Thales Cybersecurity for Transport Systems

OPEN

www.thalesgroup.com

SUMMARY

- ✓ Introduction (M. Romairone)
- ✓ Biology Inspired Cybersecurity (V. Di Massa)
- ✓ Cybersecurity Capabilities and Technologies (L. Ronchini)

SUMMARY

- ✓ **Introduction (M. Romairone)**
- ✓ Biology Inspired Cybersecurity (V. Di Massa)
- ✓ Cybersecurity Capabilities and Technologies (L. Ronchini)

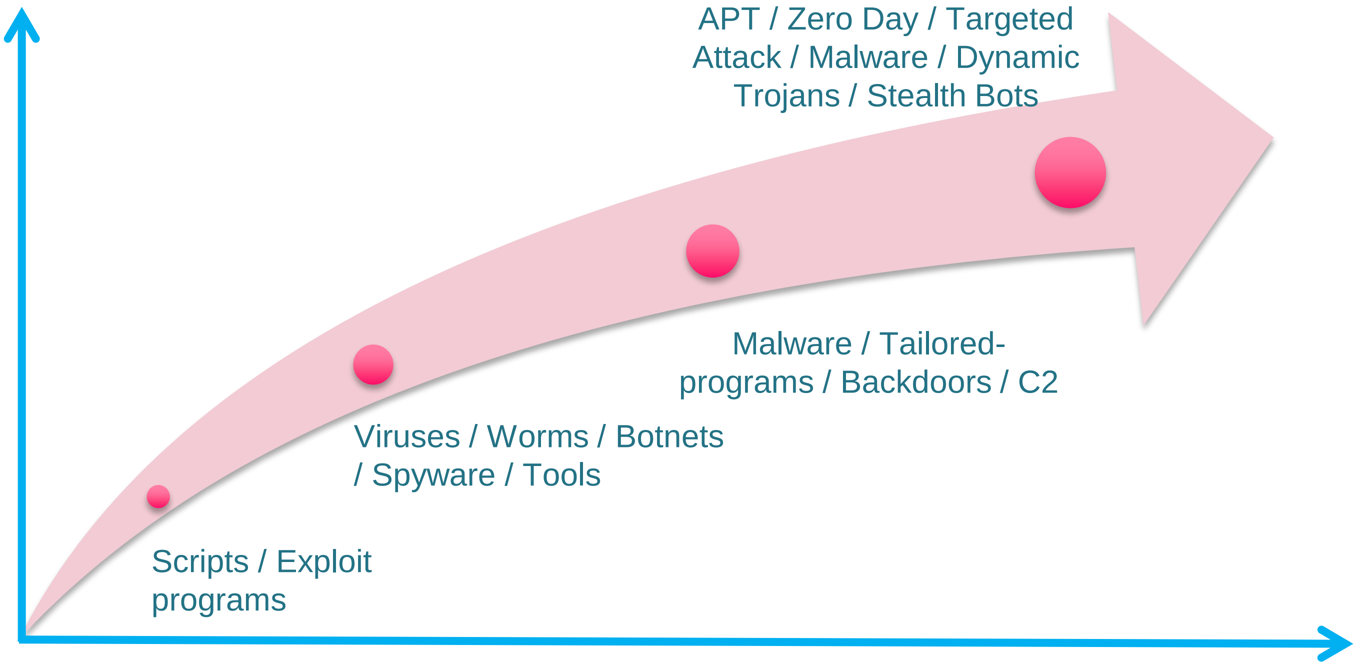
Cyber Security Landscape – Sophistication of Attacks

Critical infrastructure & Industrial Control Systems / Trade Secrets / IPs

Exfiltration of PII / PHI / Credit Card

Data Breaches / Availability

Defacement



APT / Zero Day / Targeted Attack / Malware / Dynamic Trojans / Stealth Bots

Malware / Tailored-programs / Backdoors / C2

Viruses / Worms / Botnets / Spyware / Tools

Scripts / Exploit programs

Script Kiddies

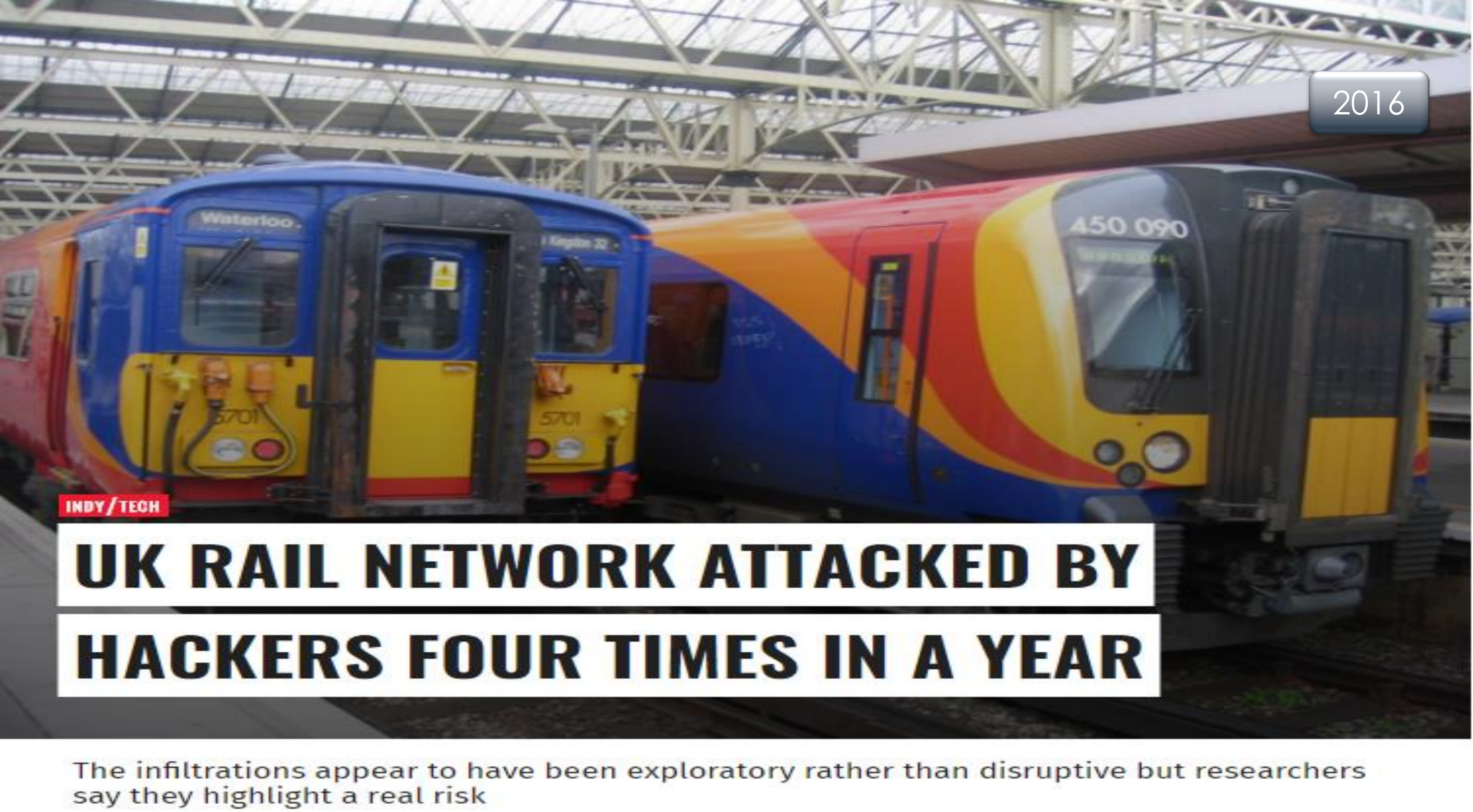
Hackers

Organized Criminals / Syndicates

State-sponsored Attacks

The chessboard for hackers has changed: evolving from private and individual targets, now to threatening government and national critical infrastructure on a global scale

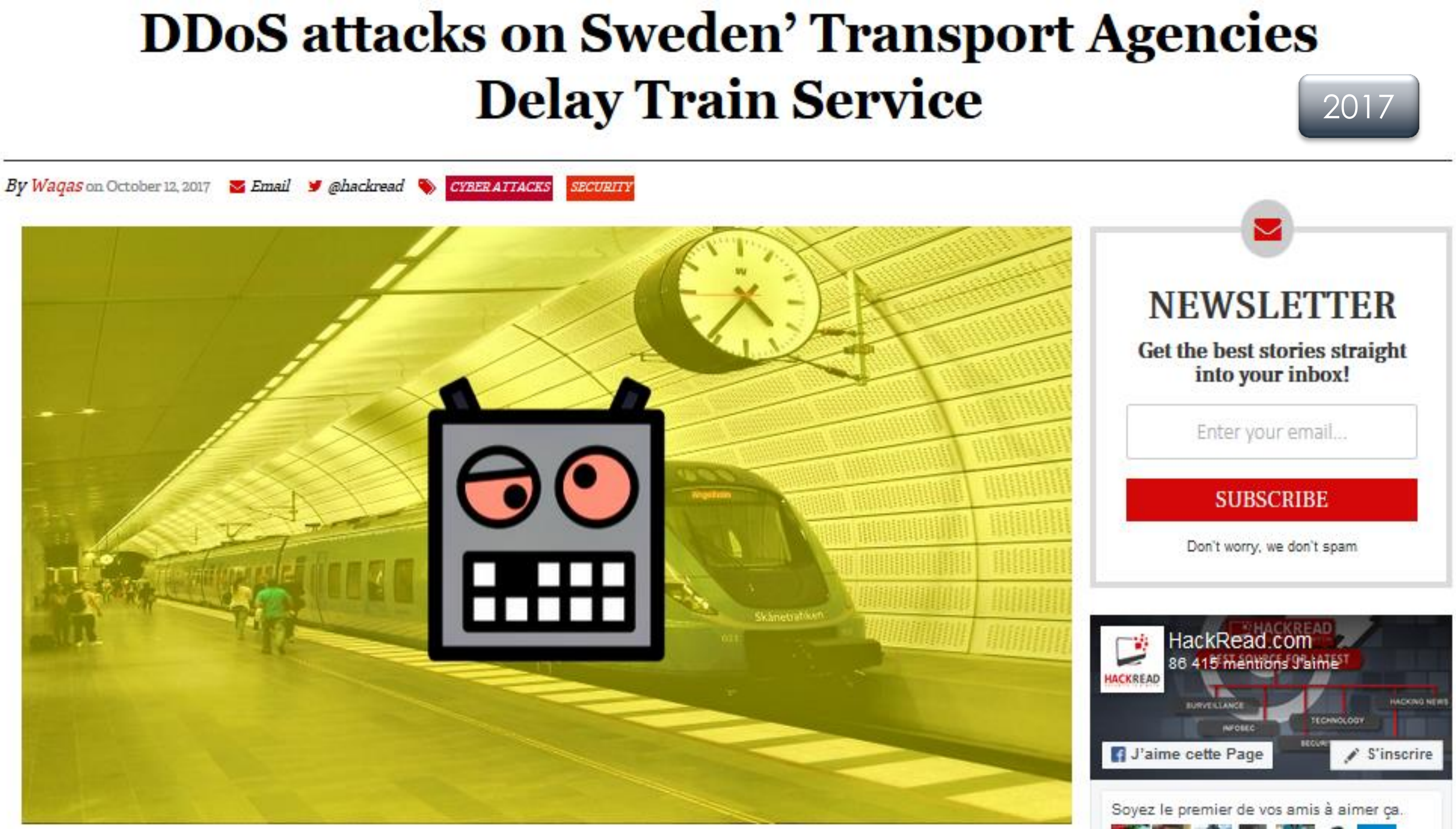
2016



INDY/TECH

UK RAIL NETWORK ATTACKED BY HACKERS FOUR TIMES IN A YEAR

The infiltrations appear to have been exploratory rather than disruptive but researchers say they highlight a real risk



DDoS attacks on Sweden' Transport Agencies Delay Train Service

2017

By *Waqas* on October 12, 2017 *Email* *@hackread* CYBER ATTACKS SECURITY

NEWSLETTER

Get the best stories straight into your inbox!

Enter your email...

SUBSCRIBE

Don't worry, we don't spam

HackRead.com
86 415 mentions J'aime

J'aime cette Page
S'inscrire

Soyez le premier de vos amis à aimer ça.

Risks of Critical Infrastructure & Security Steps

Risks of Critical Infrastructure

Complexity and interdependencies
- Highly interconnected -> increased dependencies -> increased vulnerabilities
- Complex detection

Heterogeneous
- Different protocols and adapted to business needs

Remote access required for maintenance
- Could be a risk

Not evolving
- Once deployed they are rarely updated

Built on standards without security mechanisms
- Operating system not patched
- Protocols

Industrial systems are not designed with cyber risks in mind

Business processes do not integrate this dimension
- Quality procedures (zero default)
- Safety procedures
- Maintenance procedures

Personnel is not trained neither informed

CAUTION

SAFETY CULTURE IN ACTION

8 Security Steps for a secure Critical Infrastructure

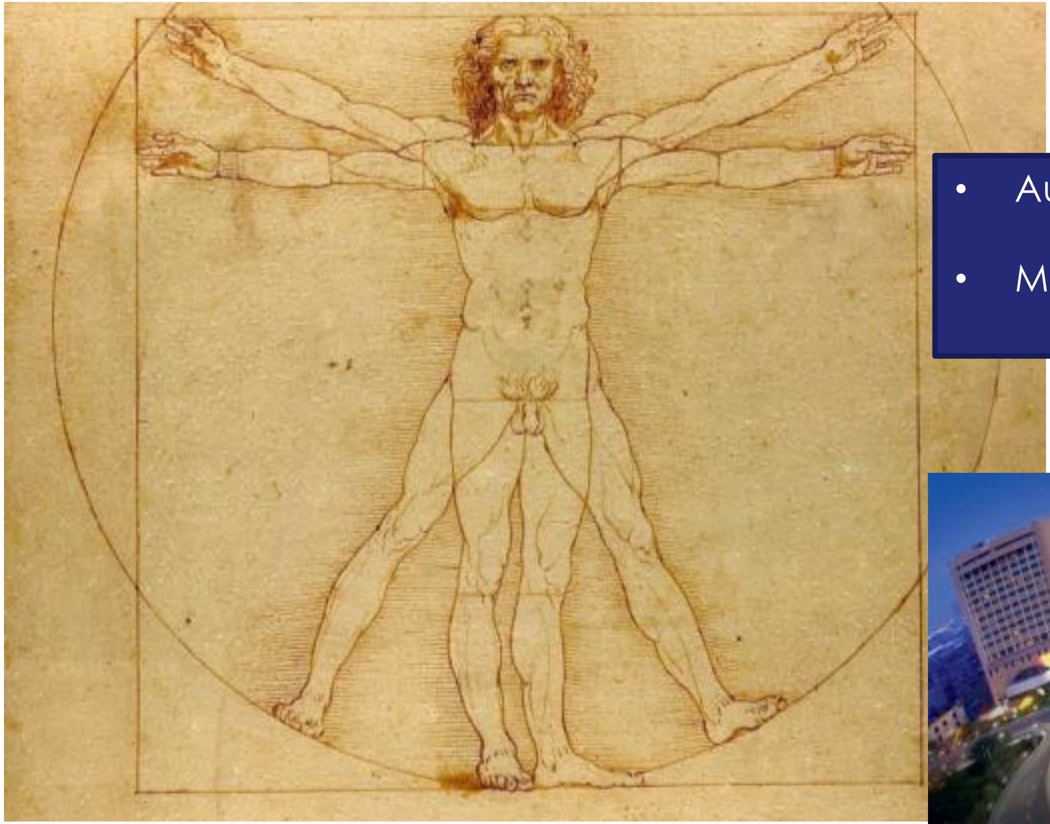
- ✓ **Establish Cybersecurity Design Principles**
- ✓ **Create a Strong Perimeter**
- ✓ **Deply System Security and Detection / Recovery**
- ✓ **Meet Cybersecurity Standard**
- ✓ **Embed Cybersecurity in the Development Lifecycle**
- ✓ **Conducting Risk Assessments and Penetration Testing**
- ✓ **Mantain Operational Conditions**
- ✓ **Mandate Safety Protection**

OPEN

SUMMARY

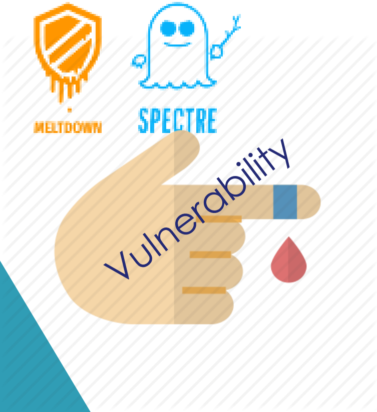
- ✓ Introduction (M. Romairone)
- ✓ **Biology Inspired Cybersecurity (V. Di Massa)**
- ✓ Cybersecurity Capabilities and Technologies (L. Ronchini)

Biology Inspired Cybersecurity

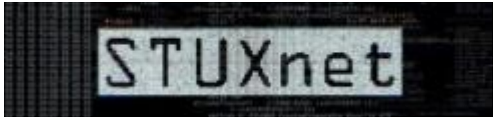


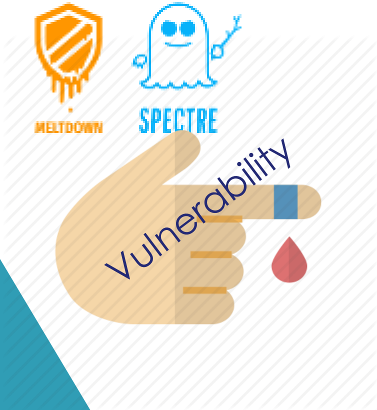
- Automatic defenses
  - Immune system / Secured by design
- Mindful response
  - Medicine / BlueTeam

Biology Inspired Cybersecurity

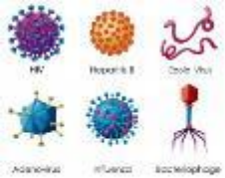


Biology Inspired Cybersecurity





Vulnerability



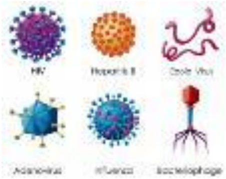
Attack vectors

Biology Inspired Cybersecurity

WannaCry
Ransomware Attack

STUXnet

Vulnerability



Attack vectors

Immune system

paloalto
NETWORKS

THALES

NVD

Vormetric
Data Security™

technology

Automatic Responses

OPEN

Biology Inspired Cybersecurity

Mindful responses

processes

ALIEN VAULT

Radar

Control Center CSOC

THALES

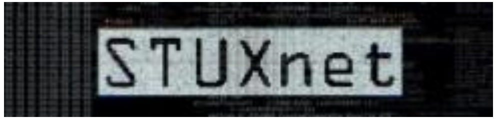
Response Team

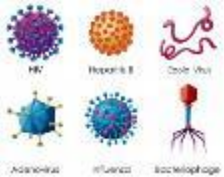
SIEM

MELTDOWN

SPECTRE

Vulnerability





Attack vectors

Immune system

paloalto NETWORKS

THALES

NVD

Vormetric Data Security™

technology

Automatic Responses

OPEN

THALES

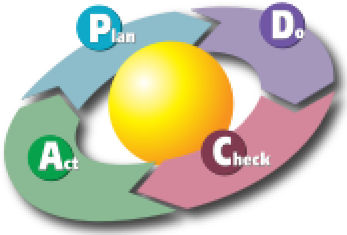
A Misconception About Security

Sterility lasts for only some time

The human body is not sterile

Cyber resilience

Antifragility



The immune system learns from examples

THALES Cybersecurity Expertise in Transport Systems

Critical information system operations and cybersecurity for **130 customers**

Thales helps to protect **world's banking transactions** and the Information Systems of largest global banks

Cybersecurity solutions for **9 of the top 10** internet giants

THALES and CYBERSECURITY

A team of **10,000** Software Developers and **5,000** critical IT and Cybersecurity Engineers

More than **50 countries,** including NATO nations, use our products and solutions

5 cybersecurity operation centres across the world (France, United Kingdom, The Netherlands, Canada, Hong Kong)

1 national cyberattack alert and response team (CERT-IST)

Certified red teams

THALES

Products for supervision

- Airport AOCC
- Rail TMS
- Urban rail & LRT – ITMS

Development of CSOCS

ISA IEC 62443

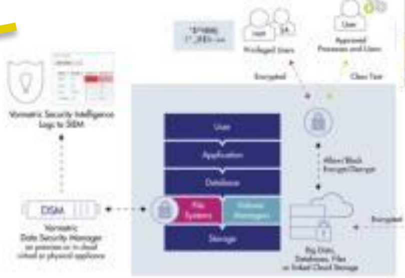
CertIST
Industrie Services Tertiaire

THALES

Thales HSMs

Vormetric Data Security

Vormetric Transparent Encryption



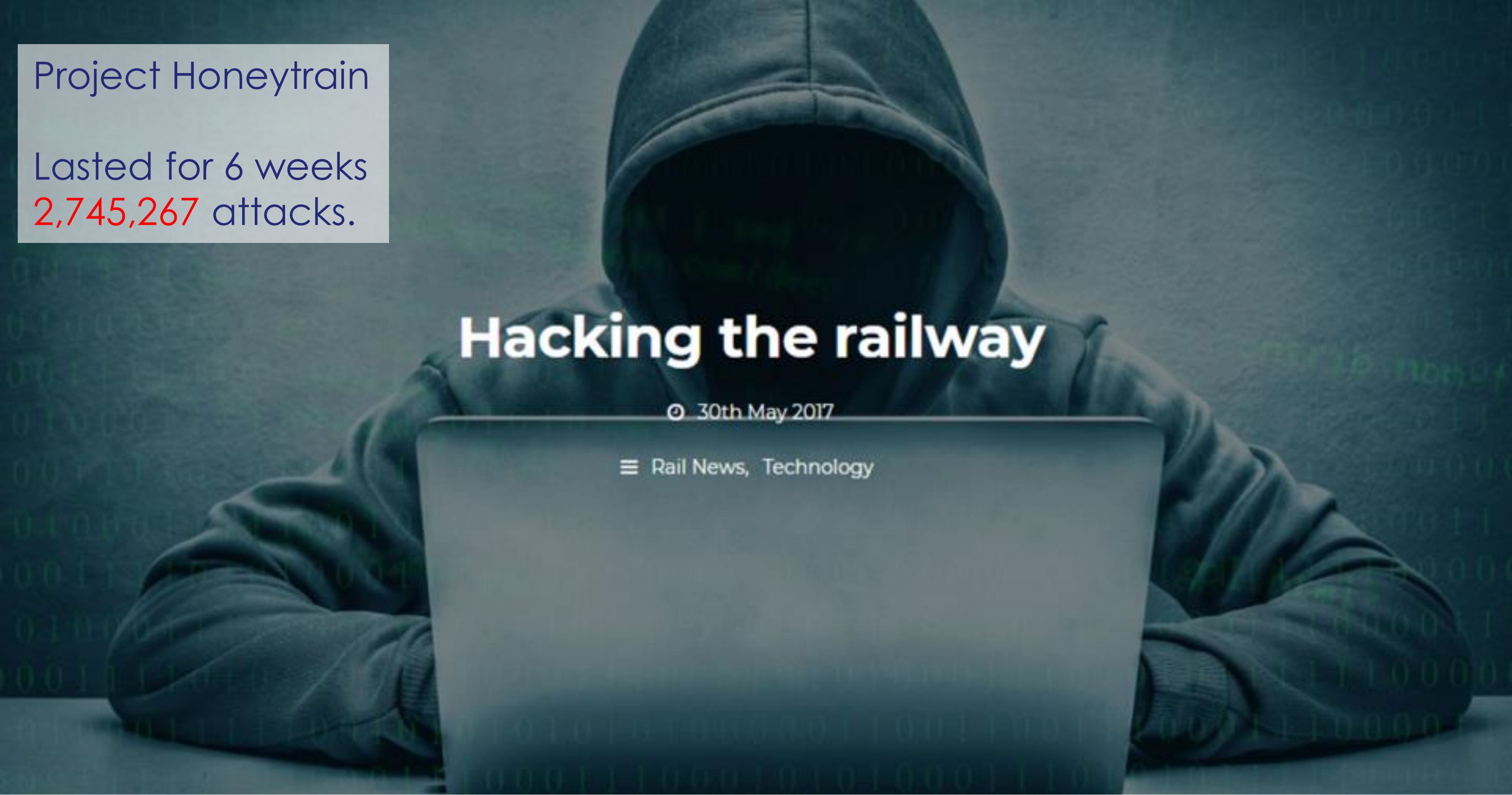
Vormetric Security Intelligence Logs to SIEM
Privileged Users
Approved Processes and Users
Encrypted
Clear Text
User
Application
Database
File Systems
Volume Managers
Storage
Allow/Block Encrypt/Decrypt
DSM
Vormetric Data Security Manager on premise or in cloud virtual or physical appliance
Big Data, Databases, Files or linked Cloud Storage
Encrypted
Cloud Provider/ Storage Administrators

CYBER SECURITY EXCELLENCE AWARDS
★ WINNER ★
2018

OPEN

Project Honeytrain

Lasted for 6 weeks
2,745,267 attacks.

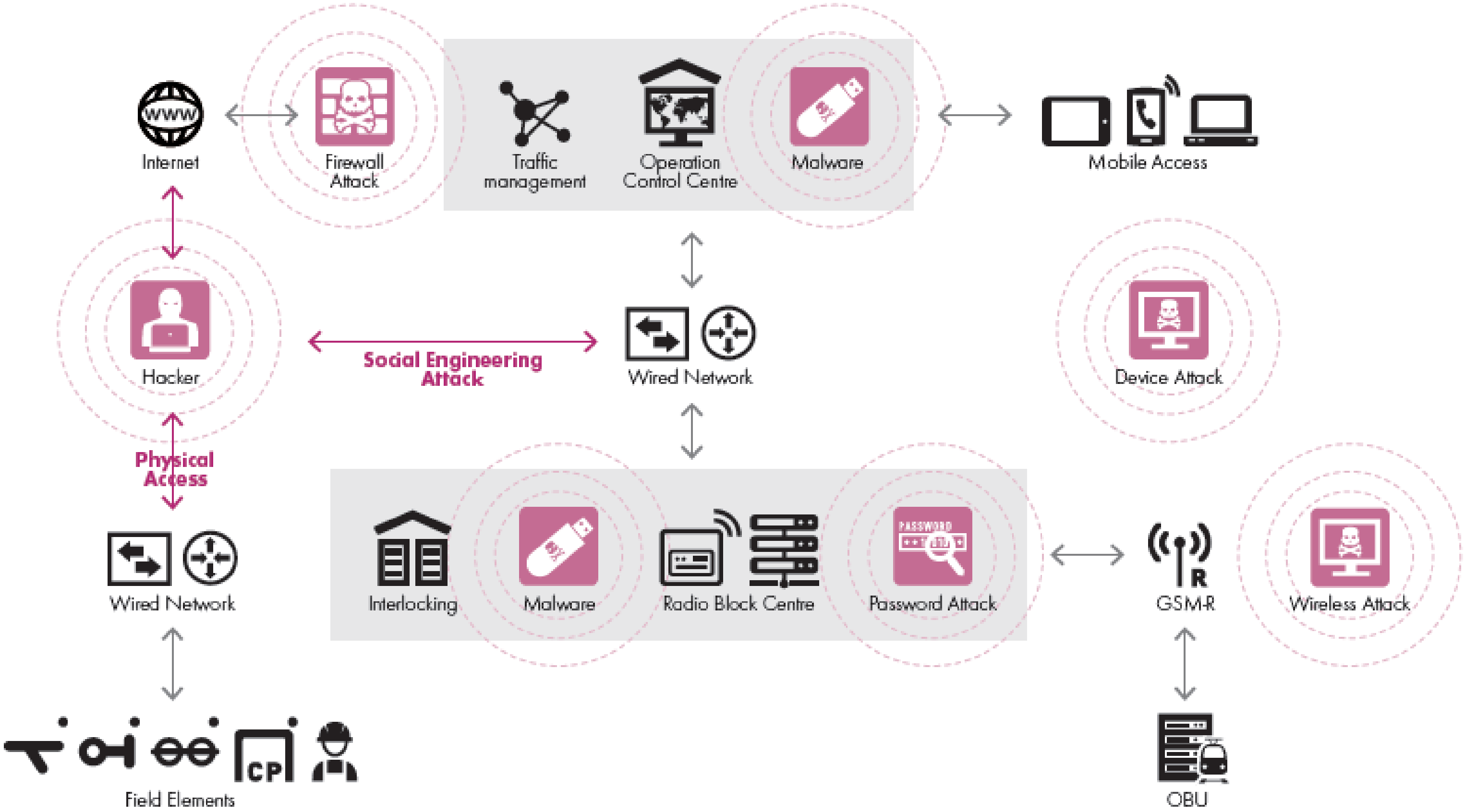


Hacking the railway

30th May 2017

Rail News, Technology

Threats We are Facing Every Day

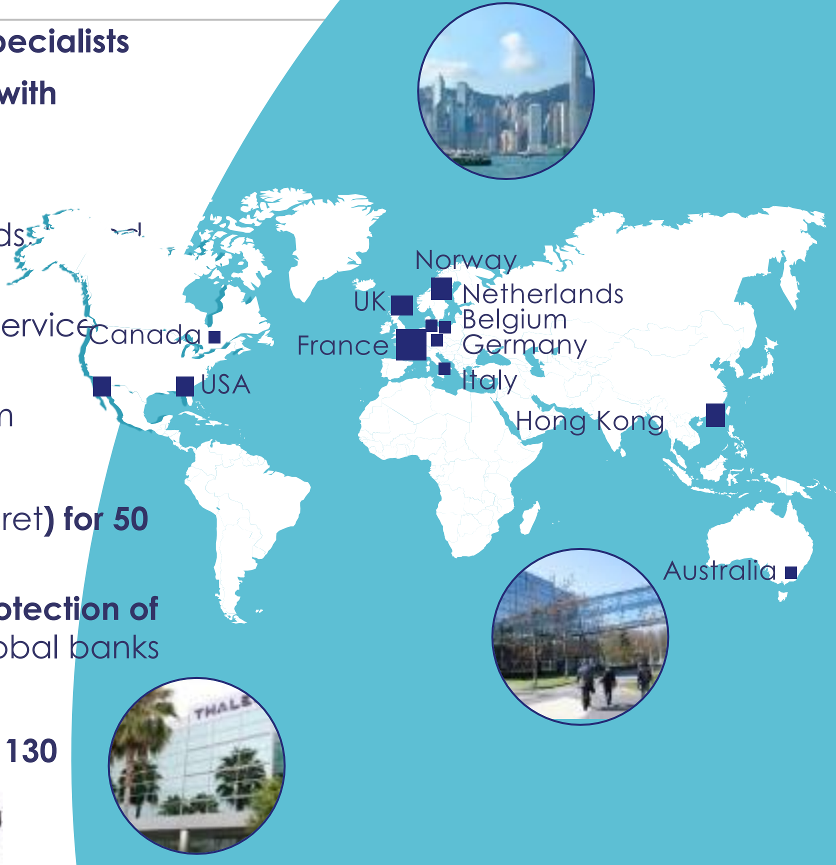


SUMMARY

- ✓ Introduction (M. Romairone)
- ✓ Biology Inspired Cybersecurity (V. Di Massa)
- ✓ **Cybersecurity Capabilities and Technologies (L. Ronchini)**

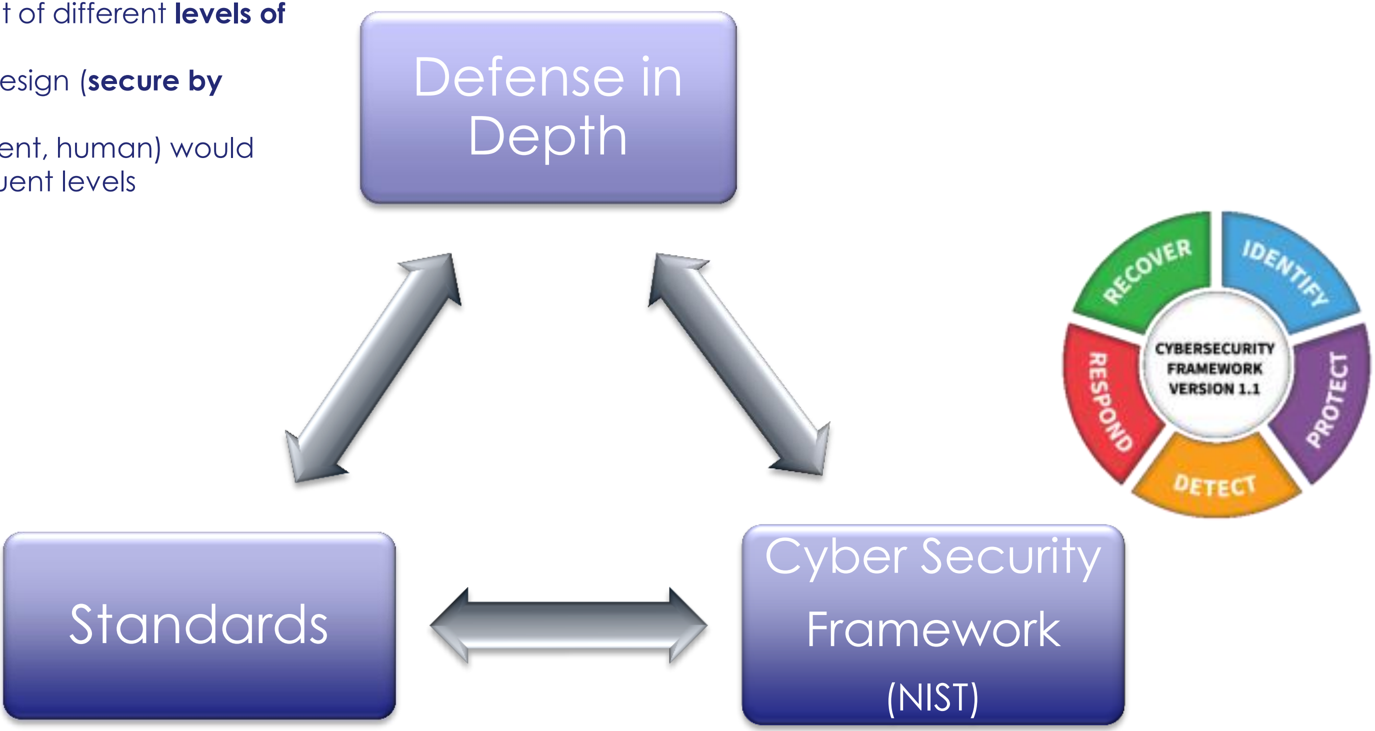
Critical Information Systems and Cybersecurity

- **5,000 IT & Security technicians,** including **1,500 cybersecurity specialists**
- **World leader in the cybersecurity market thanks to integration with Gemalto (3.2 B€ revenue and 28000 engineers in R&D)**
- **World leader in data protection**
- **5 Cybersecurity Operation Centers - CSOC** (France, Netherlands, United Kingdom, Hong Kong, Singapore)
- **1 CERT-IST** (Computer Emergency Response Team - Industry,? Service Tertiary sector)
- **5 High-security Data Centers** in France and the United Kingdom
- **1 CESTI evaluation lab**
- **Products with a high degree of security** (confidential or top secret**) for 50 countries, including NATO nations**
- Solutions and products **for 200 customers,** including **the 80% protection of global banking transactions.** Security for 19 of the 20 largest global banks
- **Cybersecurity for 9 of the 10 Internet Giants**
- **Management & cybersecurity of critical information systems of 130 customers**
- **Thales Research Laboratories**



Our 3 Cyber Security Pillars

- Hierarchical deployment of different **levels of Security** controls
- Implemented through design (**secure by design**) and operations
- A **single failure** (equipment, human) would **not propagate** to subsequent levels


Defense in Depth
Standards
Cyber Security Framework (NIST)
RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

- IEC 62443
- Common Criteria
- FIPS 140
- ISO 2700x (ISMS related)

Capability group – Thales Italia Experiences and Cyber Lab

Functional audit & Governance

- Audits ISO 2700x
- GDPR
- ISMS deployment
- Activity continuity
- Crisis management

Infrastructures & Applications Architectures

- Design Secure architectures
- Architecture audit
- Security governance
- Security accreditation processes

Forensic, Reverse & Penetration testing

- Incidents response
- Reverse Engineering
- Penetration testing
- Vulnerability assessment
- Technical audits
- Source code audits

Safety & Security Evaluation

- Hardware labs (CC)
- Software labs
- Safety labs (CNES)
- Multiple Banking certifications

Data Protection Environment

DB/ File Encryption

Customer Records

Application Encryption

Encryption Integration

Big Data

Secure Analytics

Code Signing

Script Development

Tokenization Data Masking

PCI, PHI

Transaction Security

Payment related apps

Public Key Infra (PKI)

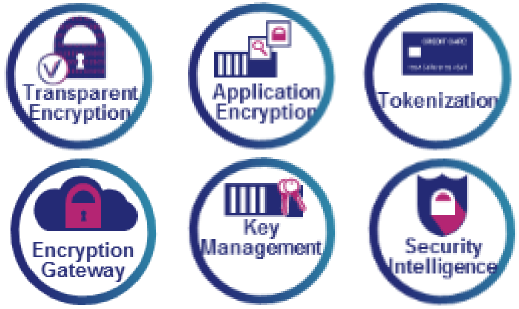
Internet of Things

Cloud Security

Cloud Migration

Use Cases

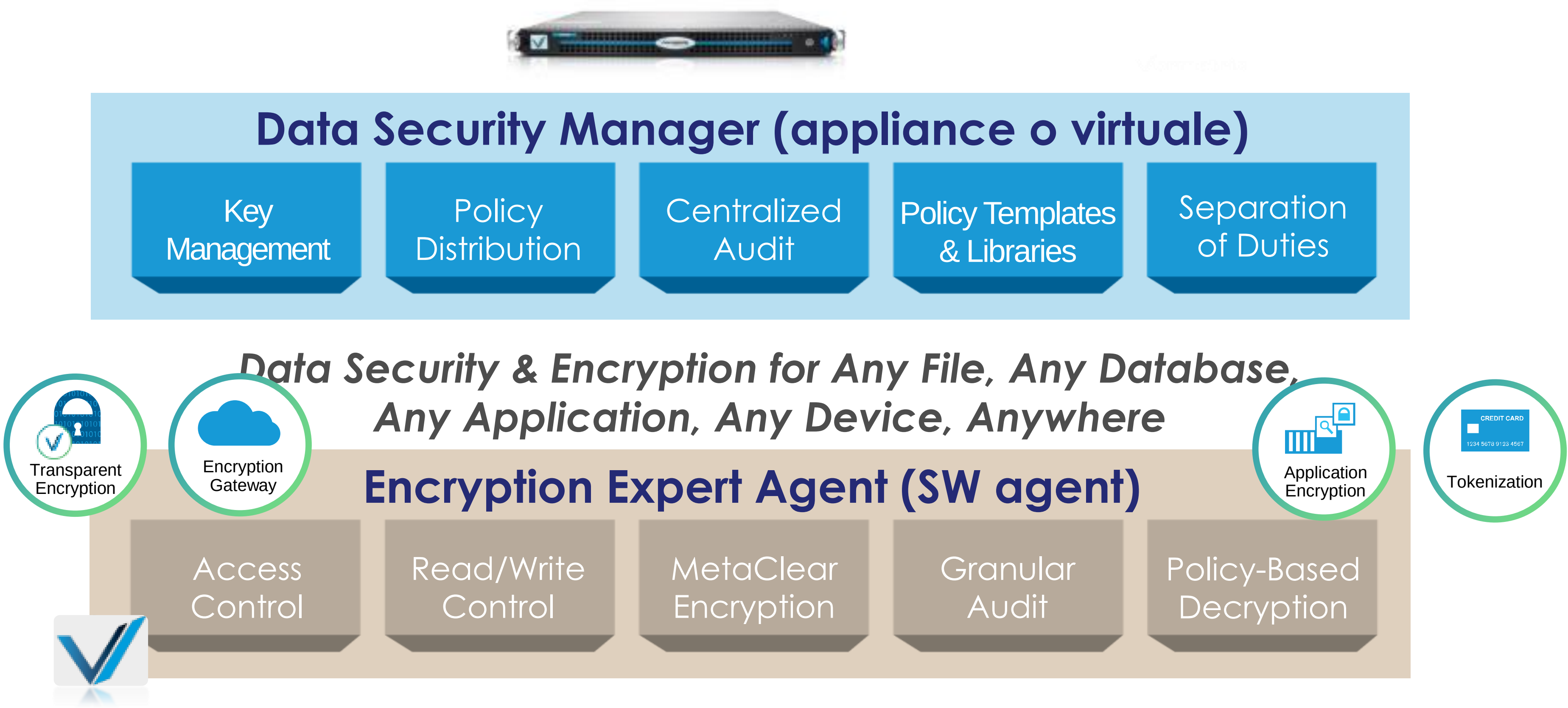
DATA PROTECTION HARDWARE



DATA PROTECTION SOFTWARE

OPEN

Thales Vormetric – Architecture



Data Security Manager (appliance o virtuale)

- Key Management
- Policy Distribution
- Centralized Audit
- Policy Templates & Libraries
- Separation of Duties

Data Security & Encryption for Any File, Any Database, Any Application, Any Device, Anywhere

Encryption Expert Agent (SW agent)

- Access Control
- Read/Write Control
- MetaClear Encryption
- Granular Audit
- Policy-Based Decryption

OPEN

Encryption - Hardware Security Module - HSM

Multi-purpose HSM

Certification FIPS 140-2 Level 3 + CC EAL4
Key Management
Encryption operations
Code Protection
Strong Authentication
Remote Administration
Better operational management
IoT Security

payShield – Payment HSM

Certification FIPS 140-2 level 3 e PCI
mPOS
Secure eCommerce- Transactions
PIN Generation
Conctactless payments

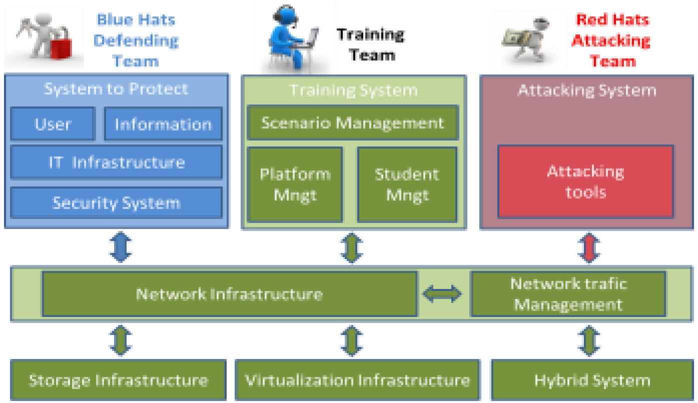
Mobile SOC & Cyber Range

Mobile SOC

- Modular architecture based on virtualized COTS
- Poor / Sporadic connectivity (SAT)
- IDS/IPS + Sandbox + Storage

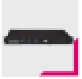
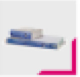
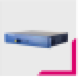
Cyber Range

- The cyber range training and test platform offers:
  - Realistic simulation of networks realized with different technologies
  - Knowledge, training and improvement thanks to the practical activities carried out by the personnel involved
  - Evaluation of internal processes and the main security standards
  - Maintenance of cyber security skills thanks to a challenging and challenging work environment

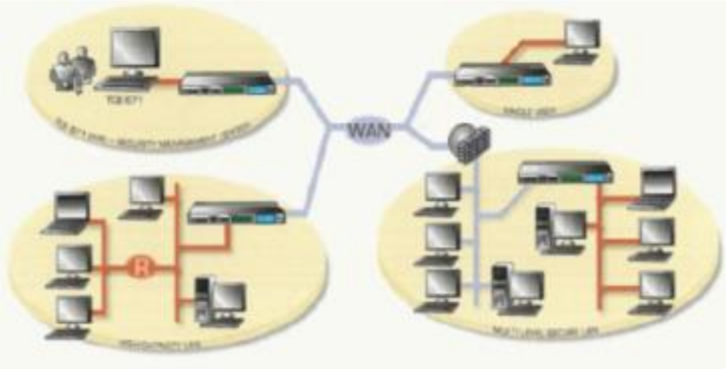


Communication Security: Thales Network Encryptors

Four platforms

- **Datacryptor** (Confidential).
- **Mistral** (Restricted).
- **Echinops** (Restricted + Secret – Export Control DGA).
- **TCE 621** (Military - Top Secret – NATO Country).



Advantages of standalone cryptography

- Less latency of embedded systems in routers, switches
- Key management within a FIPS-certified device
- Integration with PKI environments

Flexible and Secure

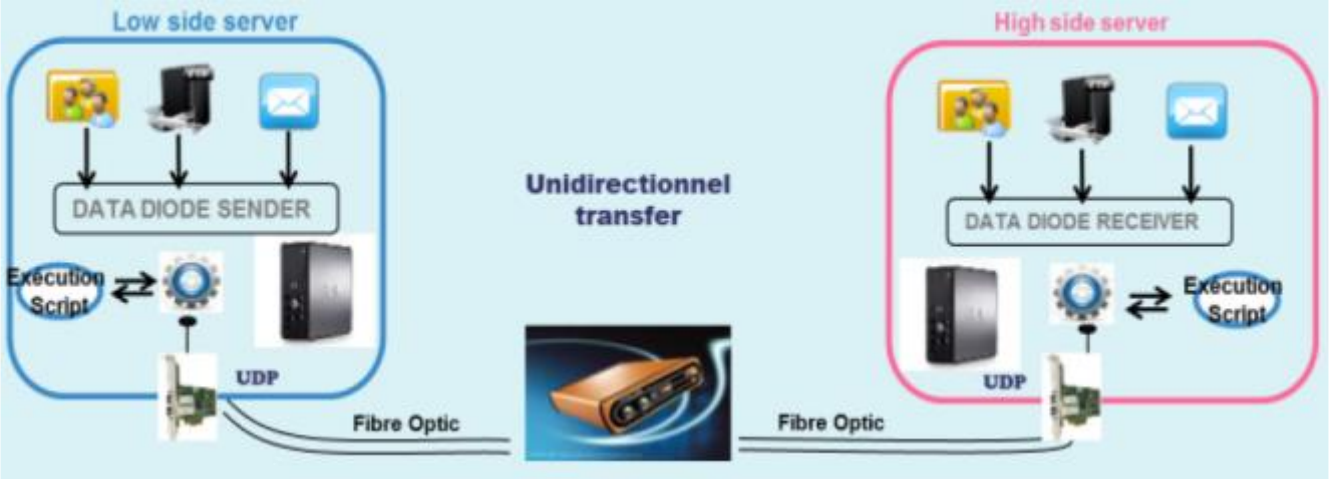
- Broad spectrum of capabilities and supported protocols
- Several certifications: FIPS, Common Criteria,UK CAPS, NATO, DISA UCAPL
- Multiprotocol

Communication Security: CyberOneComm CySecTrac 6838 Diode

- Data-Diode to protect and cybersecure Network Communication in Railway
- Ruggedized data-diode for use in railway operation.
- Designed for Ethernet/UDP communication, non-reactive on base of physical means.
- Web-GUI or SD-card based configuration
- The appliance is restricted to communicate exclusive from DATA-IN to DATA-OUT based on physical means.
- Seven switched independent Ethernet ports per DATA-IN /DATA-OUT subnet. Each of these can act as unidirectional data port.
- Cap rail mountable
- 2 x SD-Card slots for configuration (DATA-IN/DATA-OUT), physical secured
- Underlying standards: EN 60950-1, EN 61131-2, EN50121-4, EN 50155, EN 45545-2

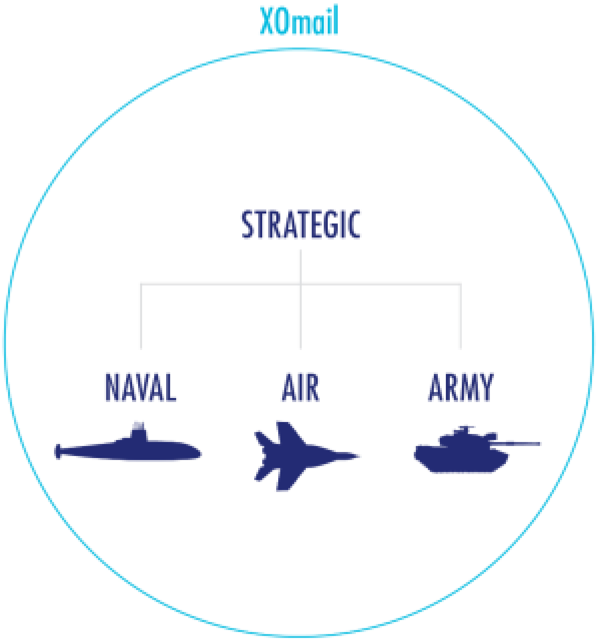
Communication Security: Elips-SD

- ELIPS-SD is a kind of "secure data diode" that enables automatic data transfer between different networks with different levels of security / classification allowing communication in one way.
- ICS / SCADA Cybersecurity, Airgap, Military environment.
- It is used for various applications: file transfer, email transfer, UDP, etc.
- ELIPS-SD can also be used for administrative and monitoring activities.

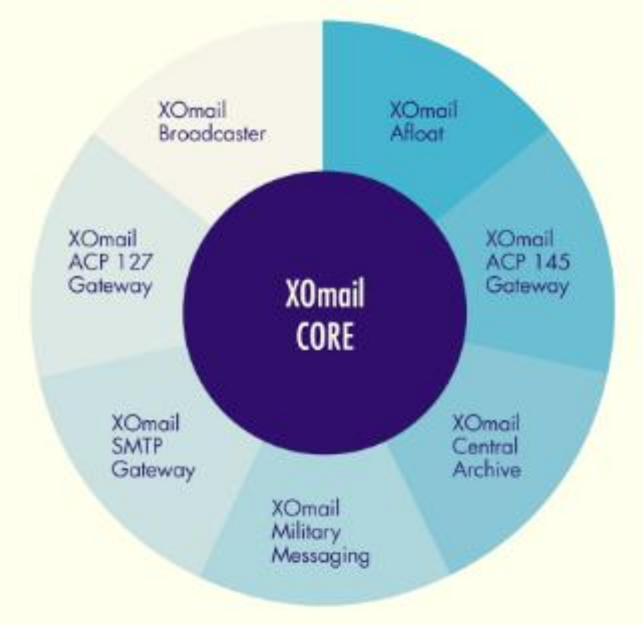


MMHS: The XOmail Product Family

A complete messaging solution for the modern cyber defense



7 components sharing a common core



DEMO CYBEL

Thales Security Intelligence: Cybels Platform

Integrity of all software system compnents (encrypted, signed)

Intrusion Detection/prevention System + Machine Learning

Behaviour Anomaly Detection

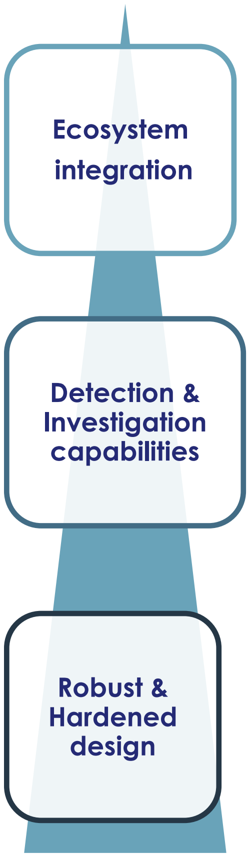
Malware Detection

Separation of Duties (Administration vs Cyber Security)

HDD and RAM encrypted

Trusted OS

Thales Cybels Sensor – Features



Signatures feed

- Thales Cyber Threat Intelligence
- Custom feeds

Ecosystem integration

- SOC tooling (Log Mgt, SIEM)
- SOC IT services (LDAP, PKI)

Intrusion Detection System (IDS)

- Protocol analysis
- Signatures correlation

Static File Analysis (SFA)

- Yara signatures correlation

Full Packet Capture (FPC)

Investigation using Metadata

- Forensics
- Search for Indicators or Compromise

Anomaly Detection System (ADS)

- Statistics algorithms
- Behavioral algorithms
- Deep inspection

Machine Learning

Collect

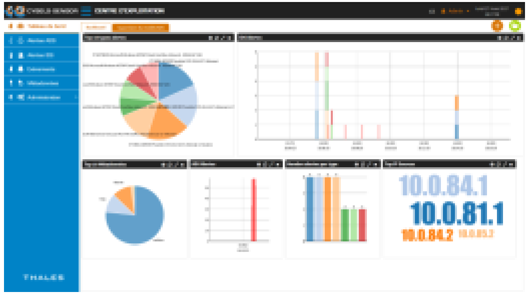
- Hardened OS and containers
- Protection of detection capabilities
- Data and Metadata collection

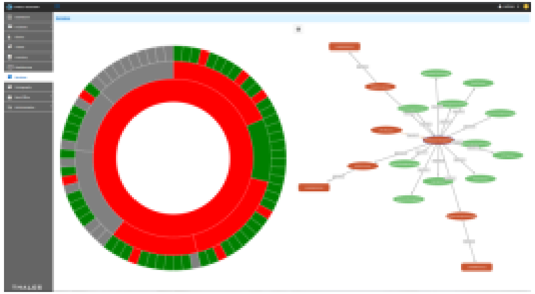
DEMO AOCC

OPEN

ICS Cybersecurity Subsystems integrated to AOCC

Security Intelligence
Cybels Decision and SIEM





Network Detection	Host Detection	Data Protection

Thales Integration Framework

Thales Cybels Sensors

Thales HIDS Sensors

Thales Vormetric

- Detection , Analysis, Remediation
- Alarm correlation and feeding to AOCC: cybersecurity+physical security