INSPIRED WORK

HOW IT WORKS – MALWARE AUTOMATION



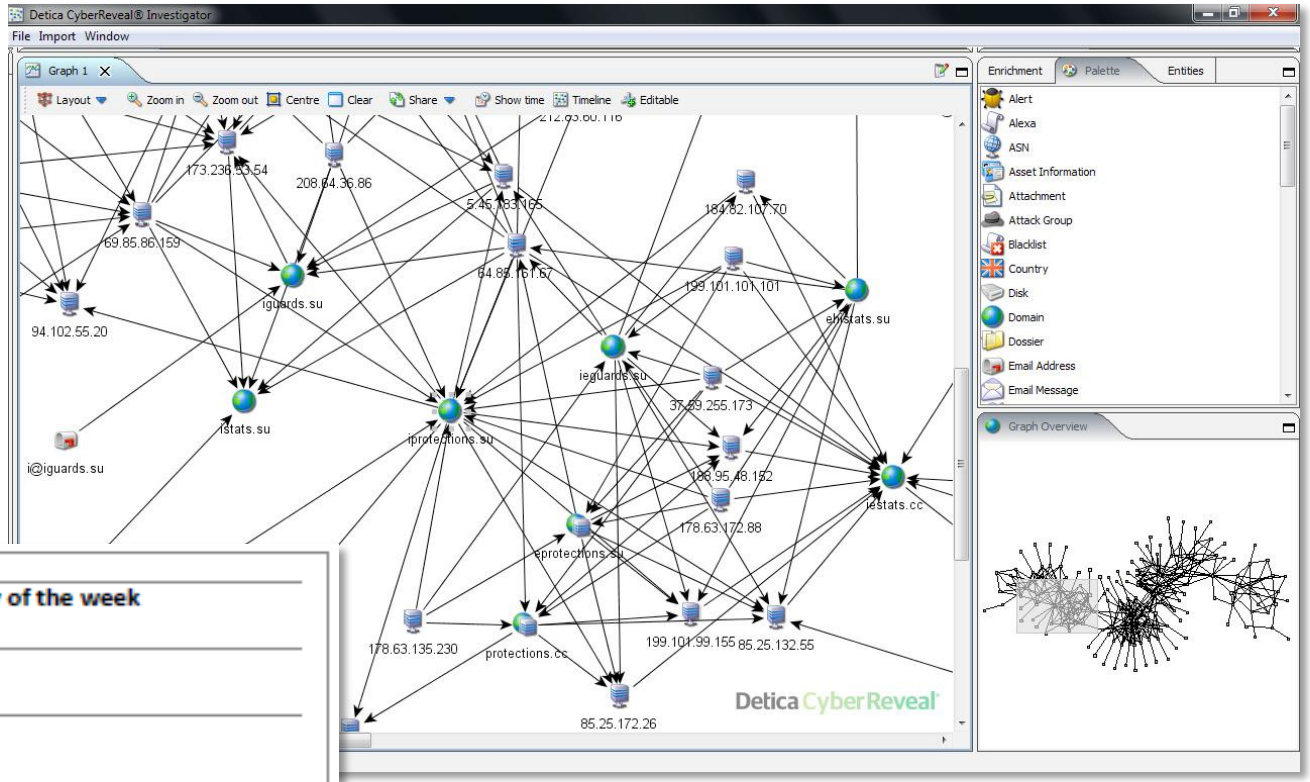
BAE SYSTEMS
INSPIRED WORK

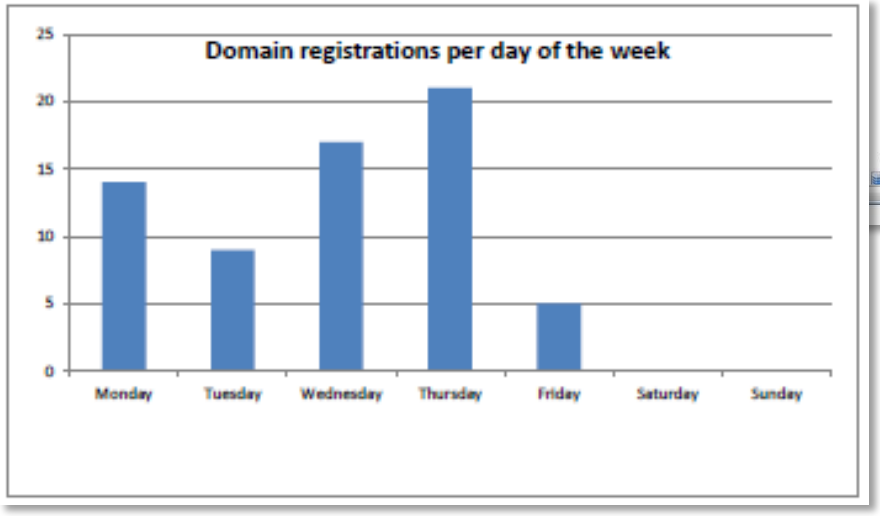
HOW IT WORKS – BANKING WEBSITE MODIFICATION

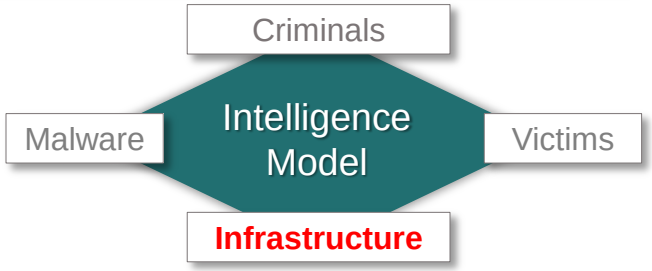


BAE SYSTEMS
INSPIRED WORK

FINDING THE C2 INFRASTRUCTURE

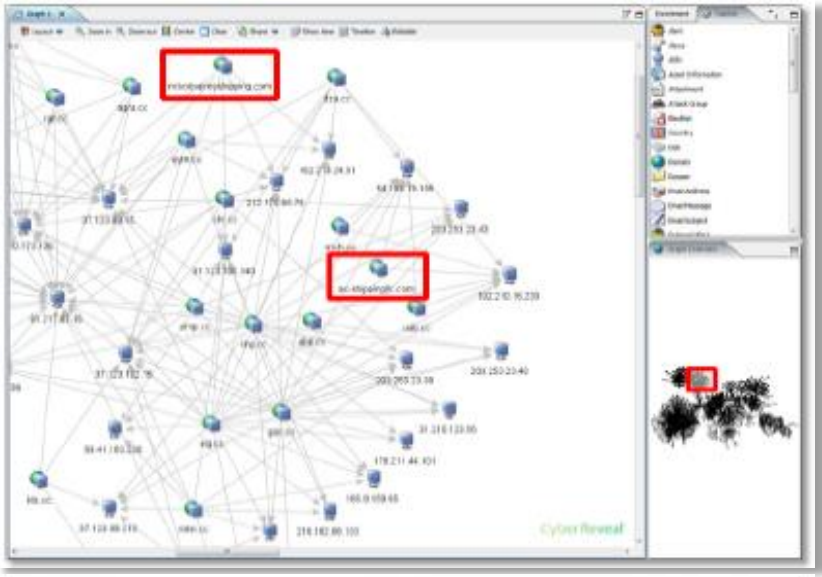


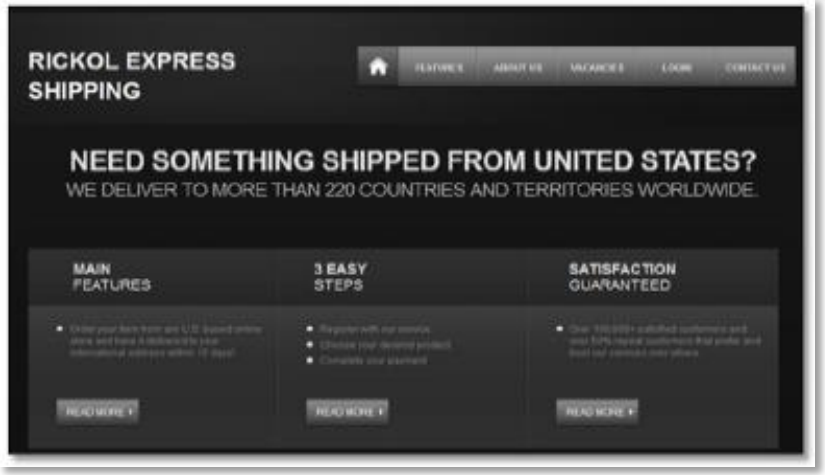


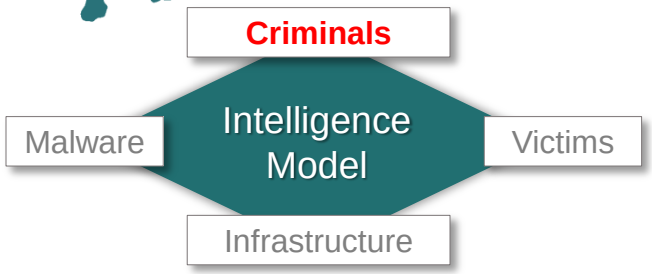


BAE SYSTEMS
INSPIRED WORK

LINKS TO MULE RECRUITMENT

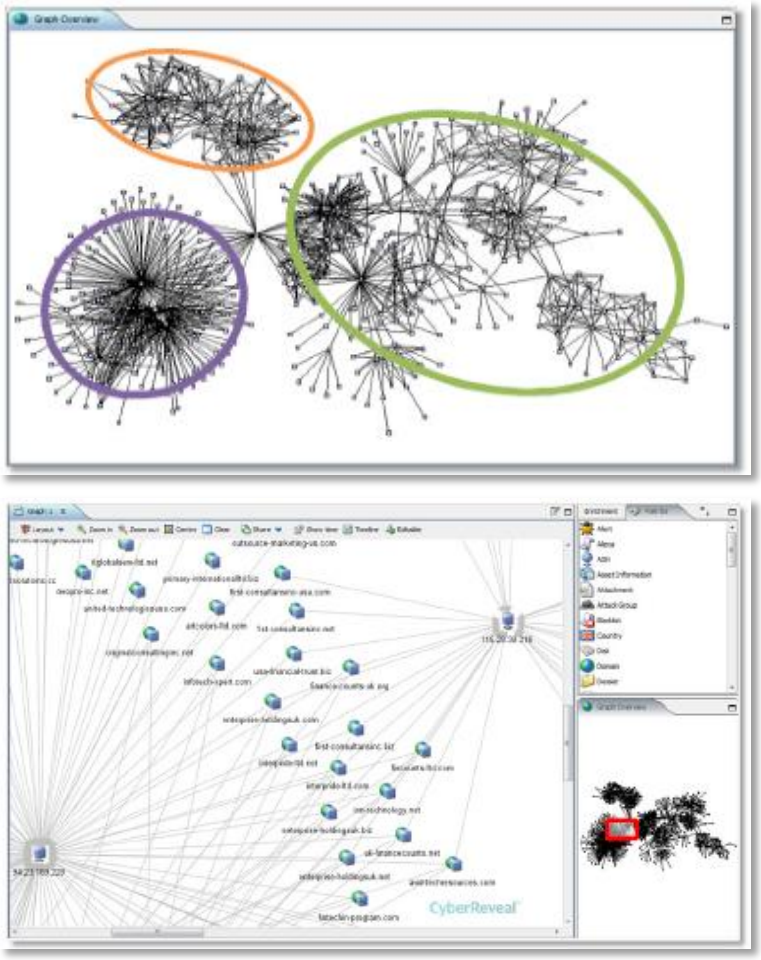


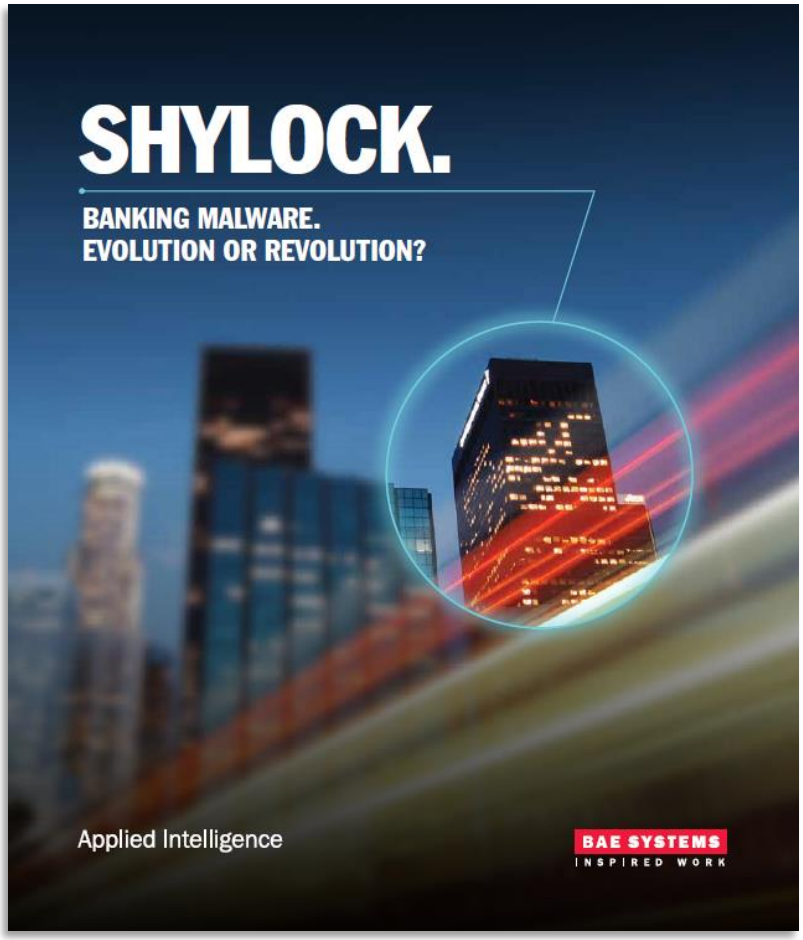




BAE SYSTEMS
INSPIRED WORK

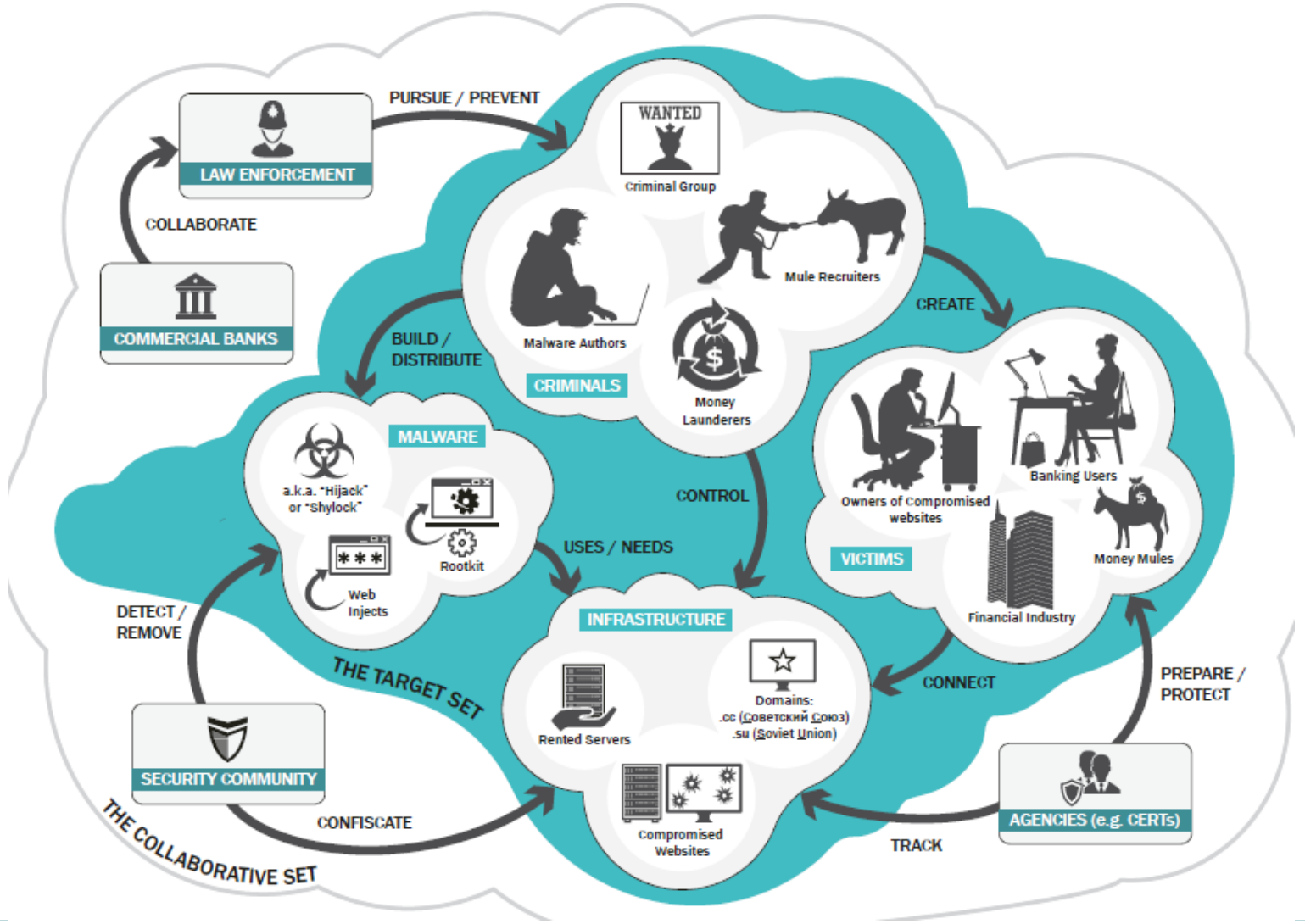
PUTTING IT ALL TOGETHER





BAE SYSTEMS
INSPIRED WORK

THE SHYLOCK TAKEDOWN – INTELLIGENCE INTO ACTION



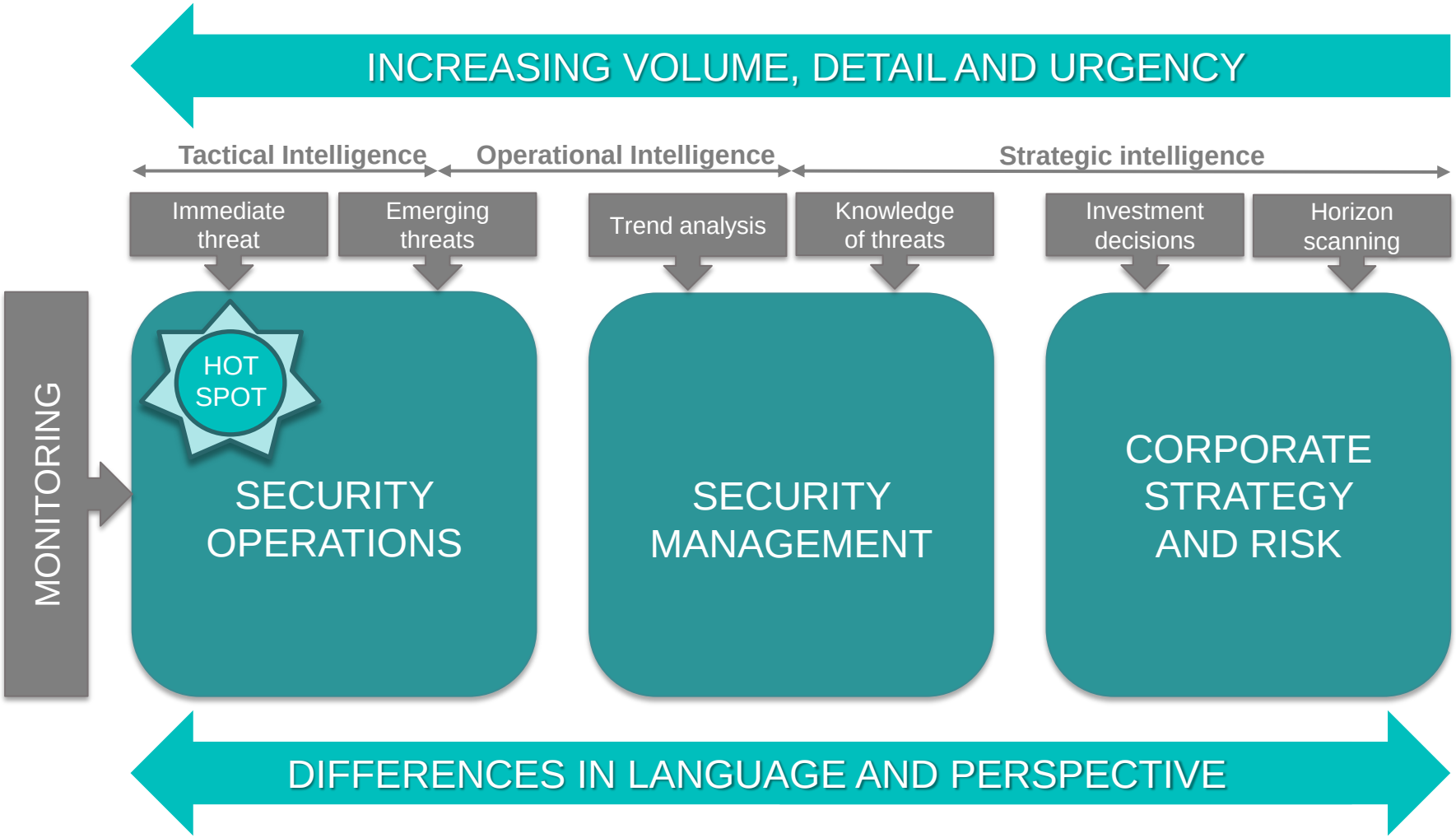
BAE SYSTEMS
INSPIRED WORK

Making threat intelligence work

Turning people, process and technology into action

BAE SYSTEMS
INSPIRED WORK

FORMS OF THREAT INTELLIGENCE

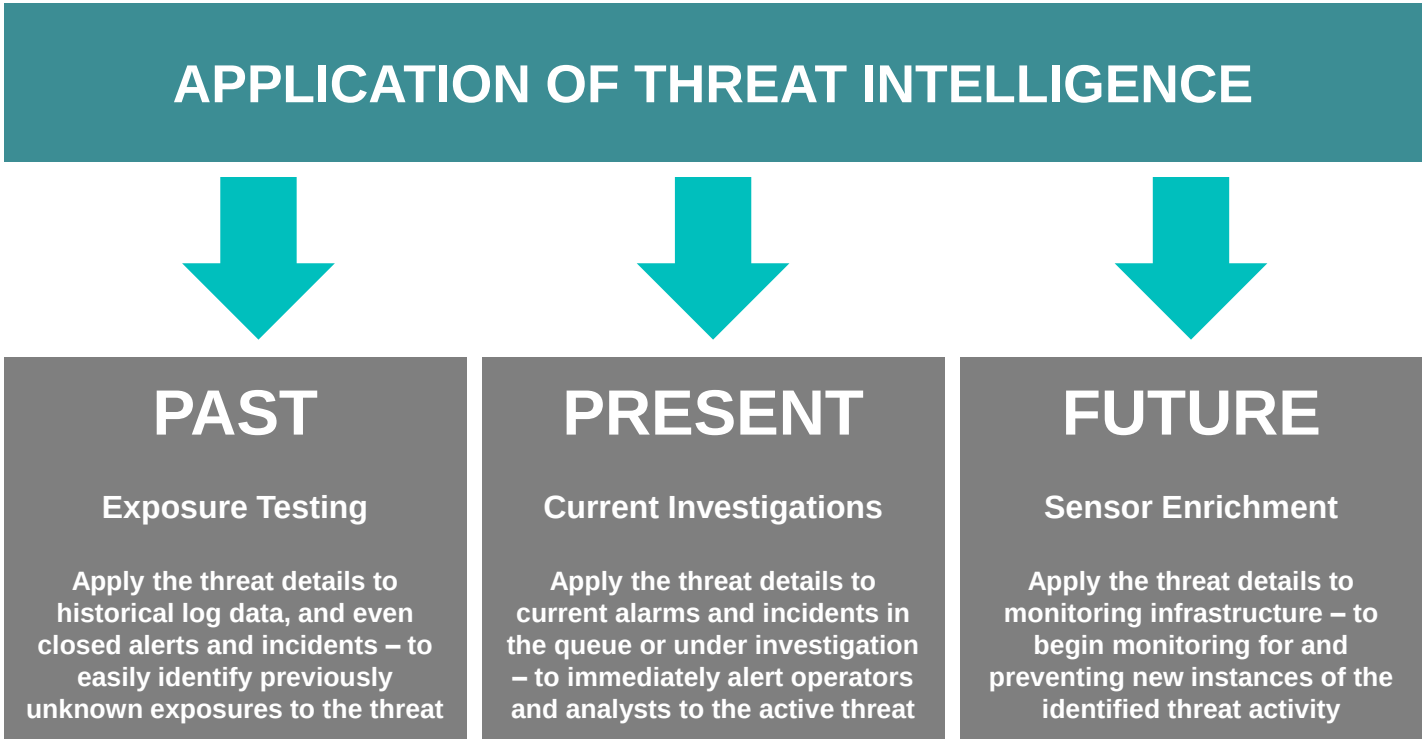


BAE SYSTEMS
INSPIRED WORK

MAKING THREAT INTELLIGENCE WORK – PEOPLE

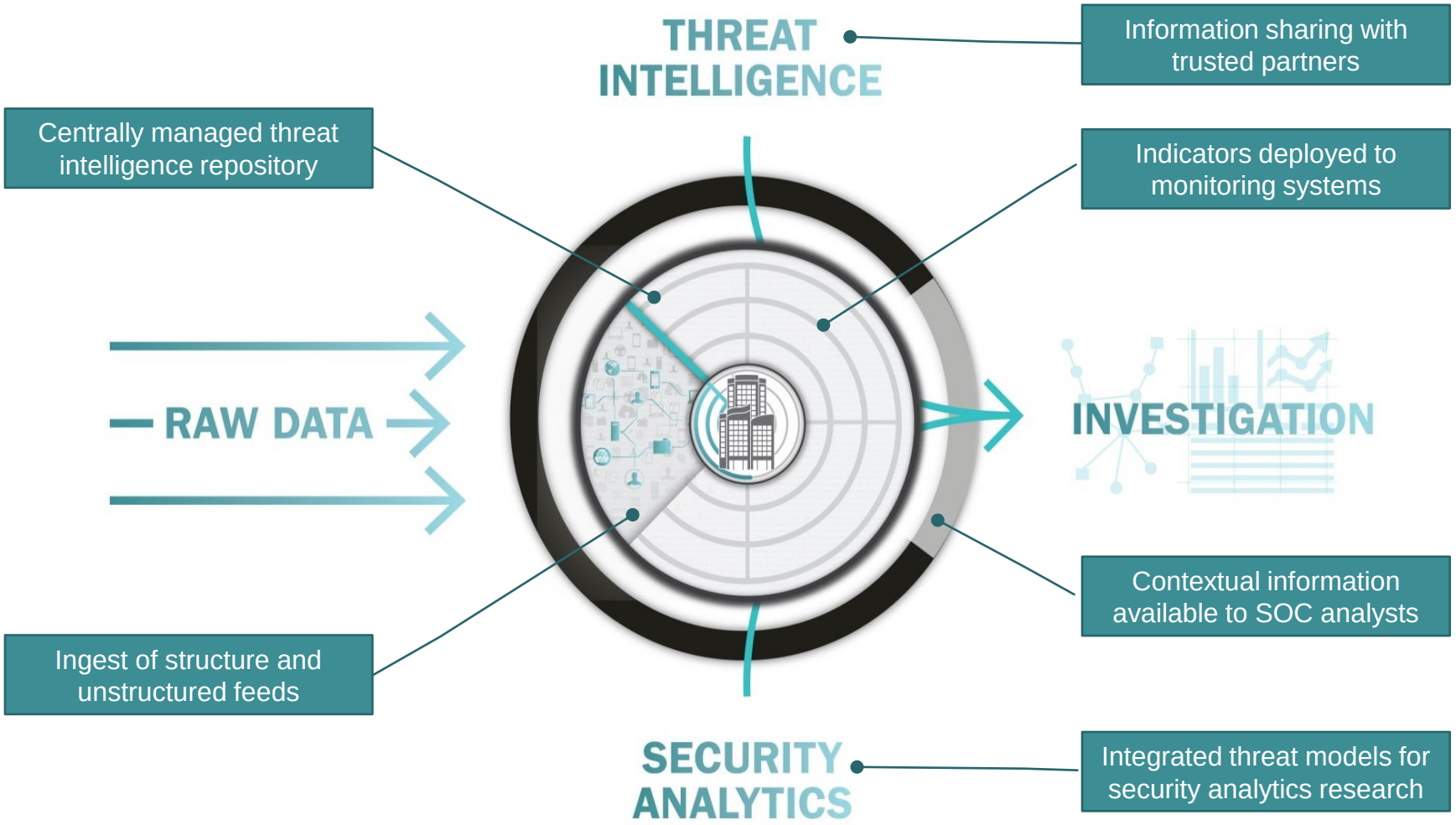
BAE SYSTEMS
INSPIRED WORK

MAKING THREAT INTELLIGENCE WORK – ACTION



BAE SYSTEMS
INSPIRED WORK

…IN A SECURITY OPERATIONS ENVIRONMENT



James Calder

Client Services Manager, Singapore

BAE Systems Applied Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur, 50450
Malaysia

T: +60 (3) 2191 3000
F: +60 (3)1483 816144

www.twitter.com/baesystems_ai

www.linkedin.com/company/baesystemsai