CGI

Experience the commitment®

Cyber Security Center

CGI Cybersecurity

Jan Mickos
Vice President, Cybersecurity

🐦 JMickos #CyberSecurity #Kyberturvallisuus
www.cgi.com/cyber
www.cgi.fi/kyber

CGI in Cybersecurity

CGI

35+ years of experience in information security across government and commercial sectors.

3 accredited test facilities Canada, US and UK

1700 cyber professionals globally

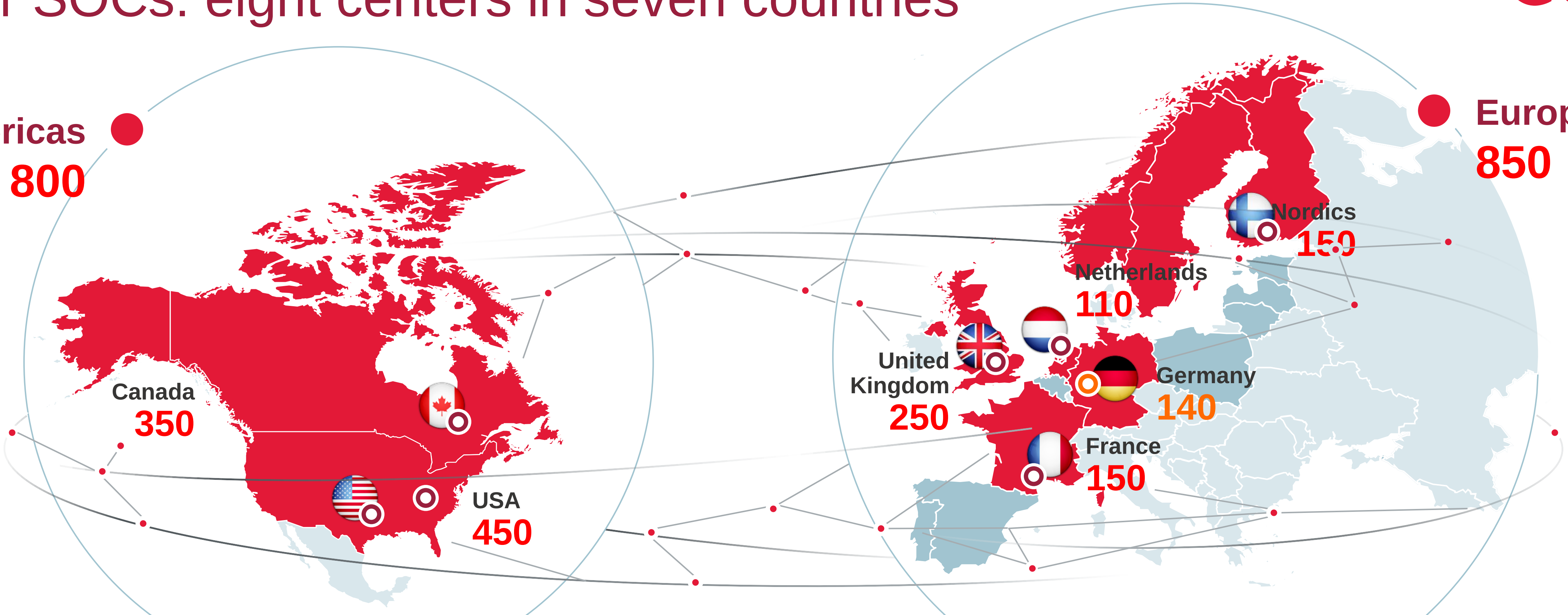
8 Security Operations Centers globally

Independence in technology, delivery, service model and operations

Tested and proven in some of the world's most sensitive and complex environments

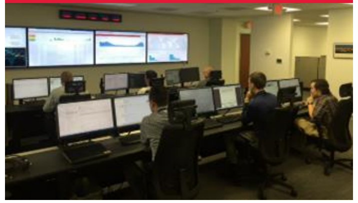
We help businesses and government clients to assess the risk, protect the business and operate with confidence in the digital world

Our SOCs: eight centers in seven countries

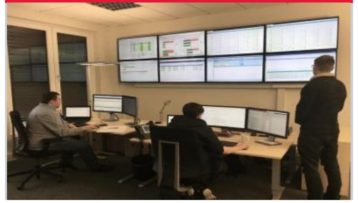


Canada

US West



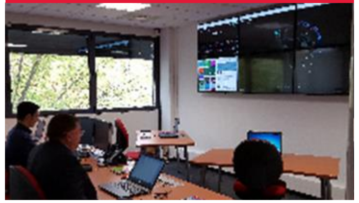
Germany

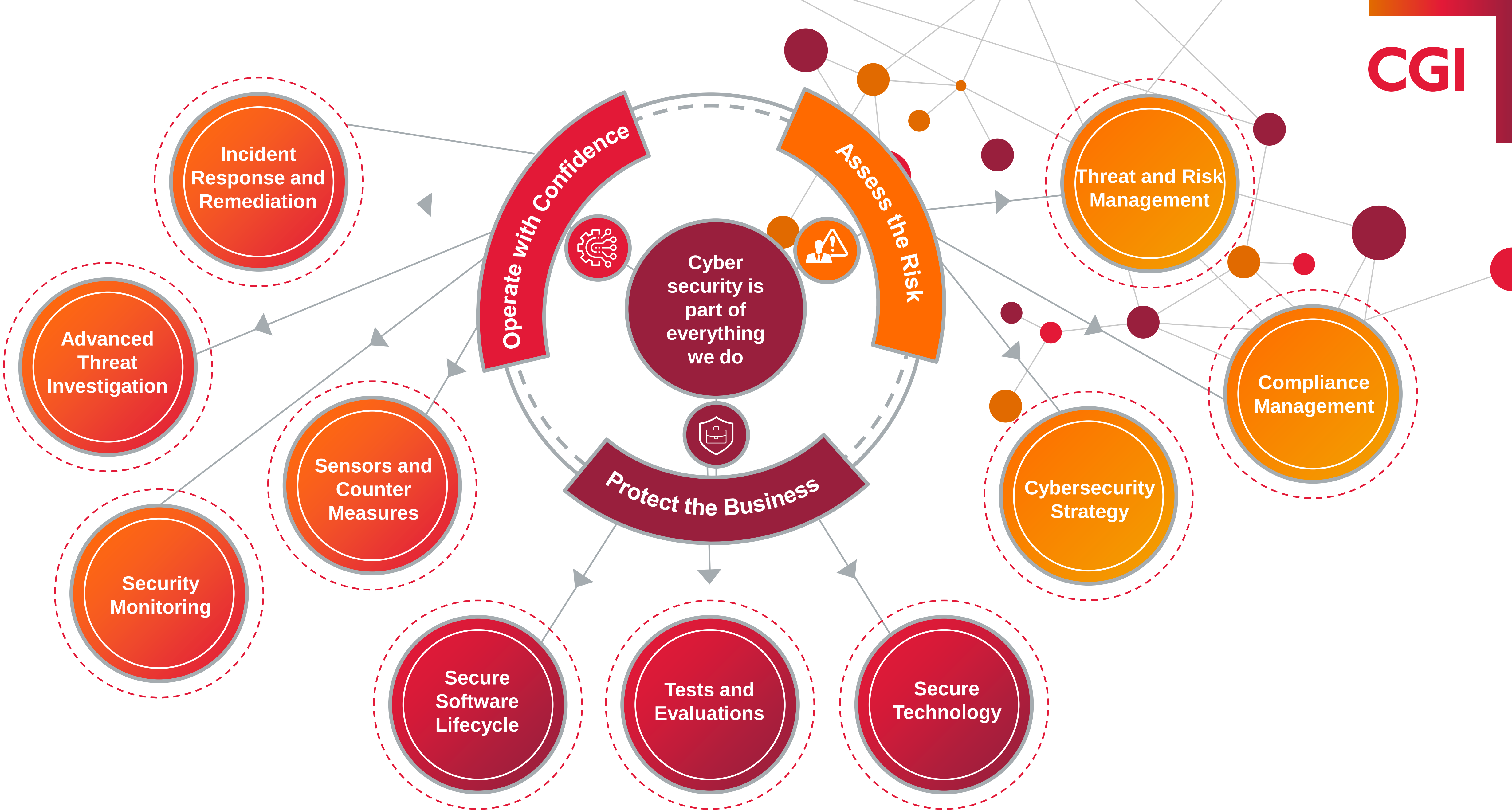


Nordics

UK

France





Cyber security is part of everything we do

Operate with Confidence

Incident Response and Remediation

Advanced Threat Investigation

Sensors and Counter Measures

Security Monitoring

Assess the Risk

Threat and Risk Management

Compliance Management

Cybersecurity Strategy

Protect the Business

Secure Software Lifecycle

Tests and Evaluations

Secure Technology

The importance of ”Cyber hygiene”

>95%

of all cyber threats is commodity malware and phishing

83%

of incidents happen because of bad cyber hygiene

…brush your teeth and wash your hands after flushing

Modern Cybersecurity Operations

CGI

→ The modern cyber security program must reflect an elevation in strategic position and intent within the business. It must also move beyond a traditional “defensive” mindset to improved detection and response capability.

→ We must move from a compliance-driven approach to a risk-driven approach – build a proactive capability based on a specific risk profile and not on a generic set of compliance standards.

IDENTIFY

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

PREVENT

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

STRATEGIC ELEVATION (POLICY, GOVERNANCE, TRAINING & AWARENESS….)

On the other hand…

CGI

40%

of cyber campaigns targeted manufacturing and service companies

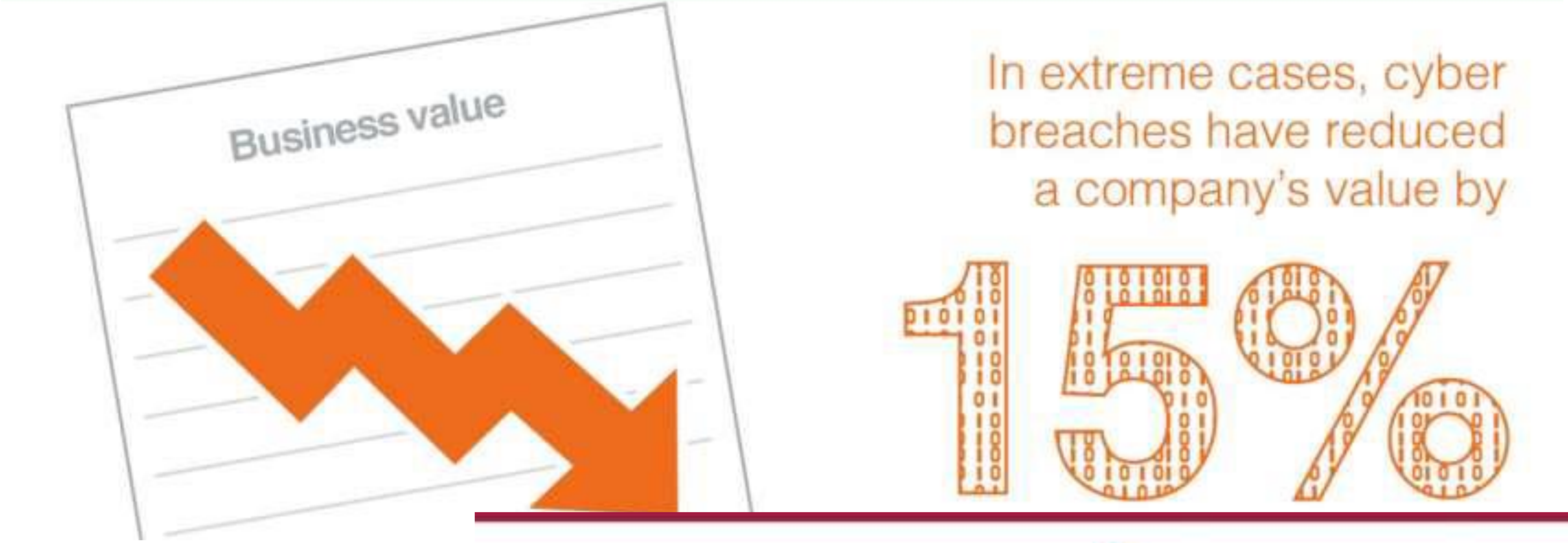
80%

of all breaches originate from the supply chain

90%

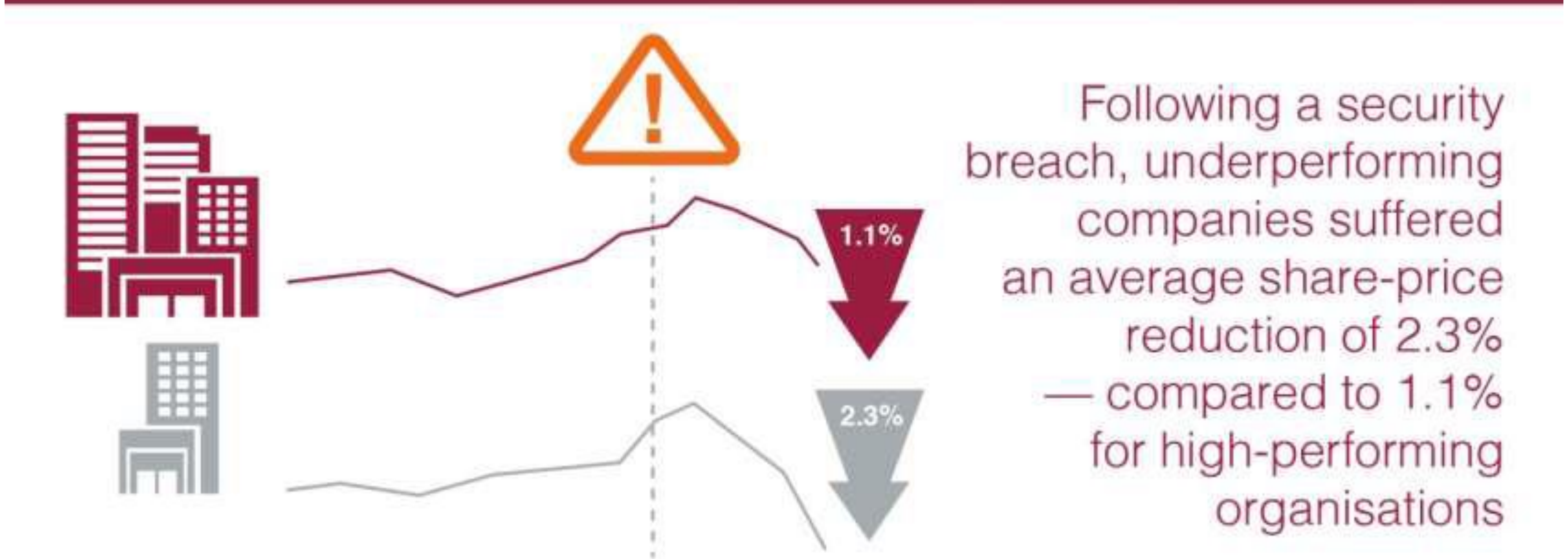
of most serious attacks against critical infra is nation state sponsored

Impact of a cyber breach



In extreme cases, cyber breaches have reduced a company's value by

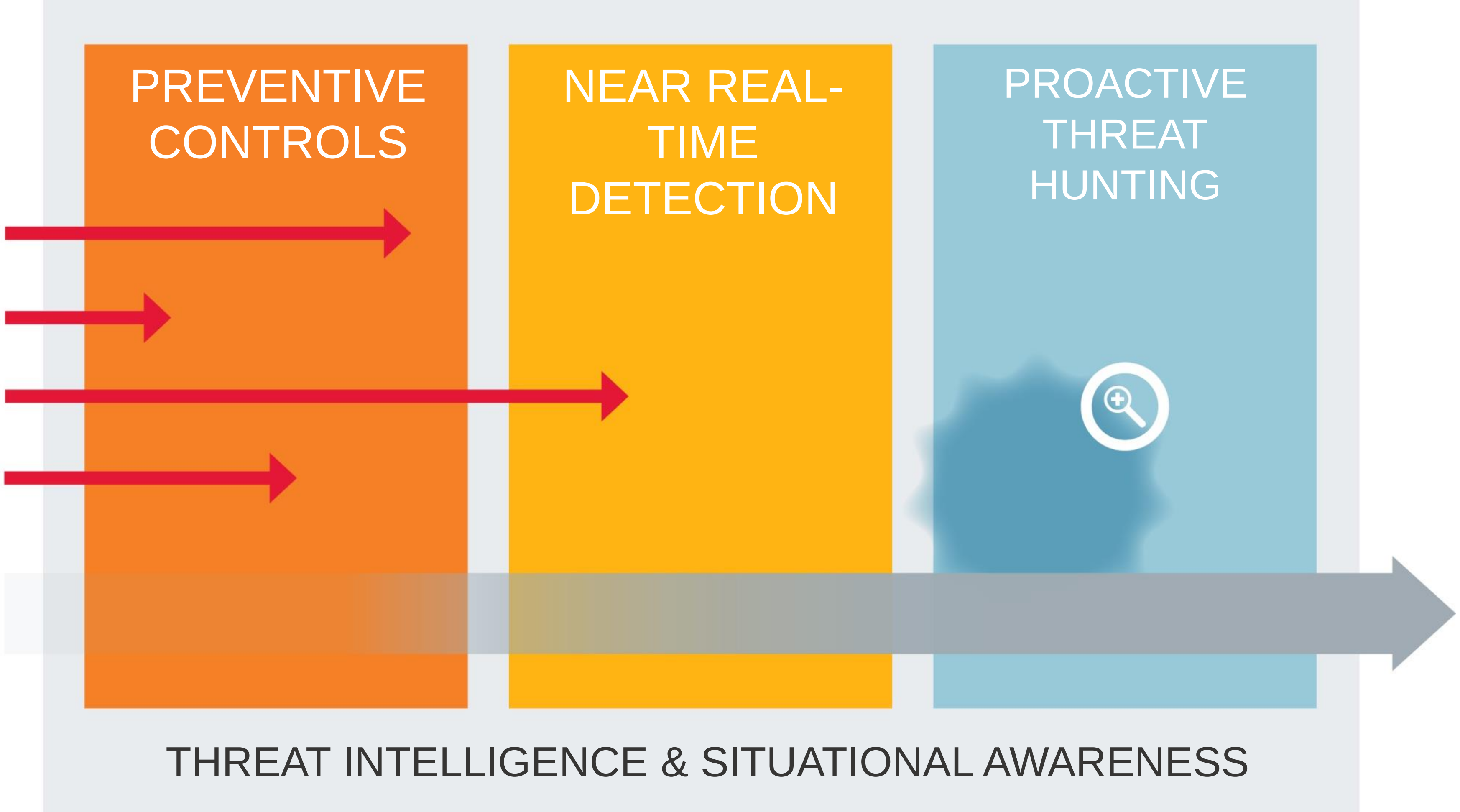
15%



Following a security breach, underperforming companies suffered an average share-price reduction of 2.3% — compared to 1.1% for high-performing organisations

Source:
The Cyber-Value Connection,
CGI and Oxford Economic

The Security Operations we need today



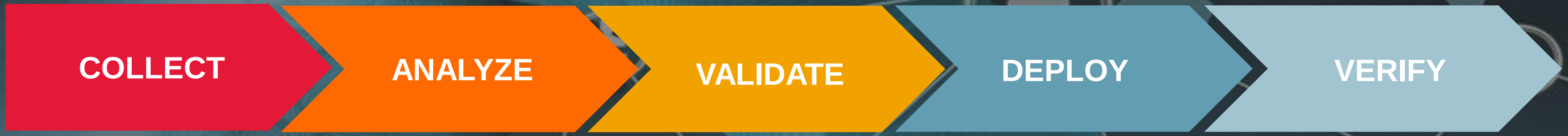
PREVENTIVE CONTROLS

NEAR REAL-TIME DETECTION

PROACTIVE THREAT HUNTING

THREAT INTELLIGENCE & SITUATIONAL AWARENESS

Threat Intelligence Analysis



GATHER AND ANALYZE

- All-source
- STIX / TAXII and Proprietary
- Machine / Human readable
- IoA / IoC / TTP
- Behavioral or Static

SECURITY OPERATIONS

- Select Intel based on Objective and Reputation
- Validate and Test (Hunt Search)
- Contextualize
- Feed to SIEM and IRP
- Develop Use-Cases

VALIDATION, VERIFICATION AND FEEDBACK LOOP

- Conduct Triage and Incident Analysis
- Verify Intel
- Feedback on source and item reputation

OUR APPROACH

We collect Threat Intelligence from a wide range of sources

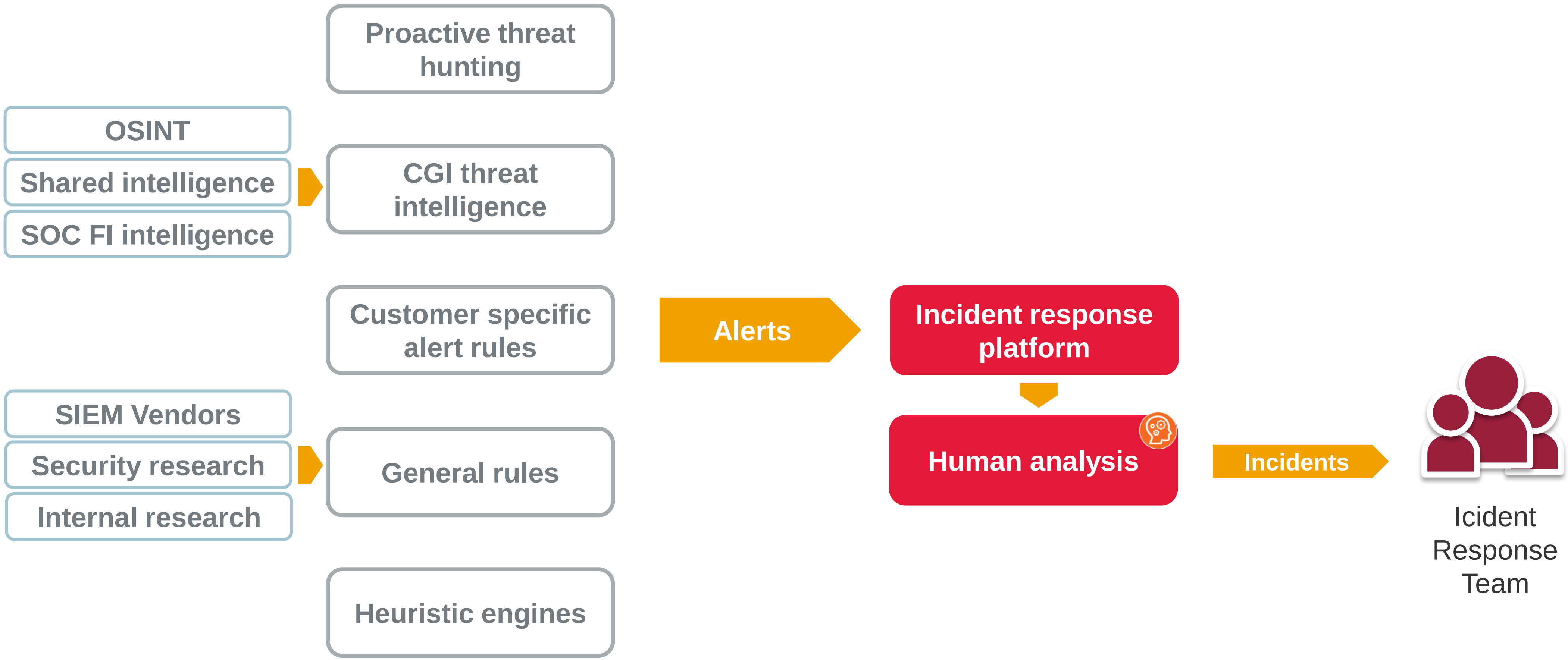
1. Open Source Threat Feeds
2. Partner and Vendor Threat Feeds
3. Commercial Threat Feeds
4. National Authorities Threat Feeds
5. CGI Internal Threat Feeds

The use of Threat Intel ranges from raising awareness of Analysts to automating responses based on known IoA’s and IoC’s.

We enhance the Intelligence based on feedback from Security and Hunting Operations, refining and creating new Threat Intelligence to share with our network of trusted partners.

CGI

Triage and analysis



Proactive threat hunting

OSINT

Shared intelligence

SOC FI intelligence

CGI threat intelligence

Customer specific alert rules

SIEM Vendors

Security research

Internal research

General rules

Heuristic engines

Alerts

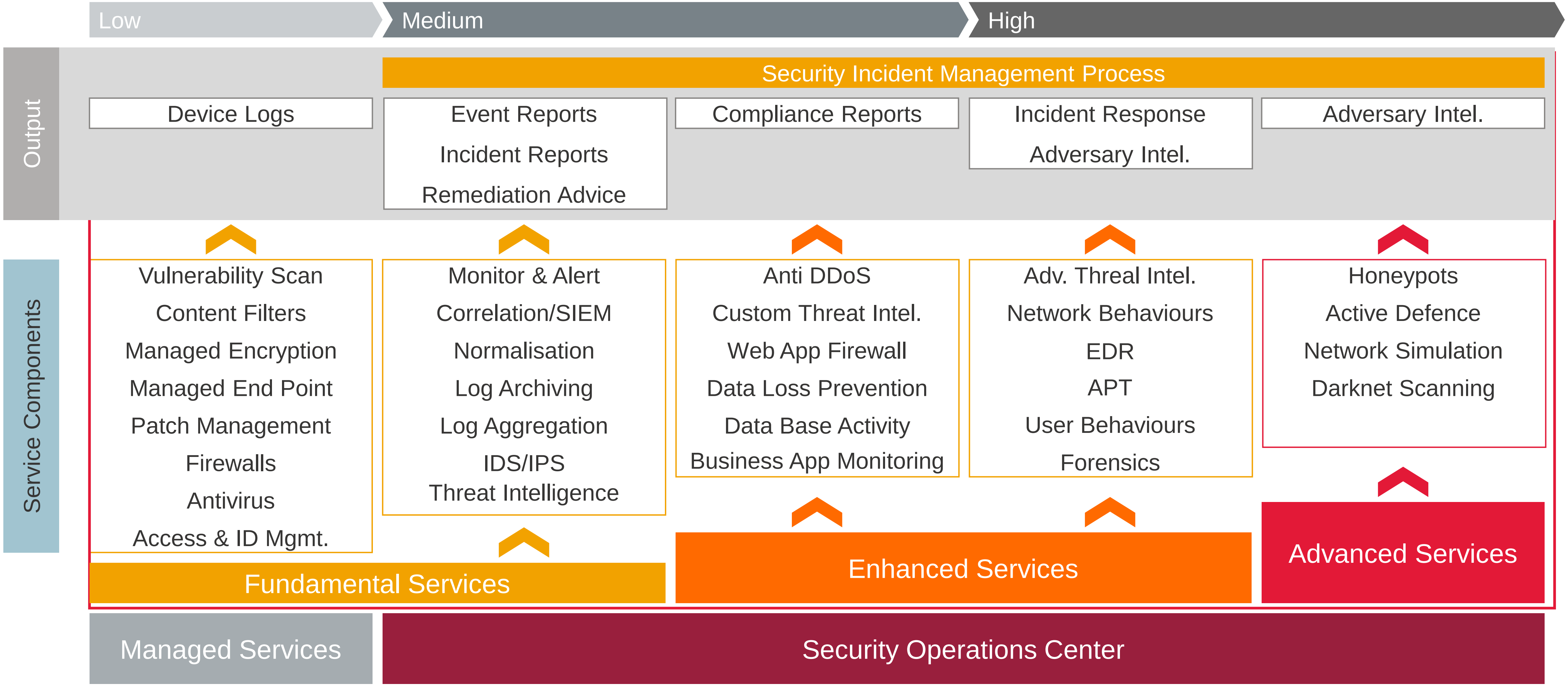
Incident response platform

Human analysis

Incidents

Icident Response Team

CGI‘s modern cybersecurity program – maturity/evolution view



Low

Medium

High

Output

Security Incident Management Process

Device Logs

Event Reports
Incident Reports
Remediation Advice

Compliance Reports

Incident Response
Adversary Intel.

Adversary Intel.

Service Components

Vulnerability Scan
Content Filters
Managed Encryption
Managed End Point
Patch Management
Firewalls
Antivirus
Access & ID Mgmt.

Monitor & Alert
Correlation/SIEM
Normalisation
Log Archiving
Log Aggregation
IDS/IPS
Threat Intelligence

Anti DDoS
Custom Threat Intel.
Web App Firewall
Data Loss Prevention
Data Base Activity
Business App Monitoring

Adv. Threal Intel.
Network Behaviours
EDR
APT
User Behaviours
Forensics

Honeypots
Active Defence
Network Simulation
Darknet Scanning

Fundamental Services

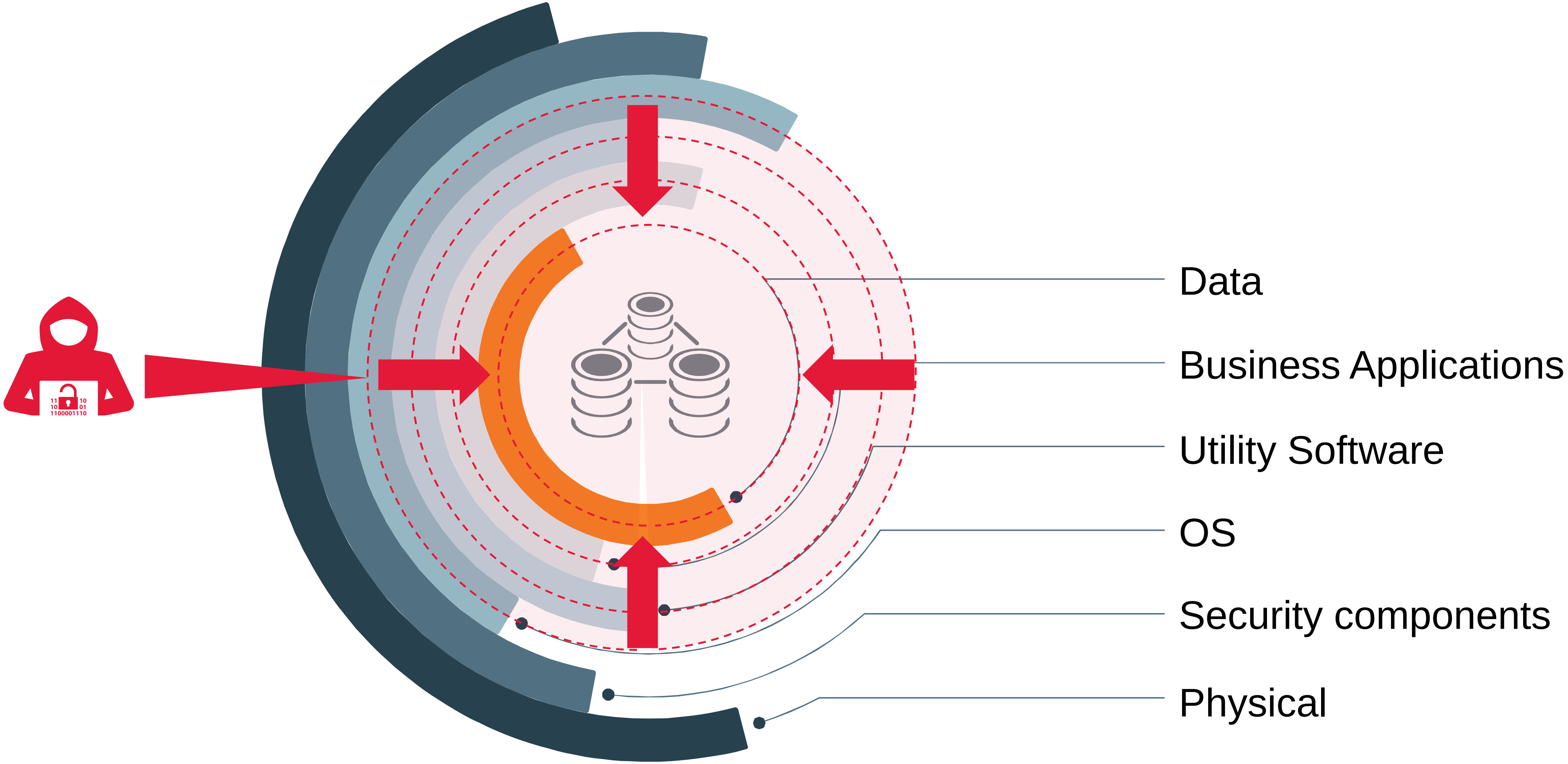
Enhanced Services

Advanced Services

Managed Services

Security Operations Center

Business Application Security Monitoring



Data

Business Applications

Utility Software

OS

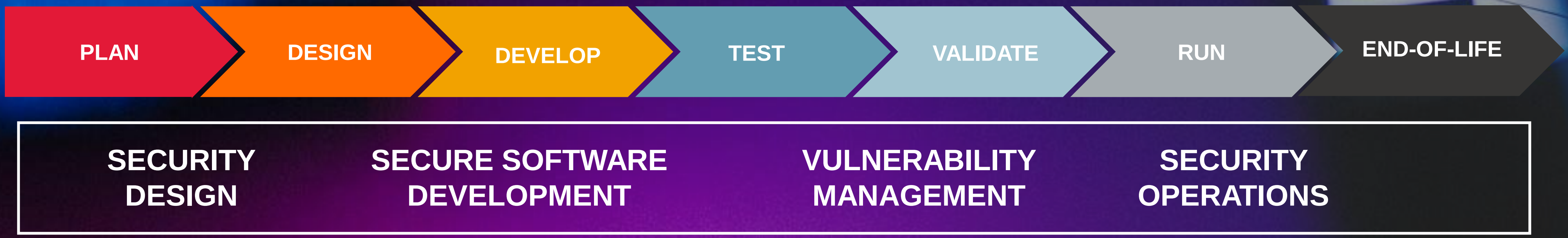
Security components

Physical

We secure your digital business

We have the people, tools and processes to protect your digital business by assessing the risks and helping you develop secure digital services, while continuously monitoring and protecting against existing and emerging cybersecurity threats throughout the service lifecycle.

SECURITY LIFECYCLE PROCESS



PLAN

DESIGN

DEVELOP

TEST

VALIDATE

RUN

END-OF-LIFE

SECURITY DESIGN

SECURE SOFTWARE DEVELOPMENT

VULNERABILITY MANAGEMENT

SECURITY OPERATIONS

Helsinki SOC
Facility Security

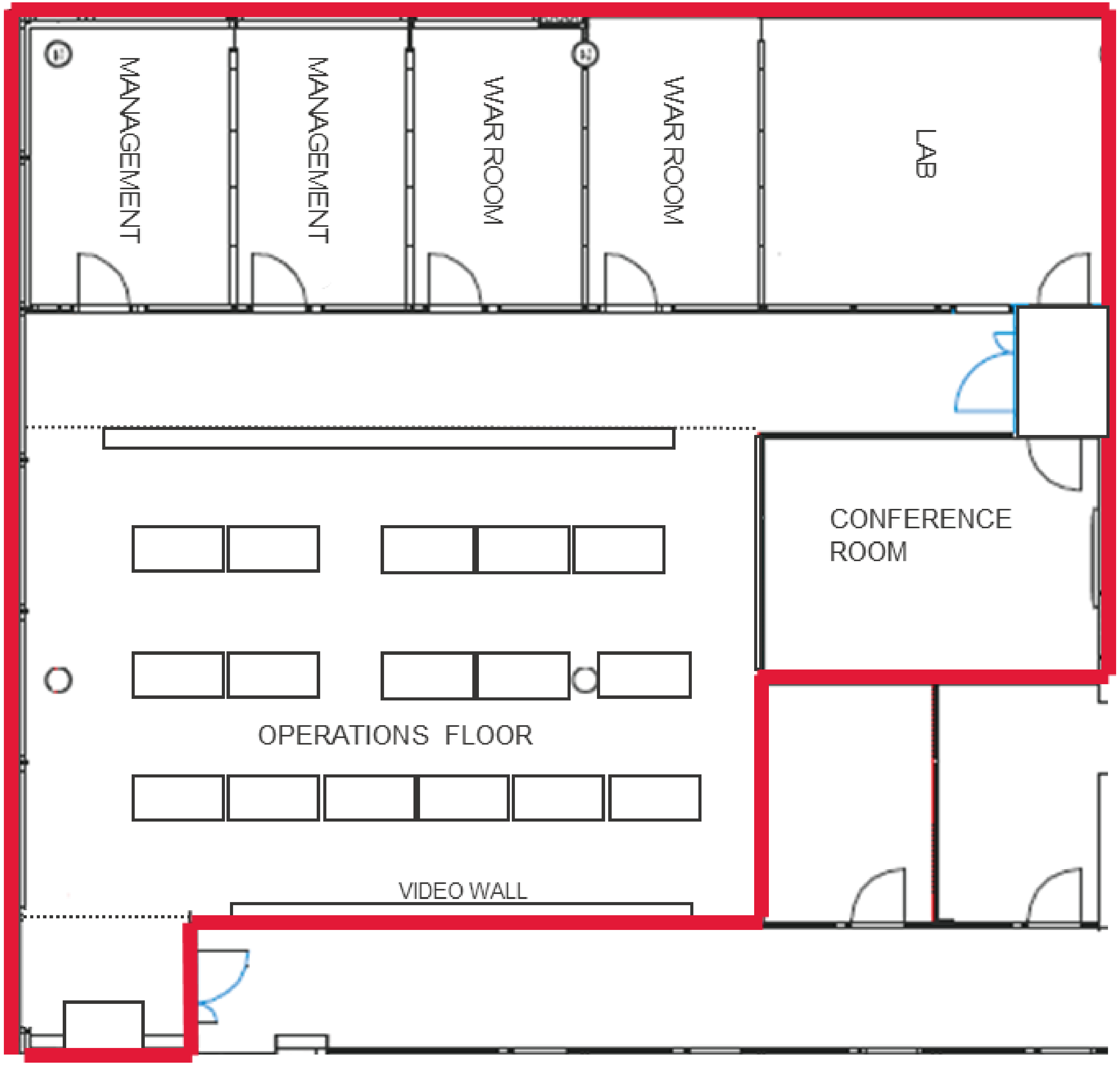
CGI ESMF Facility Security Standard

- High Security Area

International Facility Security Clearance (FSC) issued by the Finnish NSA

- Physical structure
- Personell security
- Network segregation
- Administrative security controls

All personell Finnish citizens and hold a government security clearence



We secure your digital business.

Jan Mickos

@JMickos #Kyberturvallisuus #CyberSecurity

www.cgi.fi/kyber
www.cgi.com/cyber

CGI