Ο αντίκτυπος της ΤΝ στον Κυβερνοχώρο: Βεβαιωθείτε ότι η πρόοδος προστατεύεται

Al's Impact on Cyberspace: Ensure progress is protected



George Christou

Corporate Channel Development Manager



Digital Security Progress. Protected.

The importance of data feeds in AI





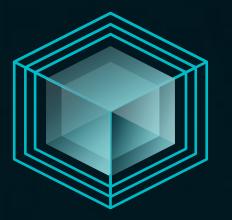
Al & Machine Learning



ESET LiveGrid® (Cloud Reputation)



Human Expertise



ESET LiveSense® Multilayered security technology



How AI is becoming a threat



Evolution with Genetic & Automation algorithms



Clever ways in bypassing intrusion detection or evade security mechanisms



Cleverer and more creative Scams



Automated and faster collection of data



Faster and smarter creation and evolution of malware



Increasing threats and frequency of attacks in general



Sandworm APT Group Overview



Sandworm Team (Trend Micro) Iron Viking (SecureWorks)

CTG-7263 (SecureWorks)

Voodoo Bear (CrowdStrike)

Quedagh (F-Secure)

TEMP.Noble (FireEye)

ATK 14 (Thales)

BE2 (Kaspersky)

Russia

State-sponsored, GRU Unit 74455

2009

Sabotage && Espionage

Zero-days, Malware, Spearphishing

Education, Energy, Government, Telecommunications

Cyber threat trends 2022-2023

Targeted Industries

Reference Names

Country

Sponsor

First Seen

Motivation

Method

On the rise: Cyber attacks on Critical Infrastructure

THREAT REPORT

How the war in Ukraine changed the global threat landscape

Sandworm uses a ne version of ArguePat attack targets in Uk

welivesecurity west

independence - and how cyber-risks come into play Soaring energy prices and increased geopolitical tensions amid the Russian invasion of Ukraine bring a

sharp focus on European energy security

Industroyer2: Industro

29 Mar 2022 - 11:30/

welivesecurity west

HermeticWiper: New data-wiping malware hits

undreds of computers in Ukraine compromised just ho

Editor

-

2022 - 10:32AM

Critical infrastrue cyberattack for L Volimi

welivesecurity west

Menu ____

I see what you did there: A look at the CloudMensis macOS spyware



Marc-Etienne M.Léveillé

19 Jul 2022 - 11:30AM

reloaded This ICS-capable malware targets a Ukrainian energy company

ESET Research 12 Apr 2022 - 11:28AM

100 days of war in How the conflict is out in cyberspace It's been 100 days since Russia invaded Ukraine, and we the conflict

Industroyer: A cyber-wea that brought down a pe grid

vesecurity wese

CaddyWiper: New wiper malware discovered in third time in as many weeks that ESET researchers have spotted previously Ukraine

Menu

BY eset

Previously unknown macOS malware uses cloud storage as its C&C channel and to exfiltrate documents, keystrokes, and screen captures from compromised Macs

NIS2 DIRECTIVE

What changes will (Network & Information Security) NIS2 bring?

Besides providing a wider and more detailed scope (see above), NIS2 will bring about the following changes/updates (compared to the original NIS which allowed much flexibility that led to vulnerabilities):

NIS2 security requirements

NIS2 Directive sets out a framework of strengthened security requirements. The measures shall be based on an "all-hazards approach" that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include "at least" the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Compliance Deadline: 17 October 2024

The NIS2 Directive will apply to companies with over 50 employees and over €10 Million yearly turnover. Critical infrastructure, which includes digital infrastructure in NIS2, is affected by the regulations regardless of size.

and sectors:

- Transport (E)
- Energy (E)
- Healthcare (E)
- Public administration (E)
- Aerospace (E)

- Waste management (I)

Digital Providers (I) All medium-sized and large organizations operating within these sectors fall under the NIS2's scope. These are classified to Essential (E) and Important (I) entities **Essential** entities: Must have a pro-active supervision and it is necessary to comply with NIS2 at all

times. **Important** entities:

NIS2 will set the baseline for cybersecurity risk management in these industries

Banking and financial market infrastructure (E)

Water supply and waste (E)

Digital infrastructure and digital service providers (E)

Postal and courier services (I)

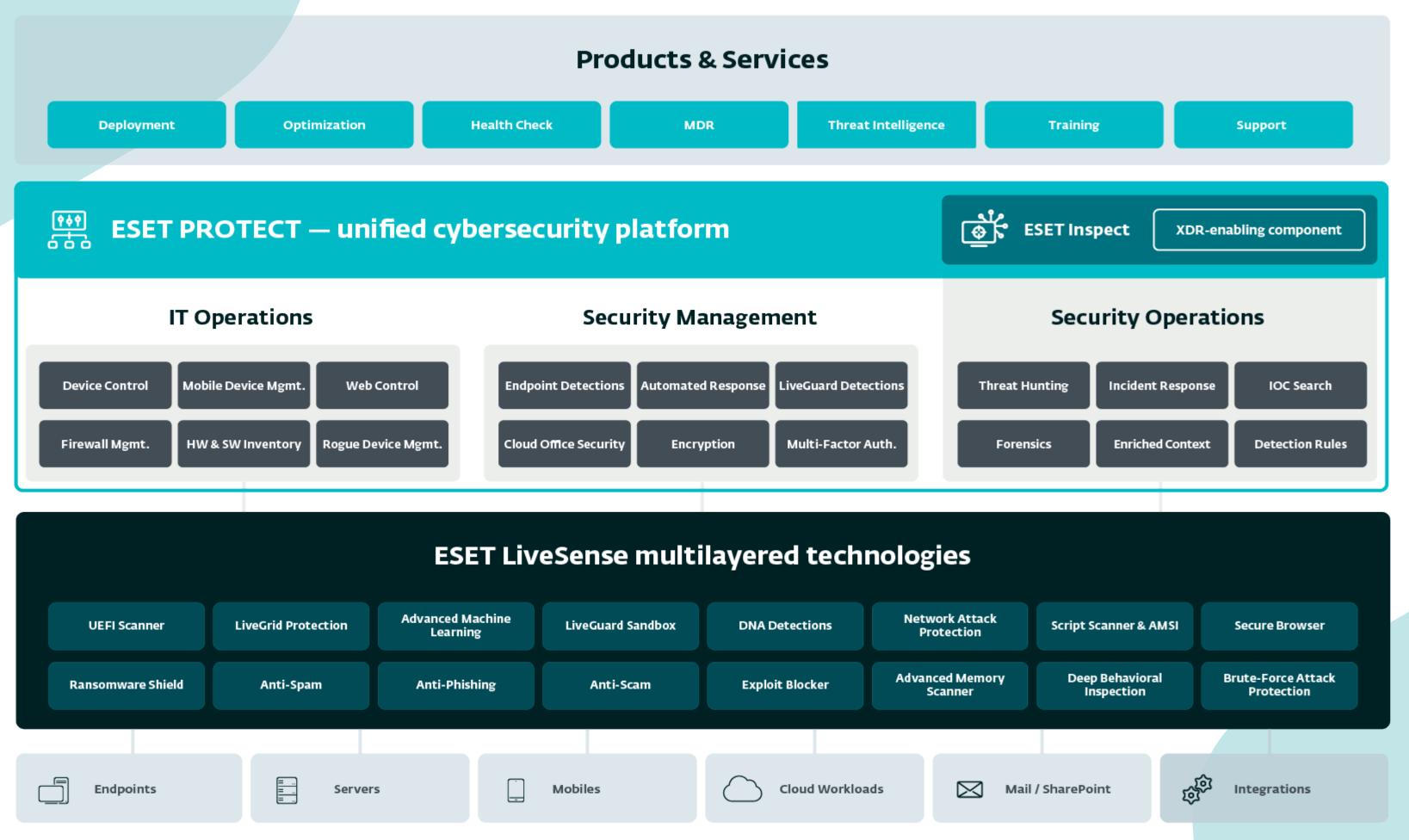
Food production, processing and distribution (I)

Manufacturing of medical devices (I)

Chemical and pharmaceutical production (I)

Will be monitored after an incident of non-compliance is reported.

ESET Approach to Security



Proactive Approach

Endpoint Security & Threat Hunting

Cloud Sandboxing

Vulnerability & Patch Management

> Encryption

>

Threat Intelligence

Insider Threat



> (

Reactive Approach

- Cybersecurity Playbook
- Firewall
- Root Cause Analysis
- **Block Unauthorized Access**
- **Disaster Recovery**

"Cybersecurity is a race between the good guys and the bad guys, and it's just a matter of who gets to the finish line first." - Mikko Hypponen

Thank You!



Digital Security **Progress. Protected.**