Report Minacce comuni W19D1

In questo report spiegheremo in due tabelle riassuntive i livelli di valutazione di Threat Connect per quanto riguarda il Threat Rating e il Confidence Rating.

Threat Rating

L’indicatore di Threat Rating è misurato su una scala da 0 a 5 teschi.
Nella propria organizzazione, è possibile creare una scala che differenzi tra un indicatore basso e uno elevato, nella tabella sottostante è stato riassunto il significato di ogni livello.

Livello	Teschi	Descrizione
Sconosciuto	0	Non ci sono informazioni sufficienti per identificare il livello della minaccia.
Sospetto	1	Non c’è stata attività malevola confermata associata all’indicatore. Ci sono però comunque attività sospette da analizzare.
Minaccia bassa	2	L’indicatore rappresenta un avversario poco sofisticato che potrebbe agire in modo opportunista ed effimero oppure indica attività preliminari a una compromissione.
Minaccia moderata	3	L’indicatore rappresenta un avversario capace le cui azioni sono moderatamente dirette e determinate. Questo tipo di minaccia è tipicamente associato alle fasi di consegna, sfruttamento o installazione di un attacco.
Minaccia alta	4	L’indicatore può essere attribuito ad un avversario avanzato. Indica che l’attività mirata e persistente è già in corso.
Minaccia	5	L’indicatore rappresenta un avversario altamente qualificato e con risorse significative. Questo livello di classificazione va riservato a indicatori provenienti da attori con capacità illimitate e che rappresentano un pericolo in qualsiasi fase dell'intrusione.

Confidence Rating

Analizzando solamente la parte di Threat Rating, non abbiamo un quadro completo della situazione, per questo motivo Threat Connect mette a disposizione un'ulteriore metro di giudizio da 0 a 100 per valutare l'indicatore assegnato alla minaccia.

Livello	Rating	Descrizione
Confermato	90 - 100	La valutazione è stata confermata da fonti indipendenti o attraverso un'analisi diretta ed è in accordo con altre informazioni sul soggetto.
Probabile	70 - 89	Anche se la valutazione non è direttamente confermata, è in accordo con altre informazioni sul soggetto.
Possibile	50 - 69	La valutazione non è confermata ed solo in parte in accordo con le informazioni sul soggetto.
Dubbiosa	30 - 49	La valutazione è possibile, ma non è la deduzione più logica. Inoltre non può essere corroborata o ripudiata dalle informazioni sul soggetto.
Improbabile	2 - 29	La valutazione è possibile, ma non è la deduzione più logica. È inoltre direttamente screditata dalle informazioni aggiuntive sul soggetto.
Screditata	1	La valutazione è confermata come inesatta.
Non valutata	0	Non è stato assegnato nessun Confidence Rating all'indicatore.

Facoltativo

Creare un elenco compreso di descrizioni e analisi dettagliate sulle minacce più comuni alla sicurezza informatica di un’azienda.

Phishing/smishing

- Descrizione: Tecnica di social engineering in cui l’attaccante invia email o messaggi che sembrano provenire da fonti attendibili, in modo da ingannare l’utente e ottenere informazioni sensibili.
- Danni potenziali: Perdita di dati, furto d’identità, accessi non autorizzati, perdite economiche.

Malware

- Descrizione: Software dannoso progettato per infiltrarsi nei sistemi informatici allo scopo di arrecare danno e disservizi.
  Alcuni esempi sono: virus, worm, trojan, spyware, ransomeware.
- Danni potenziali: Furto o perdita di dati, interruzione del servizio, richiesta di riscatto (ransomeware).

Attacchi DDOS (Distributed Denial of Service)

- Descrizione: Questo tipo di attacco mira a sovraccaricare un server, un sito o un asset con enormi quantità di traffico allo scopo di rendere il target inaccessibile agli utenti legittimi.
- Danni potenziali: Perdita di reputazione e clienti, interruzione dei servizi, perdite monetarie.

Furto di dati

- Descrizione: Accesso non autorizzato a informazioni sensibili allo scopo di sfruttarle o rivenderle.
- Danni potenziali: Perdita di fiducia da parte dei clienti, violazione della privacy, sanzioni legali.

Vulnerabilità software

- Descrizione: Sfruttamento di falle di sicurezza nei software aziendali dovute a poca sicurezza, asset non aggiornati, sistemi configurati in modo sbagliato e in generale la non conformità alle best practices.
- Danni potenziali: Accesso remoto ai sistemi, diffusione di malware ed esfiltrazione dei dati.

Insider threat

- Descrizione: Dipendenti o collaboratori dell’azienda che sfruttano i loro accessi per arrecare danno (volutamente o involontariamente).
- Danni potenziali: Sabotaggio, furto di dati, perdita di proprietà intellettuale.

Pratica extra

Scenario 1

- OWASP top 10: A03:2021 - Injection
- MITRE ATT&CK Enterprise tactic: TA0001 - Initial access
- MITRE ATT&CK Enterprise tecnique: T1659 - Content injection
- Mitigazioni MITRE ATT&CK suggerite: M1041 -Encrypt Sensitive Information, M1021 - Restrict Web-Based Content

Scenario 2

- OWASP top 10: A01:2021 - Broken access control
- MITRE ATT&CK Enterprise tactic: TA0001 - Initial access
- MITRE ATT&CK Enterprise tecnique: T1190 - Exploit Public-Facing Application
- Mitigazioni MITRE ATT&CK suggerite: M1048 - Application Isolation and Sandboxing, M1050 - Exploit Protection, M1035 - Limit Access to Resource Over Network, M1030 - Network Segmentation, M1026 - Privileged Account Management, M1051- Update Software, M1016 - Vulnerability Scanning

Scenario 3

- OWASP top 10: A08:2021 - Software and Data Integrity Failures
- MITRE ATT&CK Enterprise tactic: TA00002 - Execution
- MITRE ATT&CK Enterprise tecnique: T1203 - Exploitation for Client Execution
- Mitigazioni MITRE ATT&CK suggerite: M1048 - Application Isolation and Sandboxing, M1050 - Exploit Protection, M1051 - Update Software