Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

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

PERCHÉ MANAGED DETECTION AND RESPONSE (MDR)?

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 version 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%

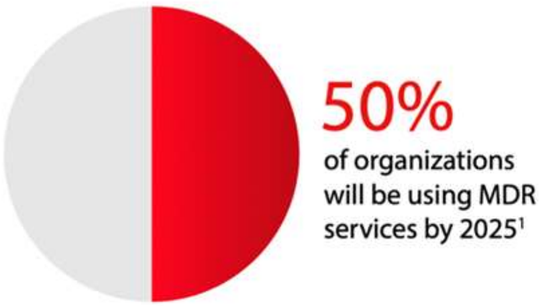
Attacchi Script-based sono ancora 56% del totale

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

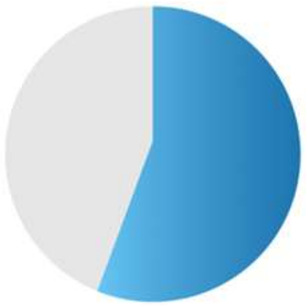
Il rilevamento richiede modelli di Machine Learning o di behavior analysis

Source: WatchGuard Internet Security Report, Q3 2023
https://www.watchguard.com/wgrd-resource-center/security-report-q3-2023

Aumento della domanda di MDR

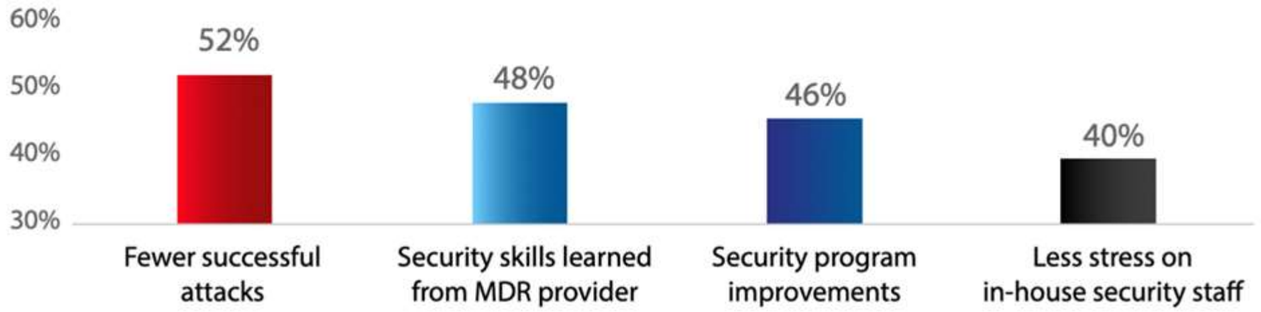


50%
of organizations will be using MDR services by 2025[1]

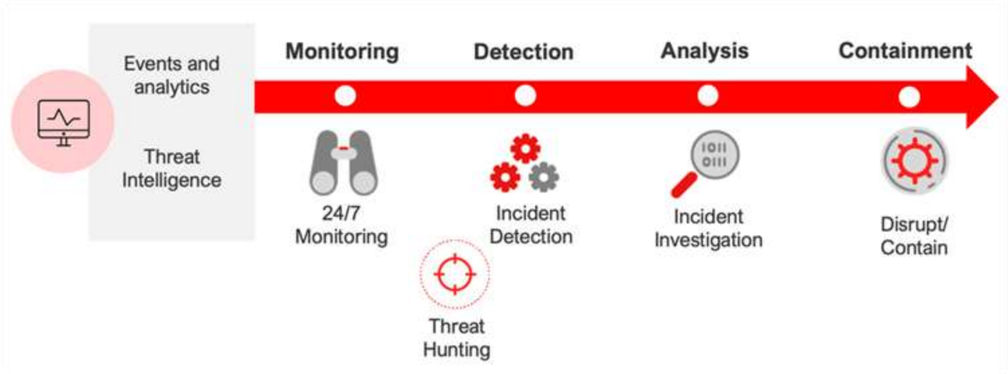


57%
of organizations believe MSPs can do a better job than they can[2]

Midmarket organizations report benefits from MDR[2]



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.**

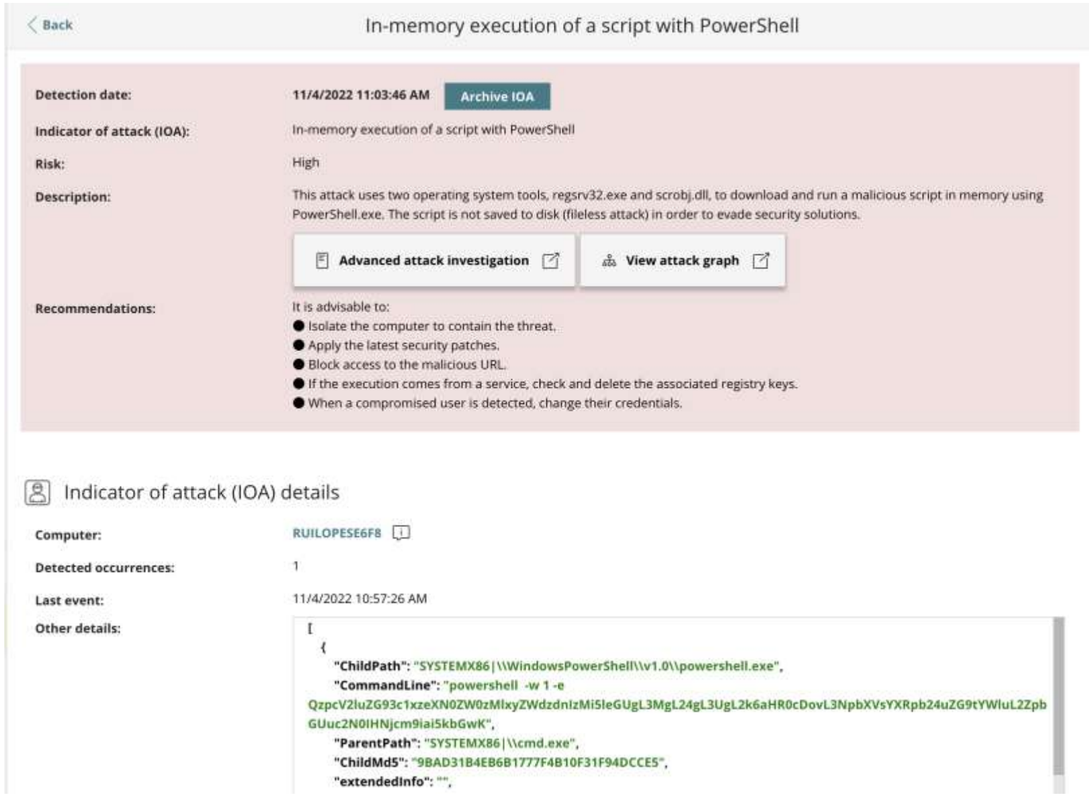
Monitoraggio dell'attivita' di rete 24/7/365

Rapida investigazione delle attivita' 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

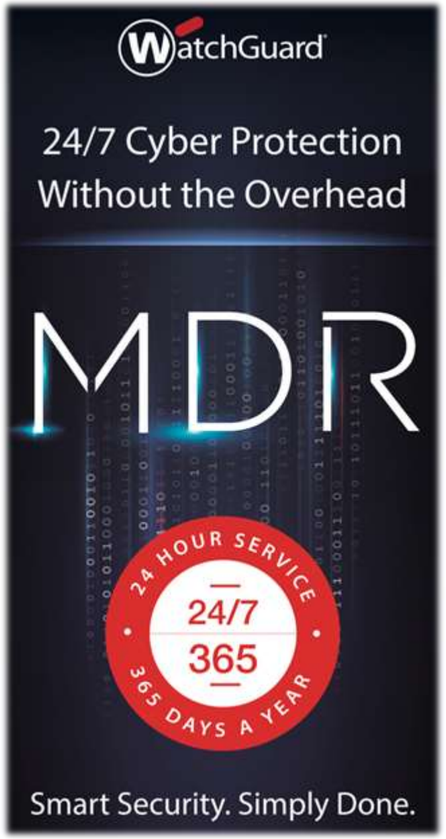
- **LotL (Living-off-the-Land) e attacchi fileless** sono una crescente preoccupazione: essi sono piu' difficili da rilevare e rendono piu' semplice per i cybercriminali attaccare in modo silente
- **Rilevamento dell'attaccante**
  - Trovare attaccanti che utilizzino tecniche Living-off-the-Land
  - 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



WATCHGUARD MDR

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 attivita' sospette

- Indicator of Compromise (IOC): Reattivo
  Analizza un problema di sicurezza che e' appena accaduto
  E' la prova che una compromissione di sicurezza e' accaduta o stava per accadere

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

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?

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:

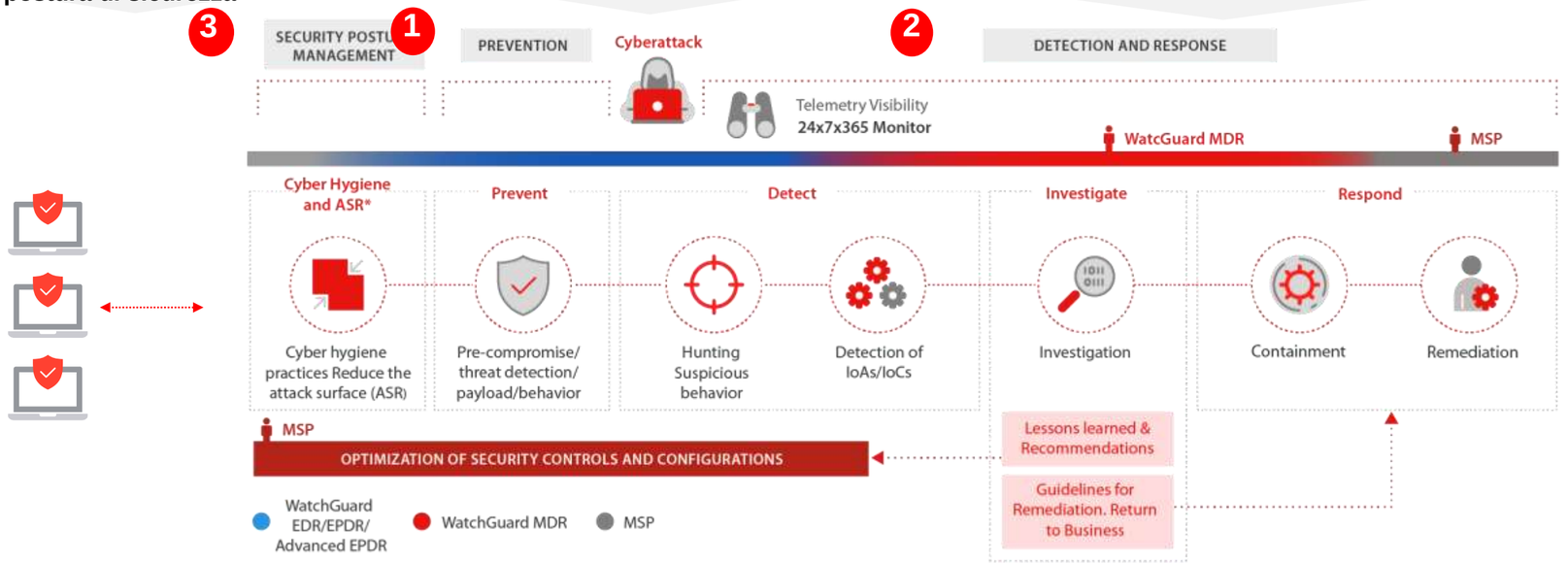
- Filtrare gli incidenti in modo efficiente
- Ridurre il carico di lavoro per lo staff
- Ridurre le violazioni

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**
- **Security analytics nel Cloud**
- **Telemetria 365-day**
- **Threat intelligence**



Requisiti

- MDR si basa sull’installazione di WatchGuard EDR, EPDR o AEPDR

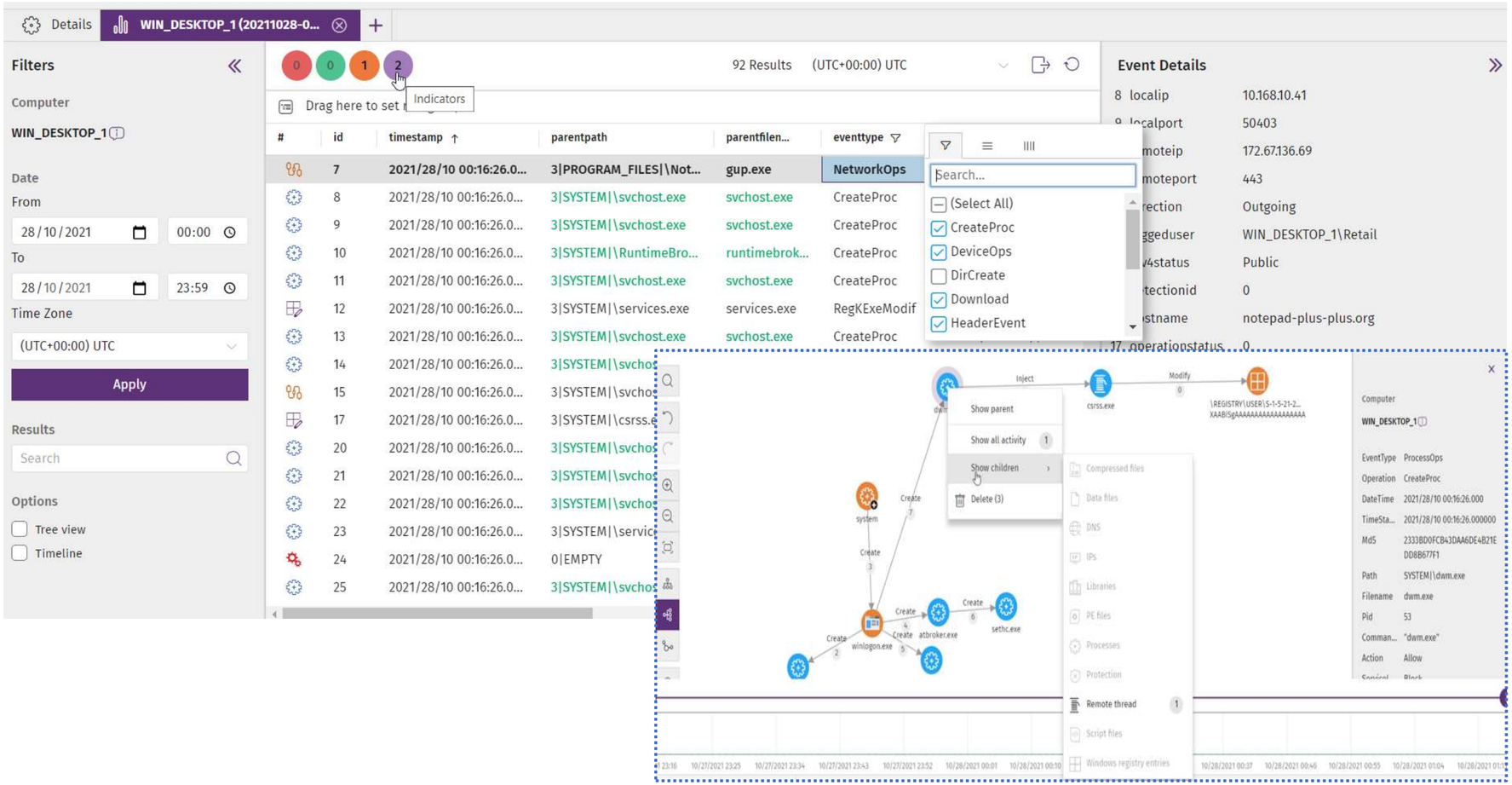
- Almeno una certificazione Tecnica WatchGuard Endpoint Security

- 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 sessione iniziale di onboarding

…Dietro le quinte….



REPORTS

Health assessment – report settimanali

- Disegnato per fornire una overview della postura di sicurezza degli endpoint dei clienti

-Permette un rapida identificazione dei rischi

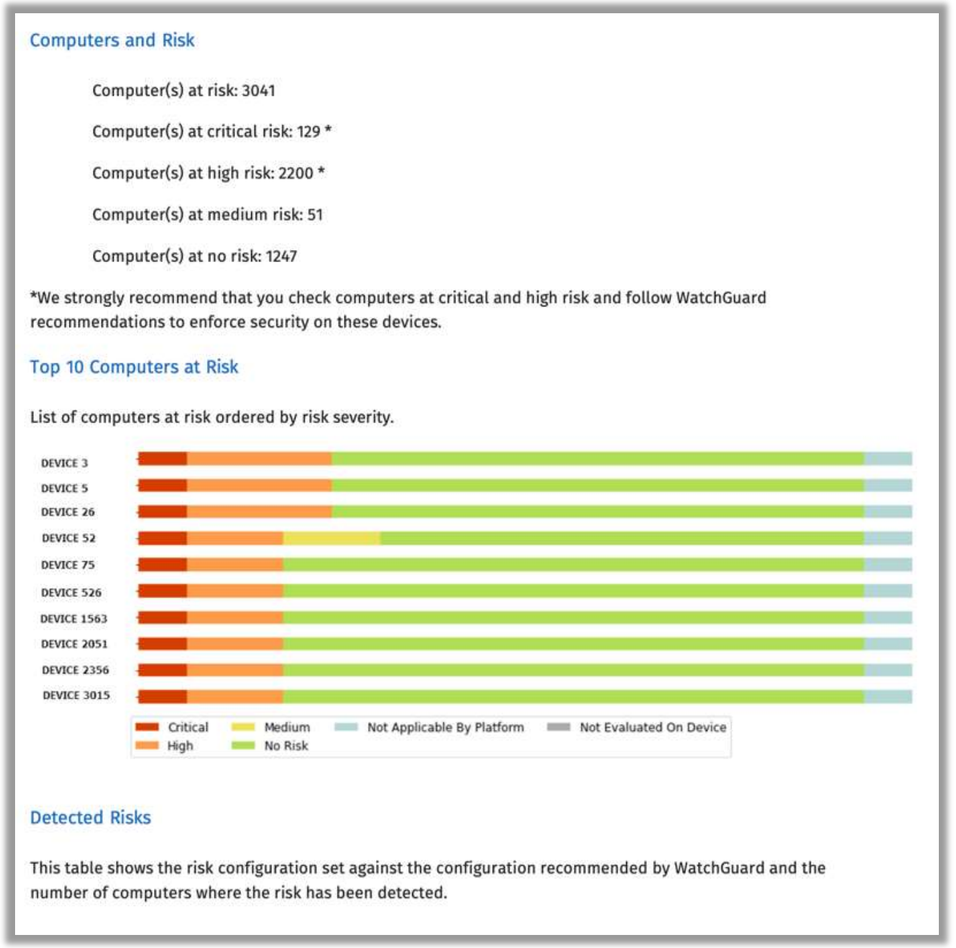
-Contiene sezioni su:

-Endpoint sprovvisti di soluzione WatchGuard Endpoint Security

-Top 10 endpoint a rischio

-Rischi generali individuati negli endpoint

-Evoluzioni dei rischi

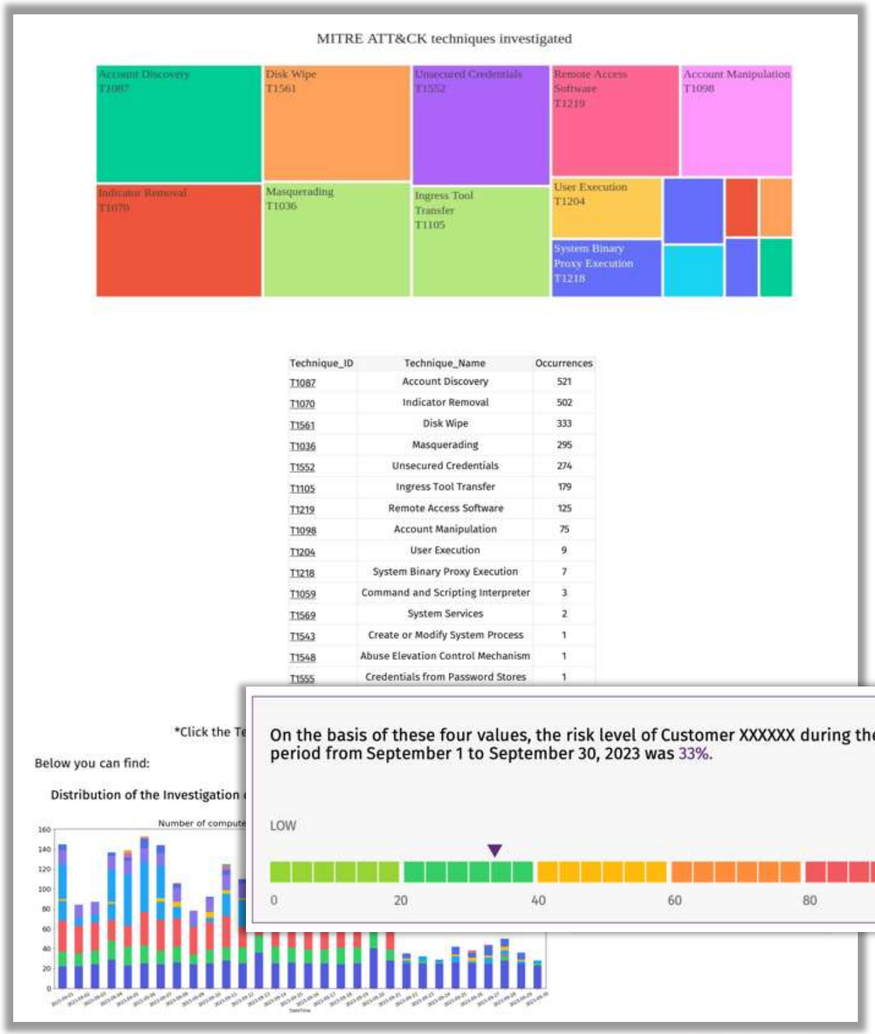


Service activity – report mensili

- Fornisce una sinossi di rilevamenti, investigazioni e contenimento degli incidenti e relative attivita' effettuate dal team del WatchGuard SOC

- I Partner possono usare questo report per avere nuove opportunita' di discussion 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 persenti nell'organizzazione
  - Attivita' mensile effettuata
  - Attivita' anomala investigata
  - Tentativi di attacco indentificati e comunicati



Q&A

VIENI A TROVARCI AL NOSTRO STAND!

CONTATTI:
GIANLUCA.PUCCI@WATCHGUARD.COM