



Exposure Management, Intelligenza Artificiale, Servizi, Prodotti: come orientarsi?

Luca Bechelli | CS Clusit
Andrea Muzzi, Technical Manager WithSecure

11.30 - 12.10 – 19 giugno 2024

Luca Bechelli

COMITATO SCIENTIFICO
PARTNER @P4I – GRUPPO DIGITAL360



Andrea Muzzi

Technical Manager WithSecure



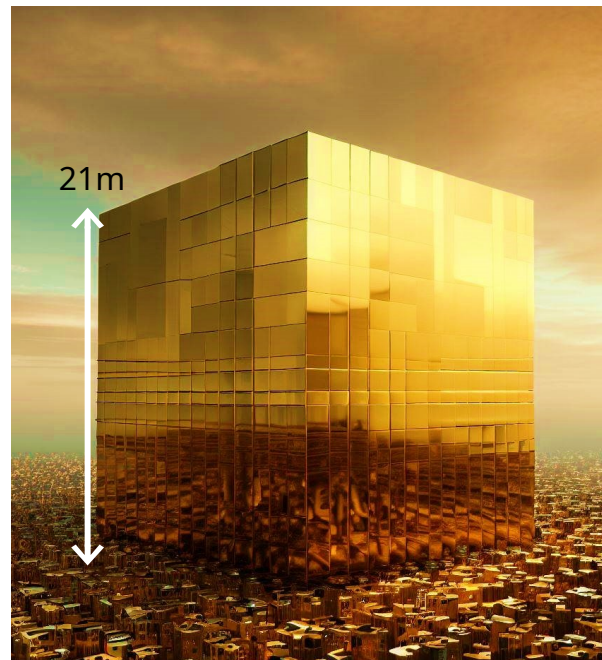
Il crime paga !

Questo cubo rappresenta tutto l'oro estratto nel mondo
Peserebbe 190.040 tonnellate

A 50 dollari al grammo **varrebbe 9,5 trilioni di dollari**
McKinsey & Co **prevede che i costi della criminalità informatica**
a livello mondiale **raggiungeranno i 10,5 trilioni di dollari all'anno**
entro il 2025

Le organizzazioni hanno speso 150 miliardi di dollari nel 2022,
ma la sicurezza informatica rimane una sfida

[https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/
new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers](https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers)



Difficile orientarsi-Normative/Regolamenti obbligatori aziende Italiane

- GDPR (Regolamento Generale sulla Protezione dei Dati).
- Direttiva NIS (Network and Information Security): Alla sua seconda edizione (NIS 2)**
- Legge 81/2008 sulla sicurezza sul lavoro: include disposizioni relative alla sicurezza specialmente per quanto riguarda il telelavoro e l'uso di dispositivi digitali
- Codice dell'Amministrazione Digitale (CAD): Specifico per l'Italia, il CAD stabilisce le regole per l'informatica nelle Pubbliche Amministrazioni.
- Direttiva eIDAS : mira a incrementare la sicurezza delle transazioni elettroniche attraverso l'uso di firme elettroniche
- Regolamentazioni settoriali specifiche: Ad esempio, il settore finanziario e quello sanitario hanno regolamenti dedicati che impongono standard di sicurezza elevati per la protezione dei dati sensibili.

Difficile orientarsi-Principali Framework di sicurezza

- **ISO/IEC 27001:** Uno standard internazionale che fornisce i requisiti per un **sistema di gestione della sicurezza delle informazioni (SGSI)**. Aiuta le organizzazioni a proteggere le informazioni in modo sistematico e costante, garantendo al Cliente finale la sicurezza dei dati.
- **NIST Cybersecurity Framework:** Questo framework offre linee guida volontarie per aiutare le organizzazioni a gestire e ridurre il rischio informatico.
- **Framework MITRE (ATT&CK):** è uno schema globale utilizzato per descrivere il comportamento degli avversari cibernetici. ATT&CK serve come base di conoscenza di tattiche, tecniche e procedure (TTP) utilizzate dagli aggressori durante le fasi di un attacco informatico.
- **PCI DSS (Payment Card Industry Data Security Standard):** è uno standard di sicurezza legato alla Direttiva eIDAS, per i pagamenti elettronici. È obbligatorio per le aziende che elaborano, memorizzano o trasmettono informazioni sulle carte di credito.

Dovrebbe interessarmi..?

Le PMI, che di fatto erano rimaste ben al di fuori della portata della NIS originale potrebbero ora ritrovarsi coinvolte

Potrebbero dover rispondere in concreto nel caso in cui si verificassero delle violazioni dei dati e dei sistemi in cui hanno voce in capitolo per via di un contratto di fornitura.

In altri termini, nella malaugurata ipotesi in cui dovesse verificarsi **un incidente** di sicurezza informatica, **a risponderne non sarà più soltanto l'azienda titolare del servizio, ma anche gli altri stakeholder che intervengono lungo la supply chain.**

L'Italia occupa il quarto posto nella classifica dei paesi dell'Unione Europea **con il maggior numero di sanzioni**, con **oltre 145 milioni di euro richiesti alle aziende dal 2018 ad oggi**. Al primo posto troviamo l'Irlanda, seguita da Lussemburgo e Francia.

Dovrebbe interessarmi..?

Gli obblighi delineati nella NIS2 comprendono principalmente tre aree chiave:

1. **Misure di gestione del rischio**
2. **Segnalazione di incidenti**
3. **Formazione e sensibilizzazione**



Requisiti minimi Nis2

- Punto 2 : Stabilire capacità per rilevare e gestire gli incidenti di sicurezza informatica

NIS2 REQUIREMENTS: 21.2(b)

- Punto 3 : Stabilire capacità per garantire la continuità aziendale durante gli incidenti di sicurezza informatica.

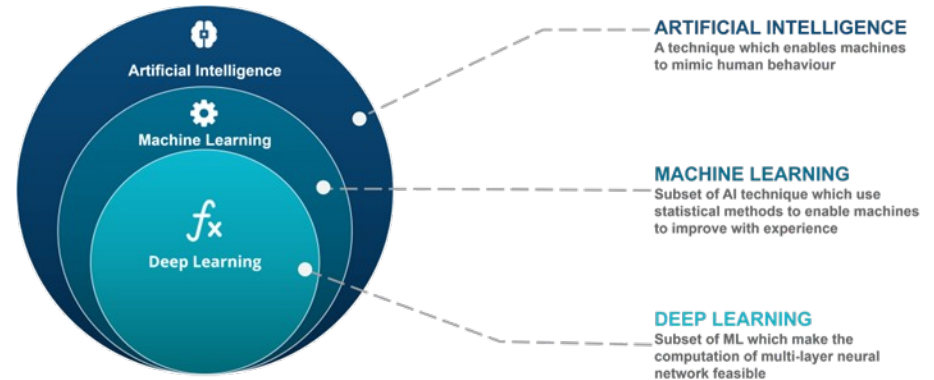
NIS2 REQUIREMENTS 21.2(c)

Cosa intendiamo per AI

L'intelligenza artificiale (AI) consente alle macchine di eseguire compiti che in genere richiedono un'intelligenza simile a quella umana.

L'intelligenza artificiale comprende una gamma di tecniche e approcci, tra cui l'apprendimento automatico, l'elaborazione del linguaggio naturale, la visione artificiale e la robotica.

In questa policy utilizziamo il termine generale "AI" per coprire tutti i modelli e i sistemi relativi all'intelligenza artificiale e il termine è specificato in casi specifici, a seconda delle necessità.



AI i Pilastri fondamentali



AI i Pilastri fondamentali

- Rispetto delle normative pertinenti sulla protezione dei dati (ad esempio GDPR) e politiche sulla privacy e sui dati personali durante la raccolta, l'archiviazione e l'elaborazione dei dati dei clienti o dei dipendenti
- Astenersi dallo sviluppare o implementare sistemi di intelligenza artificiale che potrebbero causare danni a individui, comunità o ambiente.
- Assicurati di essere in grado di “spegnere l'intelligenza artificiale” se necessario.
- Utilizzare il principio di minimizzazione dei dati, definire il periodo di conservazione, la trasparenza, supervisionare eventuali decisioni automatizzate, redigere una valutazione dell'impatto sulla privacy (PIA) prima di utilizzare l'IA modello/sistema e utilizzare tecniche di crittografia e pseudonimizzazione/anonimizzazione ove appropriato
- Affrontare e monitorare regolarmente le questioni relative a potenziali distorsioni nella raccolta dei dati, nella formazione dei modelli

Approccio all' AI - Indietro non si torna

2005 - Machine Learning addestrare motori AntiSpam

2006 - Apprendimento automatico rilevamento file dannosi-entrambi inseriti nelle soluzioni

2008 - DeepGuard, BlackLight e Gemini, un motore di rilevamento del malware basato sull'apprendimento automatico utilizzato in combinazione con la logica di analisi comportamentale lato client

2016 - Sample analysis and categorization - URL reputation and categorization - Breach detection
(We use machine learning techniques to identify suspicious behavior on networks)

2017 - Apertura centro di eccellenza per l' AI

Approccio all' AI – Indietro non si torna

2017 F-Secure lavora anche a un progetto internazionale sull'AI (Progetto Sherpa) con l'obiettivo di studiare come i sistemi di machine learning saranno attaccati –potenziali usi malevoli una volta che diventeranno più diffusi.

2019 – Progetto Blackfin. Utilizzato nella soluzione **Rapid Detection and Response (RDR)** tecniche di intelligenza collettiva come l'intelligenza di sciame e l'apprendimento multi-agente Le interazioni tra questi agenti possono spesso portare all'emergere di comportamenti inaspettati che non sono dissimili dai fenomeni cooperativi che si verificano in natura osservati nei banchi di pesci o nelle colonie di insetti.

2021 - Simulazione di attacchi di avvelenamento contro meccanismi di raccomandazione basati su filtri collaborativi
Social drogati i risultati https://github.com/r0zetta/collaborative_filtering/



WithSecure Elements AI

The screenshot displays the WithSecure Elements AI interface. On the left is a navigation sidebar with categories like ENVIRONMENT, EVENTS, SECURITY CONFIGURATIONS, and MANAGEMENT. The main area shows the 'Security Events' page for 'European Operations' with a 'Generate summary' button. A 'Security events summary' window is open on the right, containing an AI-generated summary of events for May 13-20, 2024, and a table of specific events.

Security Events Summary:

Please note that this summary is AI generated and should be treated with caution. Further investigation and professional consultation may be required to fully address all threats.

Below is a summary of security events for the company **WithElements Inc** generated on May 20, 2024, for the measurement period between May 13, 2024 to May 20, 2024 with **3 devices** and **127 total events**.

- On May 20, 2024, the EDR engine detected a severe lateral movement incident on device **DESKTOP01** (Incident ID: 183720731-1037).
Recommendation: Analyze the incident and update the resolution. If help is needed, the incident can be elevated to WithSecure for further analysis.
- Between May 15 and May 20, 2024, the DeepGuard engine blocked several suspicious applications on devices **DESKTOP01**, **Desktop03**, and **ADServer**. The blocked applications include WINWORD.EXE, Tr-DGg.exe, DG_Malware.exe, Tr-DGr.exe, Malicious_DG.exe, DemoMalware1.exe, DG_TEST_Tr-DGr.exe, and MaliciousFile.exe.
Recommendation: Analyze the processes that triggered the DeepGuard engine and determine if any exclusions are needed in the device profiles.
- On May 15, 2024, the web traffic scanning engine blocked access to the URL "hxxp://hake.takapenkki.net/PsExec64.exe" on device **DESKTOP01**.
Recommendation: Analyze the site and decide if further actions are needed. If necessary, an exclusion can be done in the device profile.

| | Time | Severity | Source | Target |
|---|---------------------------------------|-----------|-------------------------------------|---------|
| 3 | 9 hours ago May 20, 2024, 07:20:09 | Attention | DeepGuard Real-time scanning | DESK... |
| 2 | 9 hours ago May 20, 2024, 07:19:10 | Attention | DeepGuard Real-time scanning | Desk... |
| 1 | 9 hours ago May 20, 2024, | Attention | File scanning Real-time scanning | Desk... |

WithSecure Elements AI

W/ Elements™ European Operations
WithElements Inc

Events / Broad Context Detections

Broad Context Detections

[Broad Context Detections](#) [Event Search](#)

[Back to Detections list](#)

Broad Context Detection 1 of 8

Severe 100 ID: 183720731-1037, Category: Lateral movement

New

Summary Process Tree Analysis Comments Log

Quick actions

Info and above (default)

Generate BCD Summary

Scan device

Collect forensics package

More response actions

Elevate to WithSecure

✓ Elevated

OUTLOOK.EXE WINWORD.EXE POWERSHELL.EXE

POWERSHELL.EXE CERTUTIL.EXE CERTUTIL.EXE POWERSHELL.EXE POWERSHELL.EXE

BCD 183720731-1037

Please note that this summary is AI generated and should be treated with caution. Further investigation and professional consultation may be required to fully address all threats.

Executive Summary:

On 2024-05-20T07:05:22Z/2024-05-20T07:05:50Z, the user 'WITHELEMENTS\michael.smith' on the 'Desktop01.withelements.com' host was observed engaging in a series of suspicious activities. This included the execution of the Microsoft Word application (winword.exe) launching child processes, such as PowerShell (powershell.exe), which were used to download files from external URLs, decode and execute payloads, and create scheduled tasks for persistence (T1059.001 - Command and Scripting Interpreter: PowerShell, T1053 - Scheduled Task/Job, T1204 - User Execution). The CertUtil utility was also used to decode and execute a potential ransomware payload (T1140 - Deobfuscate/Decode Files or

Close

Exposure Management

Elements Exposure Management è un insieme di processi e funzionalità che consentono alle organizzazioni di valutare in modo continuo e coerente l'accessibilità, l'esposizione e la sfruttabilità delle risorse fisiche e digitali.

L'obiettivo principale è ottenere un piano di miglioramento e correzione del livello di sicurezza coerente e attuabile che i dirigenti aziendali possano comprendere e su cui i team tecnici possano agire.

Components of Exposure Management re. Gartner:



Exposure Management in breve



1. Scopri

Scopri il tuo perimetro digitale e identifica le risorse e le identità più critiche

2. Prioritizza

Ottieni consigli pratici e basati sull'intelligenza artificiale su cosa dare la priorità in base ai dati integrati provenienti dall'intelligence sulle minacce, dai percorsi di attacco e dal contesto aziendale.

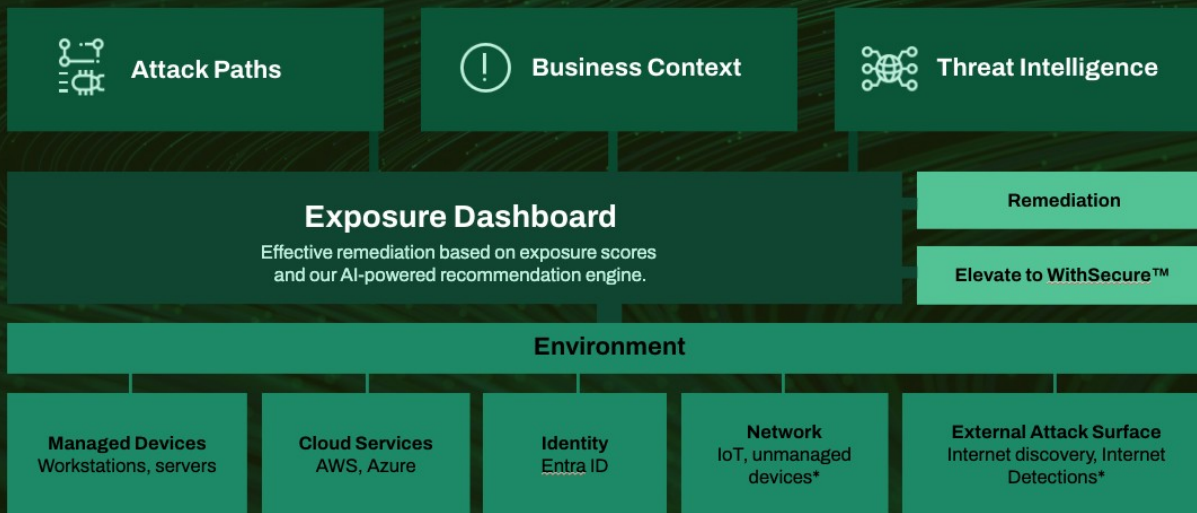
3. Agisci

Implementa azioni correttive prioritarie per ridurre la superficie di attacco e diminuire il livello di rischio aziendale, utilizzando la nostra guida pratica.

WithSecure Elements Exposure Management

WithSecure™ Elements Exposure Management

Continuous assessment of threat exposure, using the attacker's view of your environment.



W / T H
secure

Q&A

Security Summit

Roma, 19 giugno 2024



Contatti

Stand
Mail
Extra