GENERAL DYNAMICS
Page Europa

ACHEMA 2018: Cyber Security – why and how

The cyber security for the protection of integrated ICT and SCADA systems

Filippo Silvestri
BD & Sales Manager GD
General Dynamics Page Europa

June 14th , 2018

ISA Italy Section

GENERAL DYNAMICS
Page Europa

Introducing GD and PAGE Europa

GENERAL DYNAMICS

AEROSPACE

COMBAT SYSTEMS

INFORMATION SYSTEMS & TECHNOLOGY

MARINE SYSTEMS

GD Corporation
EMPLOYEES: 90,800
About US$ 32 Billion Revenues

GD Mission Systems
EMPLOYEES: 12,500
FACILITIES: 113
COUNTRIES: 27
CUSTOMER SERVICE 24/7

GENERAL DYNAMICS
Mission Systems

60 YEARS OF INNOVATION AND EXPERIENCE

GENERAL DYNAMICS
Page Europa

PAGE Europa Offer

Turn Key

Systems Integration

Services

Telecoms, Security & IT Systems

Design, Engineering, Procurement, Integration, Validation, Test & IFAT, On-Site Installation - Activities & Services, Maintenance, Training & Technical Support

Customer Benefits

- ✓ SINGLE INTERFACE & SINGLE SOURCE of RESPONSIBILITY for Engineering, Procurement & Delivery of several multi-disciplinary fully integrated systems
- ✓ REDUCED RISKS
- ✓ PRICE EFFECTIVE Projects
- ✓ DELIVERING “Right First Time”, ON-TIME & ON-BUDGET

GENERAL DYNAMICS
Mission Systems

Page Europa Main customers

Oil & Gas Companies

QP (Qatar), Ras Gas (Qatar), BP, SHELL, ExxonMobil, ENI, NESTE OIL, ADCO (UAE), AGIP KCO (Kazakhstan), KPO (Kazakhstan), SONATRACH (Algeria), Anadarko (Algeria), SABIC-YANBU (KSA), PDO (Oman), SCOP (Iraq)

EPC & PMC Contractors

PETROFAC, KBR / KELLOGG,
AMEC, WorleyParsons,
FLUOR, CB&I, JGC, HYUNDAI HI,
AKER KVAERNER / SOLUTIONS, BECHTEL, TECHNIP, SAIPEM / SNAMPROGETTI

Ministries of Interior/Defence& Government Agencies

Turkey, Poland, Portugal, Germany, The Netherlands, Greece, UK,
Norway, Belgium, UAE, Italy, Albania

Port & Airport Authorities

Dubai & Abu Dhabi (UAE), Oman,
Italy, Kingdom of Saudi Arabia

NATO Agencies

NCIA, NC3A, NAMSA, NACMA,
SHAPE, AF South, AF Cent, AF North

GENERAL DYNAMICS
Mission Systems

Ministero della Difesa
SEGRETARIATO GENERALE DELLA DIFESA E
DIREZIONE NAZIONALE DEGLI ARMAMENTI
DIREZIONE INFORMATICA, TELEMATICA E
TECNOLOGIE AVANZATE
(TELEDIFE)

ATTESTATO DI RICONOSCIMENTO
N. 0018

Il Sistema di Gestione per la Qualità realizzato dalla Ditta:

Soc. PAGE EUROPA S.r.l.

è stato valutato da Teledife e riconosciuto rispondente ai requisiti della pubblicazione:

NATO AQAP – 2110/160

Tale sistema viene attuato presso le sedi di Roma e di Monterotondo (RM) per le seguenti attività:

Progettazione, produzione, installazione e manutenzione di sistemi HW/SW fissi e mobili per forniture militari nei settori: telecomunicazioni, sicurezza, energia elettrica, contromisure elettroniche, simulazione, addestramento, assistenza alla navigazione, sistemi di gestione e controllo apparati, dati e reti.

Il presente attestato ha una validità di tre anni dalla data di emissione ed è revocabile in caso di inadempienze accertate da questa Direzione.

Roma 13 MAR. 2017

IL VICE DIRETTORE TECNICO
Magg. Gen. Ing. Stefano DEGLI ESPOSTI ZOBOLI

BUREAU VERITAS Certification

PAGE EUROPA SRL

Head Office and Operative Site:
Viale Egeo, 100-106 – 00144 ROMA (RM) – ITALY

Operative Unit:
Via Archimede, 24 - 00016 MONTEROTONDO SCALO (RM) - ITALY

Bureau Veritas Italia spa certify that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

Standard

ISO 9001:2008

Scope of certification

Study, technical design, production and technical support for facilities and telecommunications, security and automation systems for military, civil and industrial applications.
Development of the associated software.

EA Sector(s): **19, 33**
Certification cycle start date: **11 January 2016**
Subject to the continued satisfactory operation of the organisation's Management System, this certificate expires on: **15 September 2018**
Original certification date: **14 January 2004**

Certificate No. 206935 Version N. **1** Revision date: **11 January 2016**

LODOVICO JUCKER – Local Technical Manager

Certification body address:
Bureau Veritas Italia spa, Via Miramare, 15, 20126 Milano, Italia

ACCREDIA

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.
To check this certificate validity please refer to the website www.bureauveritas.it

BUREAU VERITAS Certification

PAGE EUROPA SRL

Registered Site:
Viale Egeo 100-106 - 00144 ROMA (RM) – ITALY

This is a multi-site certificate, additional site(s) are listed on the next page

Bureau Veritas Certification Holding SAS – UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO 14001:2015

Scope of certification

Study, technical design, production (through assembly) and technical support of telecommunications, security and automation systems for military, civil and industrial applications. Development of the associated software.

EA Sector(s): **19, 33**
Original cycle start date: **15 April 2005**
Subject to the continued satisfactory operation of the organization's Management System, this certificate expires on: **13 April 2020**
Certification / Recertification cycle start date: **12 April 2017**

Certificate No. *IT173815/UK* Version: **1** Revision date: **12 April 2017**

ANDREA FILIPPI – Local Technical Manager
Signed on behalf of BVCH SAS UK Branch

Certification body address: 5th Floor, 66 Prescot Street, London E1 8HG, United Kingdom
Local office: Via Miramare, 15 - 20126 Milano – Italia

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.

To check this certificate validity please call: +39 02-270911

UKAS MANAGEMENT SYSTEMS
0008

Page 1 to 2

BUREAU VERITAS Certification

PAGE EUROPA SRL

Registered Site :
Viale Egeo 100-106 – 00144 ROMA (RM) – ITALY

This is a multi-site certificate, additional site are listed in the appendix to this certificate

Bureau Veritas Italia S.p.A certify that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

Standard

OHSAS 18001:2007

Scope of certification

Study, technical design and technical support of telecommunications, security and automation systems for military, civil and industrial applications. Development of the associated software.

Certification awarded in conformity with the requirements of ACCREDIA RT-12
EA Sector(s): **19,33**

Certification cycle start date: **13 April 2017**

Subject to the continued satisfactory operation of the organisation's Management System, this certificate expires on: **14 April 2020**

Original certification date: **15 April 2005**

Certificate No. 170858 Version N. **1** Revision date: **13 April 2017**

ANDREA FILIPPI – Local Technical Manager

ACCREDIA

Certification body address:
Bureau Veritas Italia spa, Via Miramare, 15, 20126 Milano, Italia

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.
To check this certificate validity please refer to the website http://www.bureauveritas.it/certificate

GENERAL DYNAMICS
Mission Systems

Next Generation Security Systems

Command & Control

Situation Management


Manager Dashboard


Department Situation Management


Mobile Team App


User App

System of Systems

Sensor & Sub-Systems Agnostic

IT/OT Integration | Correlation | Analytics | Smart Prediction | Rules Engine | Procedure Manager | Simulation Manager

Platform Infrastructure

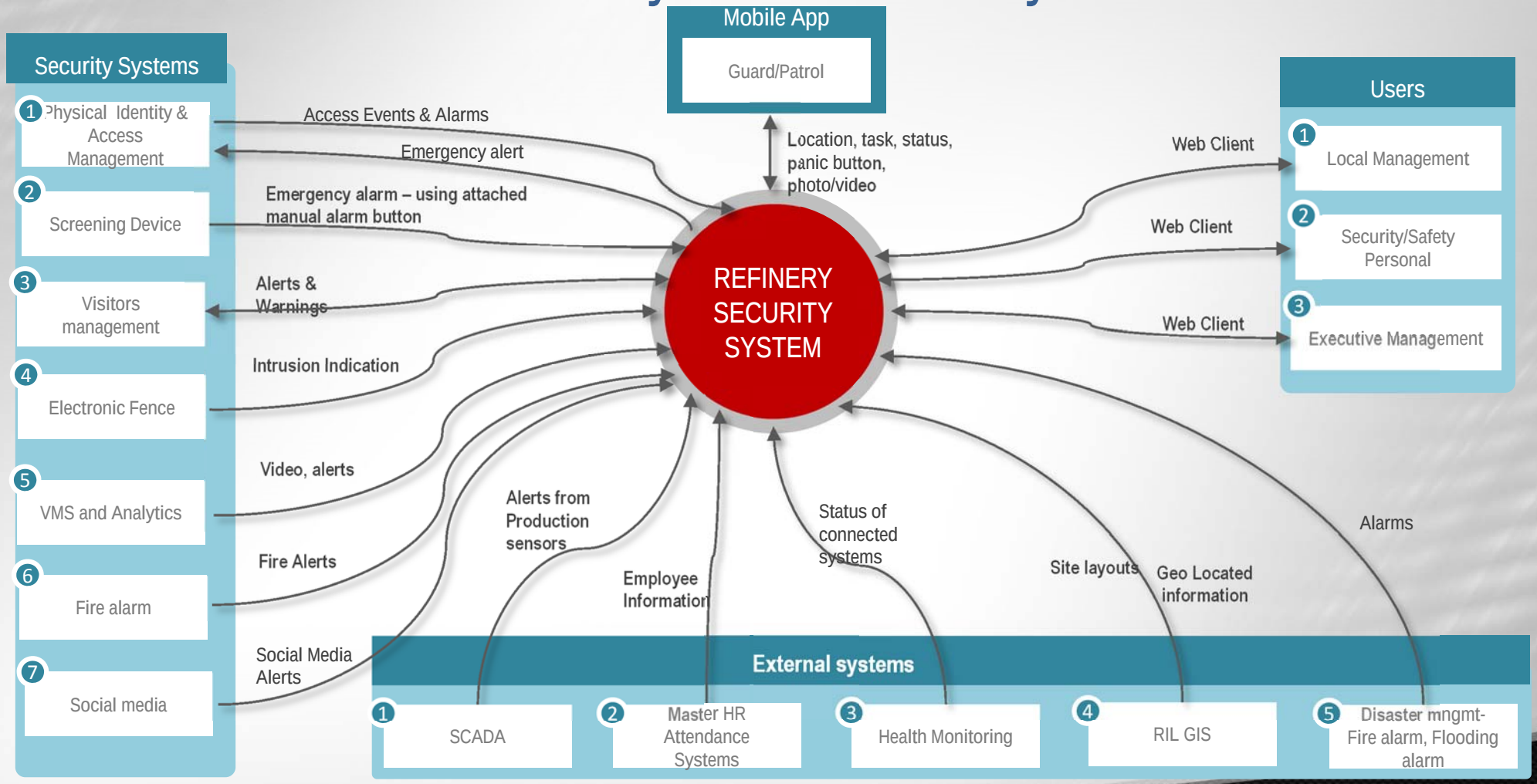
Site Manager | User Manager | DB Manager | Work Force Manager | Report Generator | ...

Sensor & Sub Systems

VMS System | Parking | Environmental Monitoring | Access Control | HR | Water | Fire\Smoke | PIDS | RADAR | Panic Button

GENERAL DYNAMICS
Mission Systems

Refinery: one holistic system



GENERAL DYNAMICS
Mission Systems

GENERAL DYNAMICS

Page Europa

About subject…

Vulnerabilities by ICS Component Types

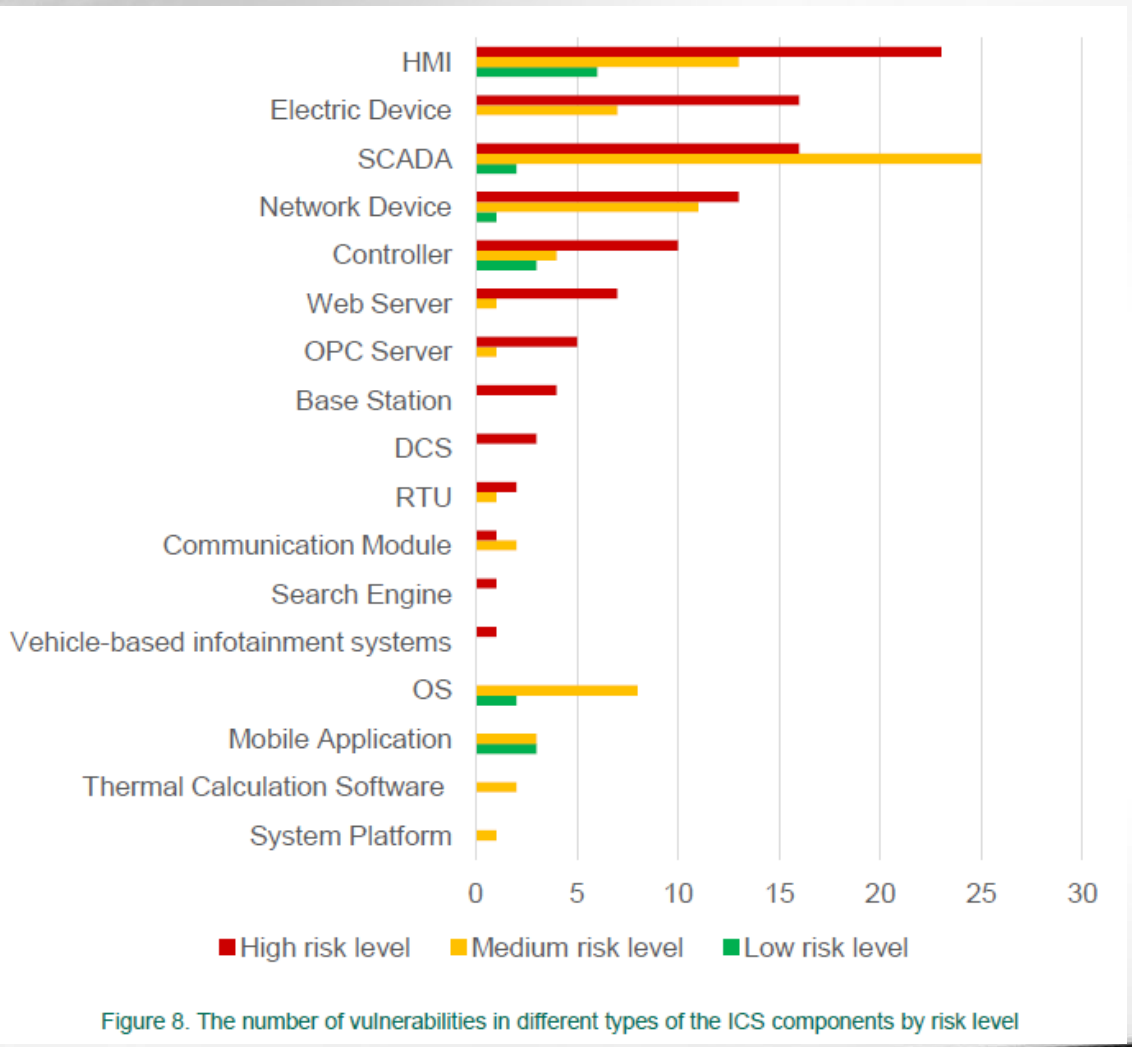


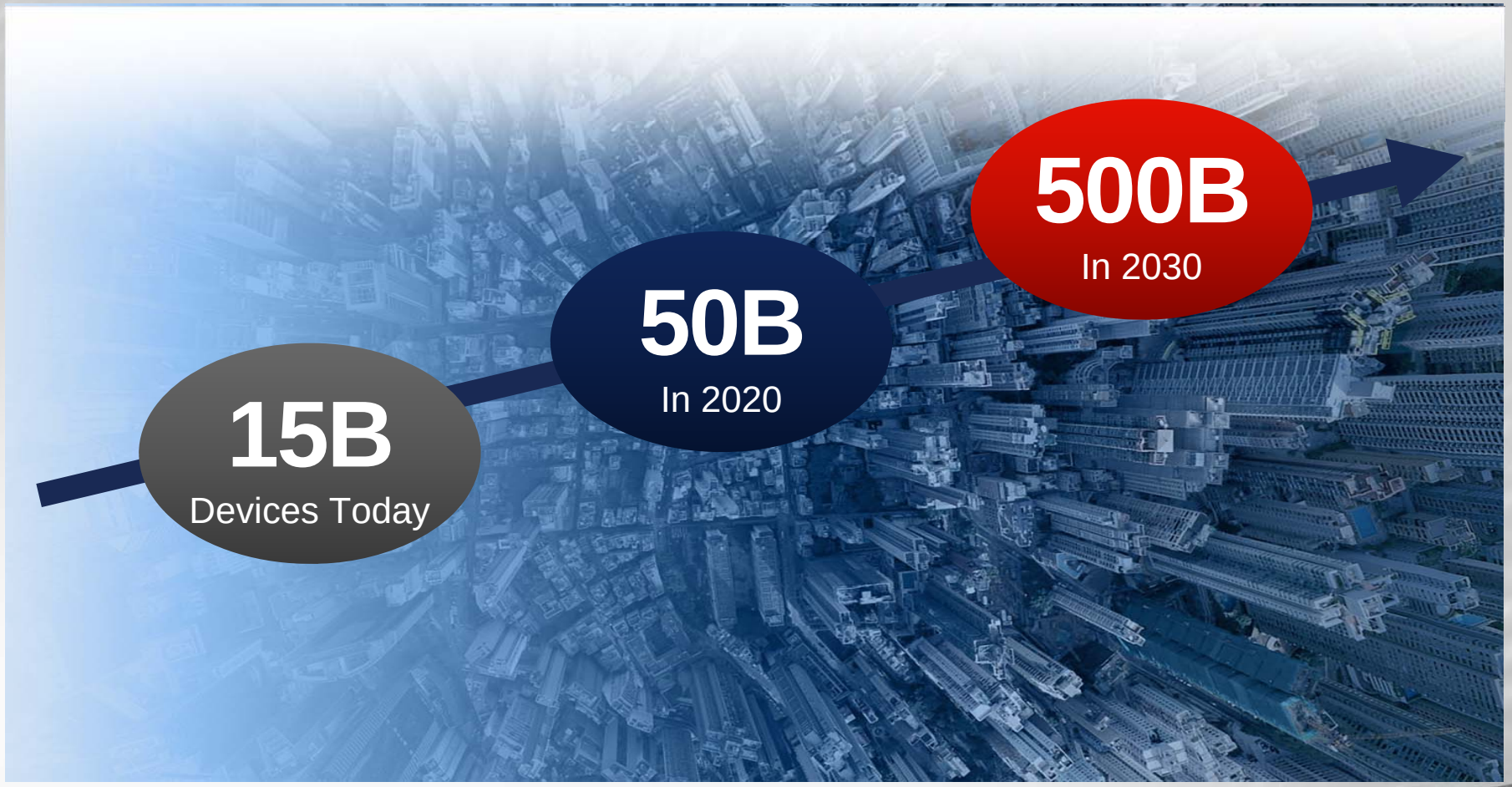
Figure 8. The number of vulnerabilities in different types of the ICS components by risk level

In the last years, **the most vulnerable Industrial Control Systems components were HMI – Human Machine Interface, Electric Devices and SCADA systems.** The "Electric Device" category consists of distance protection devices, gas detectors, pumps, power analyzers, recloser control and relay platform units.

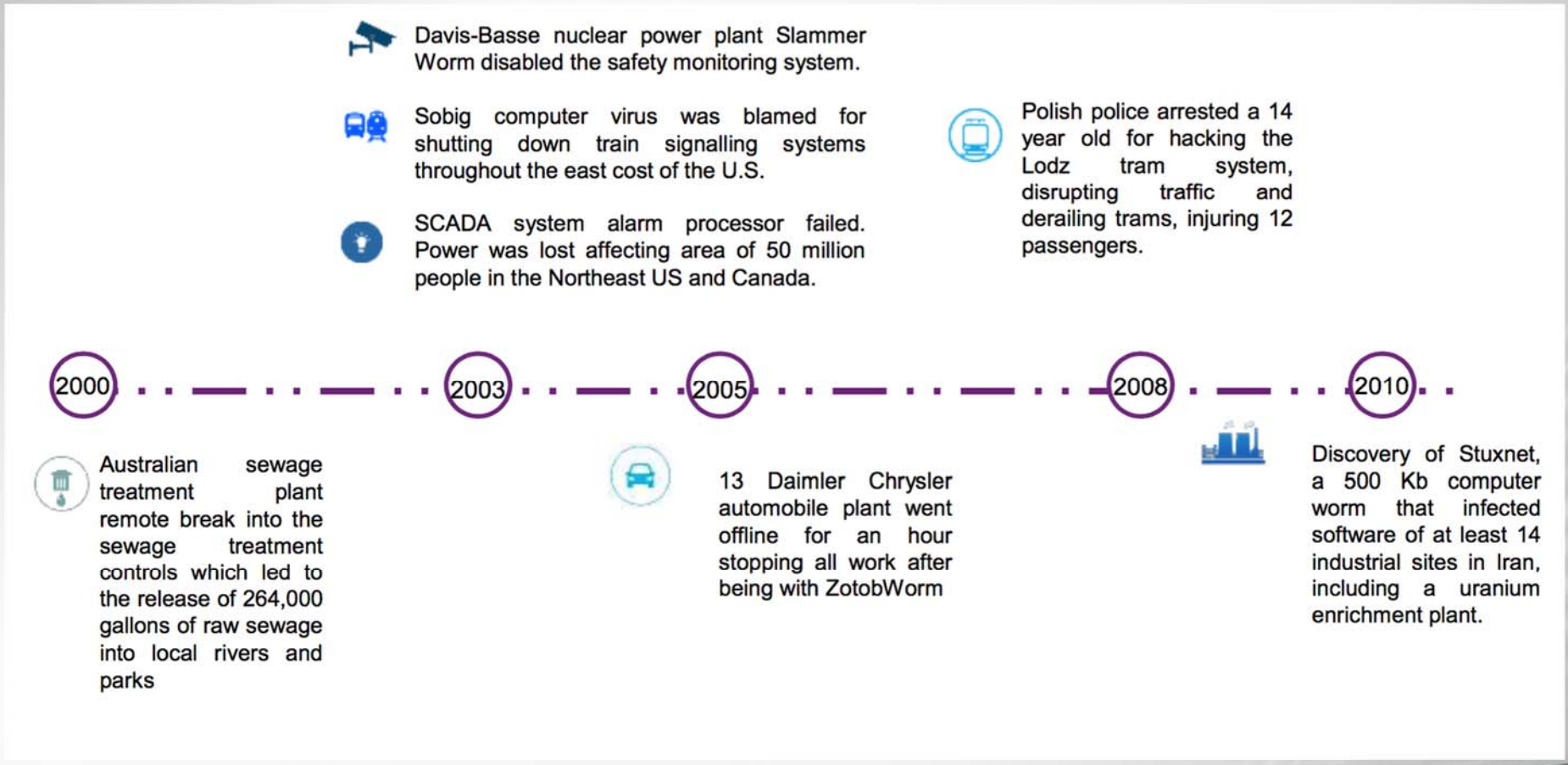
The graph demonstrates the vulnerability severity distribution for different types of ICS components.

(Karspersky Lab, ICS Vulnerabilities Statistics)

Rapid Digital growth



Incidents – Chronological Perspective



Incidents – Chronological Perspective

Hackers attacked German Steel mill control system such that a blast furnace was unable to shutdown resulting in massive damage.

A water treatment facility reported to ICS-CERT that it suspected that an overflow of wastewater treatment process was due to unauthorised employee access.

In October, 2016 Dyn was attacked by group called Anonymous. Various IoT devices used to create DDoS on Dyn servers is which is provider for major internet platforms and services.

2012 — 2014 — 2015 — 2016

Cyber espionage campaign dubbed Energetic Bear or Dragonfly targets grid operations, energy industrial equipment. Includes information stealing, remote access and sabotage capabilities.

In December 2015, Ukraine Power Grid was attacked. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporary disrupt electricity supply to the end consumers.

Incidents – Chronological Perspective

2010

MALWARE: Stuxnet

TARGET
Iran

AGGRESSOR
Unknown
(secret services are suspected)

BACKGROUND
Stuxnet is a computer worm that infects industrial programmable logic controllers (PLCs).

Stuxnet infiltrated Iranian nuclear facilities via USB sticks.

The attack destroyed a sixth of Iran's capacity to enrich uranium.

2012

MALWARE: Flame

TARGET
Middle East, especially Iran

AGGRESSOR
Unknown (secret services are suspected)

BACKGROUND
Flame is a complex form of malware for audio recording, screen monitoring, the capture of keyboard input and network activities.

It spreads via USB sticks or the local network.

MALWARE: Shamoon

TARGET
Saudi Arabian oil company

AGGRESSOR
Hacker group "Swords of Justice"

BACKGROUND
The attack sought to interrupt oil production.

Although major production outages were averted, it took about a week to recover the 30,000 systems that were affected.

2013

MALWARE: Red October

TARGET
Unknown

AGGRESSOR
Unknown (Russian-language malware)

BACKGROUND
This malware propagated itself via e-mail attachments.

It aimed to steal data from computers, smartphones and network storage devices.

2014

MALWARE: Uroburos

TARGET
Unknown

AGGRESSOR
Unknown (secret services are suspected)

BACKGROUND
To this day, it has been impossible to ascertain how Uroburos infiltrates systems.

The malware has been in circulation since 2011 but was not detected until three years later.

MALWARE: Regin

TARGET
Private individuals and companies; mainly telecom companies in Russia and Saudi Arabia

AGGRESSOR
Unknown (secret services are suspected)

BACKGROUND
The Regin malware targeted both companies and government institutions (the EU Commission).

A modular malware concept allowed functionality to be added retroactively.

A virtual file system makes Regin hard to detect.

MALWARE: No name

TARGET
E-commerce group

AGGRESSOR
Hacker group "Syrian Electronic Army"

BACKGROUND
More than 200 million users' personal data was stolen.

The data stolen included user names, passwords, telephone numbers and addresses.

When the attack became known, the targeted company's stock price collapsed.

MALWARE: No name

TARGET
Film corporation

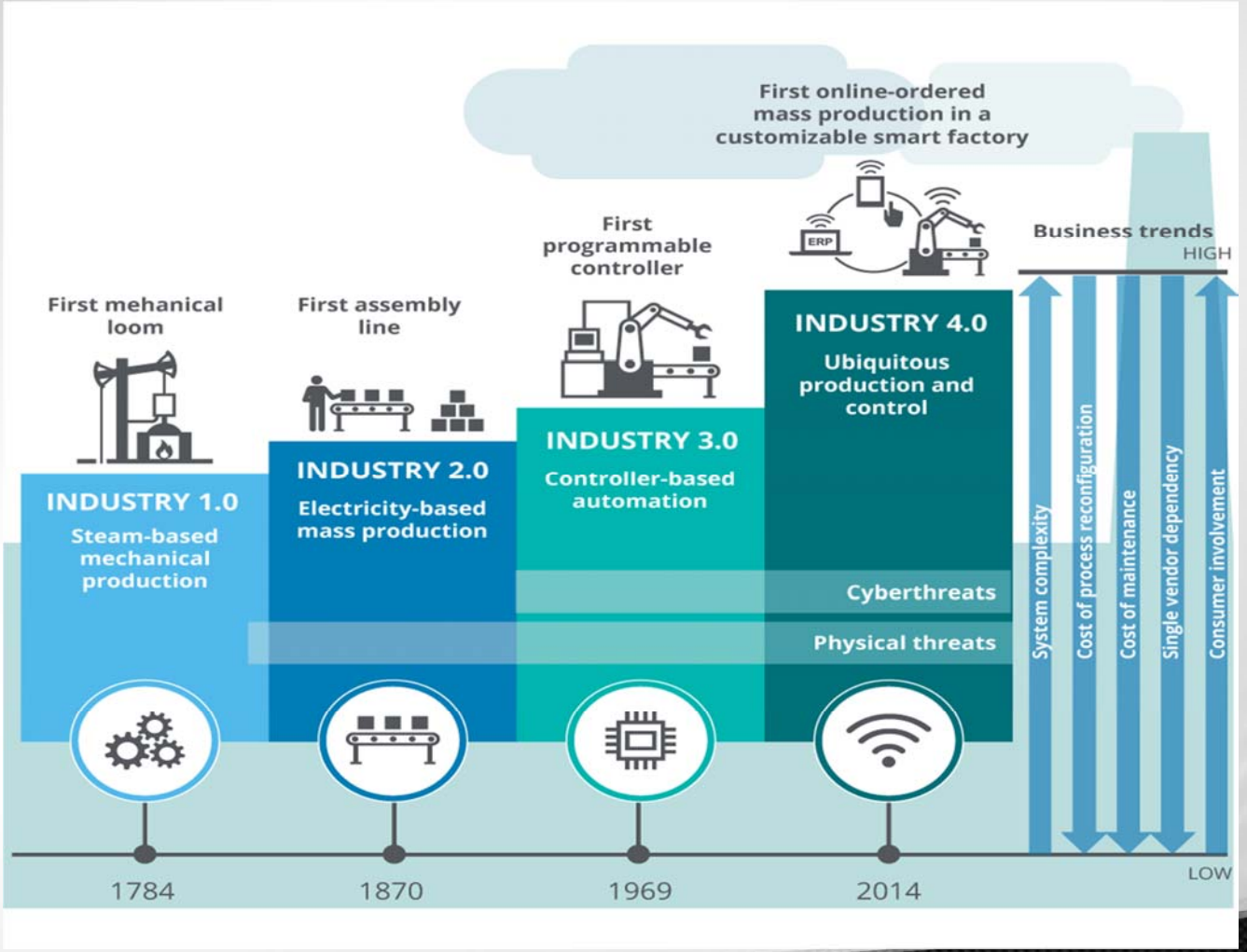
AGGRESSOR
Unknown (speculation points to an attack from North Korea or a company insider)

BACKGROUND
Hundreds of gigabytes of confidential e-mails and documents were stolen from company servers, including unpublished films and film scripts.

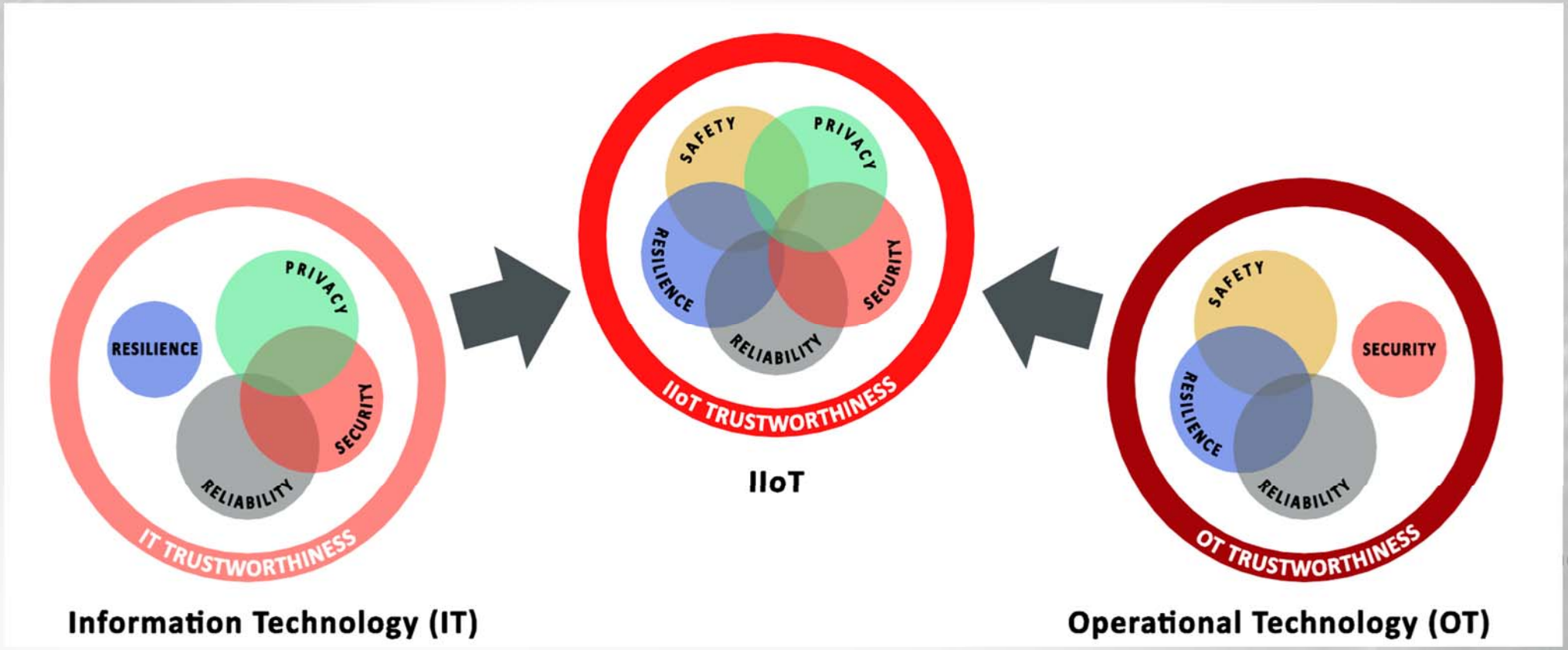
Parts of the company's computer networks were paralyzed.

The launch of a comedy film about North Korea was initially canceled as the hackers threatened terror attacks.

Industry 4.0



Industial IoT TRUSTWORTHINESS



Cyber Security evolution – It's an hard challenge

Traditional security vendors are dependent on signature-based technology. Their research teams explore cyberspace, catalog threats, attack vectors, vulnerabilities, signatures, and other techniques to learn how attackers think and design their attacks.

Then, vendors push regular updates our to their customers that are designed to alert when they recognize a familiar threat pattern. This concept of "blacklisting & shipping" is, in fact, a losing war, as it cannot deal with what is unknown.

Next came the next-generation technologies - decoy honeypots, containment, behavioral detection, machine learning and artificial intelligence.

Additional technologies focused on detecting threats via their attack vector. Yet the threats continue to get through - bypassing security technologies layer by layer, until reaching their final destination - endpoints and servers. Once the malware reaches their destination, the damage stage of the attack begins: deleting files, altering data, data exfiltration or data encryption.

Cyber Security evolution – It's an hard challenge

A new security paradigm seems to be the solution, in order to prevent any future threats, without actually having to know anything about the threat in order to prevent it.
A solution designed on following assumptions:
1. The attacker will eventually find a way to bypass all security means;
2. The threats are already inside, undetected.

Relying on the operating systems behavioral patterns map, it distinguishes between "good" and "bad" actions, detecting and preventing any malicious activity – regardless the threat type, attack vector and origin.

GENERAL DYNAMICS

Page Europa

The solution


NYOTRON
SECURING THE WORLD

The biggest challenge in today's digital era is to effectively deal with both current and future threats

- while knowing nothing about them.

THE EVOLUTION OF SECURITY

THE KNOWN

Traditional AV

THE KNOWN UNKNOWN

Next Gen Technologies

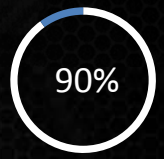
THE UNKNOWN UNKNOWN

Threat-agnostic Defense

THE COST OF ATTACKS

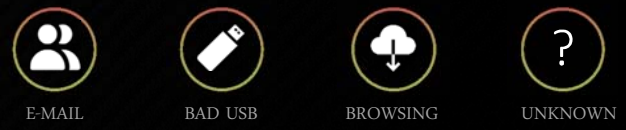
Cost of attack per company

Cost of global cyber activity



Of enterprises contain malware in their network

New threat per second



The investment paradox

Perimeter

SMTP AV

NAC

IPS

FIREWALLS

Decoy

Application control

DLP

Sandbox

IDS

Anti Bot

Anti spam

Proxy

SSL Inspection

DDoS

Web Filtering

File sanitation

WAF

80%

Endpoint

HDLP

AV

HIPS

20%

Your data

Paranoid: **Threat-agnostic Defense ™**

Protects Your Data Regardless of Type of Threat or Attack Vector

- Effectiveness Doesn't Rely on Prior Knowledge About the Threat
- Assumes Threats are Already Inside or Will Bypass Security Layers
- Acts as Last Line of Defense
- Holistic Approach - Detect. Prevent. Respond. Analyze.

THE NYOTRON DIFFERENCE

Threat-agnostic Defense ™ Approach

ATTACK METHOD

Drive By Download

Buffer Overflow

Cross-Zone Attack

Heap Spray

Privilege Escalation

Cross-Site Scripting

Symbolic Link Race

Metamorphic Code

DLL Hijacking

Format Strings

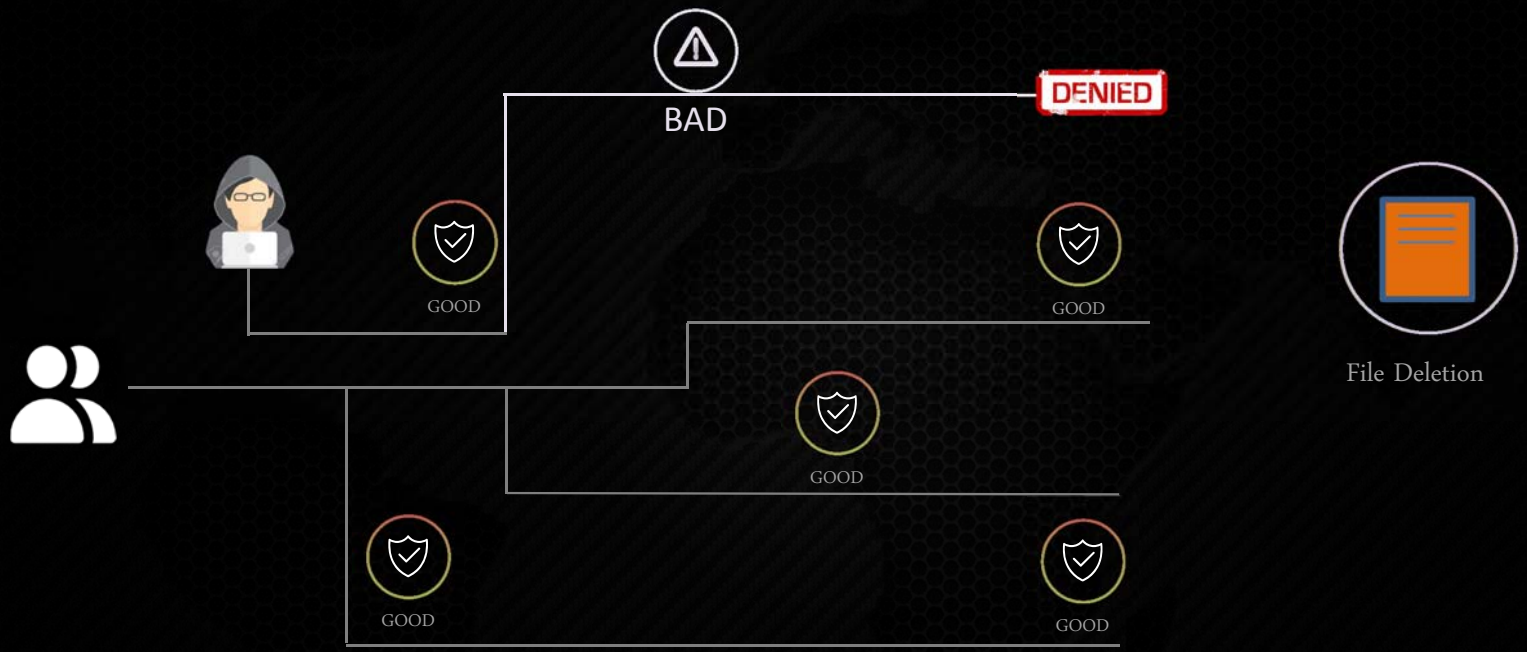
Macros

Polymorphic Code

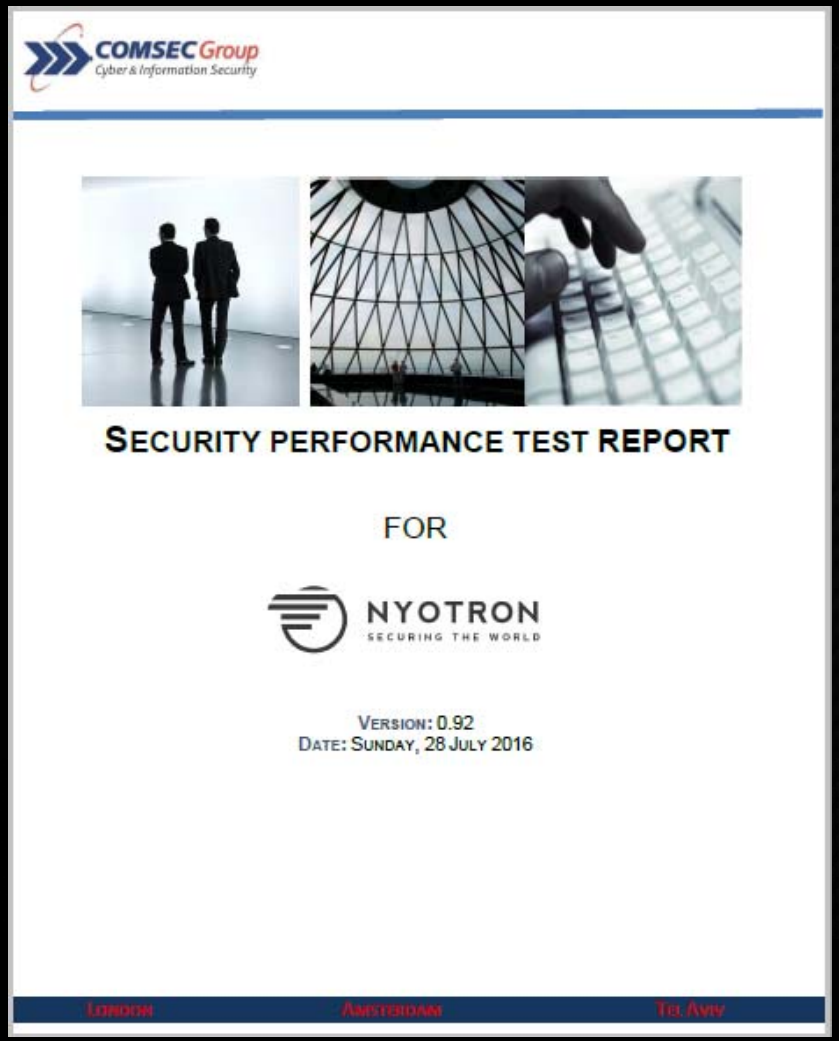
Click jacking

Buffer Overrun

Behavior mapping technology (BPM)



INDEPENDANT PERFORMANCE REPORT JULY 2016



"Nyotron Paranoid solution is focused on zero-day attacks prevention when all other protection measures were exhausted".

- *100% of the tested ransomware were not able to cause damage to data*
- *100% of the tested malwares were not able to cause any damage.*
- *Paranoid system could handle 1000 simultaneous threats.*
- *No performance or user experience issues were detected.*

Operational & BUSINESS MODELS

CHOOSE YOUR MODEL

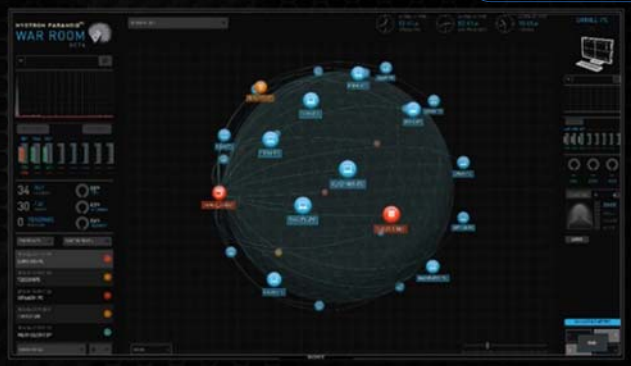
1. YOU MANAGE
2. WE MANAGE
3. PARTNER (MSSP)

MONITORING & ALERTING

ACTIVITY MANAGEMENT

OPERATIONS VIEW

FORENSICS VIEW



INCIDENT VIEW

GLOBAL
WAR ROOM

INTELLIGENCE

CRISIS RESPONSE

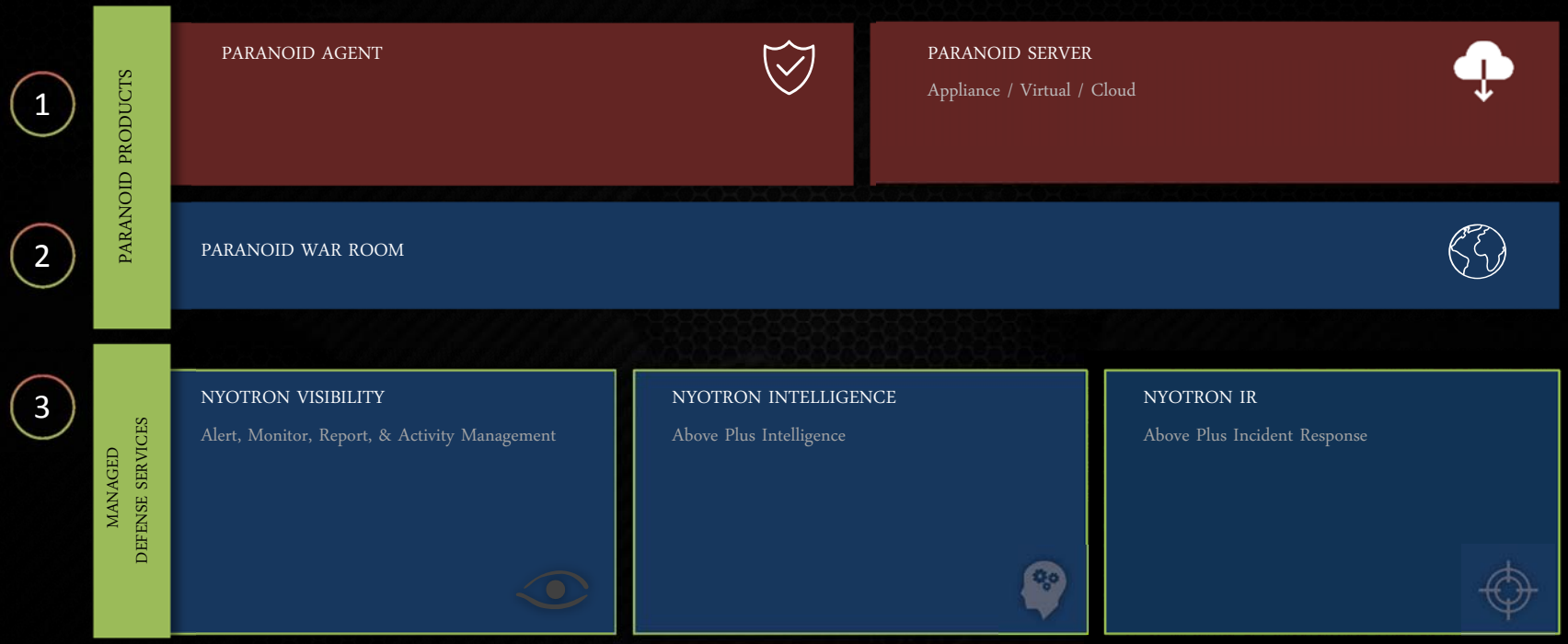
We have a great success with Paranoid as a service. Nyotron's Global War Room center helping us through detection and remediation handling. Acknowledging the fact that our traditional security means, such as Anti-Virus and Firewall systems, cannot protect against Zero-day attacks and APTs,

it is a fact that our security posture went up by having Paranoid on board...

CISO, Major US Law Enforcement Agency

NYOTRON endpoint protection PLATFORM

Three ways to get Threat-agnostic Defense ™ - You Manage, Nyotron Managed or Partner Managed



GENERAL DYNAMICS
Page Europa

Thank you for your attention!

filippo.silvestri@pageuropa.it

www.pageuropa.it