Sigurnosne prijetnje na Internetu

Threat Hunting

Matija Alojz Stuhne, 15.1.2025.

Pregled predavanja

1. Motivacija
2. Pitanja za ispit
3. Threat Hunting
4. MITRE ATT&CK
5. Stvarni i potencijalni primjeri
6. Zaključak

Pitanja za ispite

- Što je to Threat Hunting te što mu je cilj?
- Objasnite razliku između reaktivnog i proaktivnog pristupa kibernetičkoj sigurnosti.
- Ukratko opišite proces Threat Hunting-a.
- Navedite važnost baze znanja MITRE ATT&CK.
- Što su to taktike, a što tehnike opisane bazom znanja MITRE ATT&CK. Navodite po jedan primjer za svaku.

Motivacija

- Zašto je Threat Hunting važna tema?
  - Moderni napadi, poput *APT*-ova, sve su sofisticiraniji.
  - Tradicionalni alati često ne prepoznaju prijetnje na vrijeme.
  - Lov na prijetnje omogućuje rano otkrivanje i sprječavanje velikih incidenata.

Povećana potražnja za stručnjacima koji su upoznati sa navedenim područjem.

Threat Hunting - Općenito

- Proaktivna strategija identificiranja kibernetičkih prijetnji te ranjivosti sustava.
  - Cilj je identificirati prijetnje prije nego što one uzrokuju značajnu štetu unutar sustava.

- Uključuje potragu za i izolaciju naprednih prijetnji koje nisu detektirane od strane tradicionalnih sigurnosnih alata.

- Poželjno je dijeliti otkrivene prijetnje sa zajednicom u svrhu prevencije budućih napada.

Threat Hunting - Općenito

Reaktivan pristup ***- Incident Response -***	**<u>Proaktivan pristup</u>** ***- Threat Hunting -***
• Prijetnja se detektira tek nakon što je kibernetički napad već pokrenut i njegov cilj je već ispunjen. • Re(akcije) su usmjerene na ograničavanje utjecaja napadača, smanjenje vremena oporavka i smanjenje financijskih troškova.	• Aktivno traženje prijetnji u svrhu sprječavanja potencijalne štete. --> Pristup: "bolje spriječiti nego liječiti". • Provodi se proučavanje sistemskih podataka te korištenjem dostupnih obavještajnih podataka o prijetnjama. • Pokušavaju se otkriti potencijalne prijetnje koje nisu detektirane od strane tradicionalnih sigurnosnih alata.

Threat Hunting – Proces - *Assume breach*

Podatci
Prikupljanje heterogenih podataka.

Hipoteza
Postavljanje hipoteze o potencijalnim prijetnjama.

Lov
Potraga za tragovima štetnog djelovanja koji potvrđuju hipotezu.

Klasifikacija
Identificirane prijetnje kategoriziraju se u skupine prema karakteristikama.

Evaluacija
Ljudski analitičar provjerava klasifikaciju prijetnji te moguću pojavu lažnih pozitivnih vrijednosti.

Reakcija
Korištenje prikupljenih informacija u svrhu bolje zaštite sustava.

Threat Hunting - Općenito

	IoC ***- Indicator of Compromise -*** **Indikatori kompromitacije**	**TTP** ***- Tactics, techniques, and procedures -*** **Taktike, tehnike i procedure**	**CK** ***- Common Knowledge -*** **Opće poznato znanje**
Fokus	Što se dogodilo.	Kako napadač djeluje.	Skup poznatih korištenih tehnika i napada.
Upotreba	Reaktivna analiza.	Proaktivni lov.	Proaktivni lov.
Primjeri	Hash neke datoteke, zlonamjerne IP adrese, ...	Phishing, Exploitation of Remote Services, ...	Poznate aktualne zloćudne kampanje.
Vrijeme detekcije	Nakon kompromitacije.	Tijekom ili prije napada.	Tijekom ili prije napada.
	Proces lova na prijetnje koristi sve ove informacije.		

Threat Hunting - Korišteni alati

Ručni	Automatizirani
• **alati digitalne forenzike** (Yara, VirusTotal…) • **alati za praćenje mrežnih aktivnosti** (Wireshark, …) • **platforme i baze znanja s korisnim informacijama** (MITRE ATT&CK, MISP)	• **SIEM sustavi** (IBM QRadar, LogRhythm, ...) • **EDR rješenja** (Crowdstrike Falcon, Microsoft Defender for Endpoint, …) • **NDR rješenja** (Darktrace DETECT, Cisco Secure Network Analytics, ...) • **MDR rješenja** (Crowdstrike Falcon, SentinelOne Vigilance Respond, …)

MITRE ATT&CK

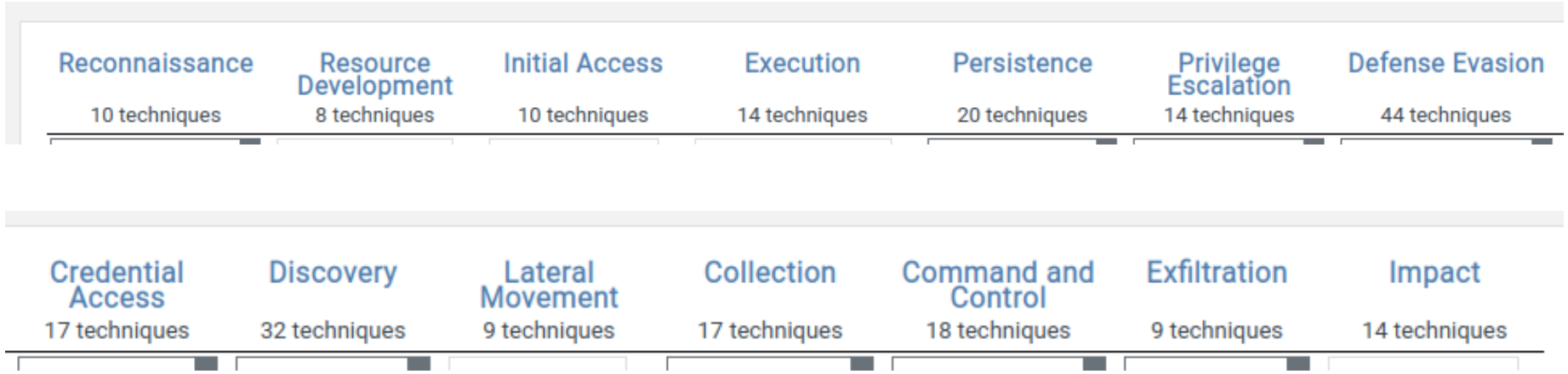
- (*Adversarial Tactics, Techniques, and Common Knowledge*)
- Predstavlja bazu znanja koja sadrži strukturirani popis taktika, tehnika i procedura koje koriste napadači.

- Nudi standardizirani okvir za mapiranje uočenih problematičnih sigurnosnih događaja na moguće taktike i tehnike napadača.
  --> Stručnjaci i automatizirani alati imaju "zajednički jezik".

- Taktike opisuju zašto napadač nešto radi, dok tehnike opisuju kako to radi. Svaka taktika unutar sebe sadrži različite tehnike te primjere njihovih upotreba u stvarnim napadima.

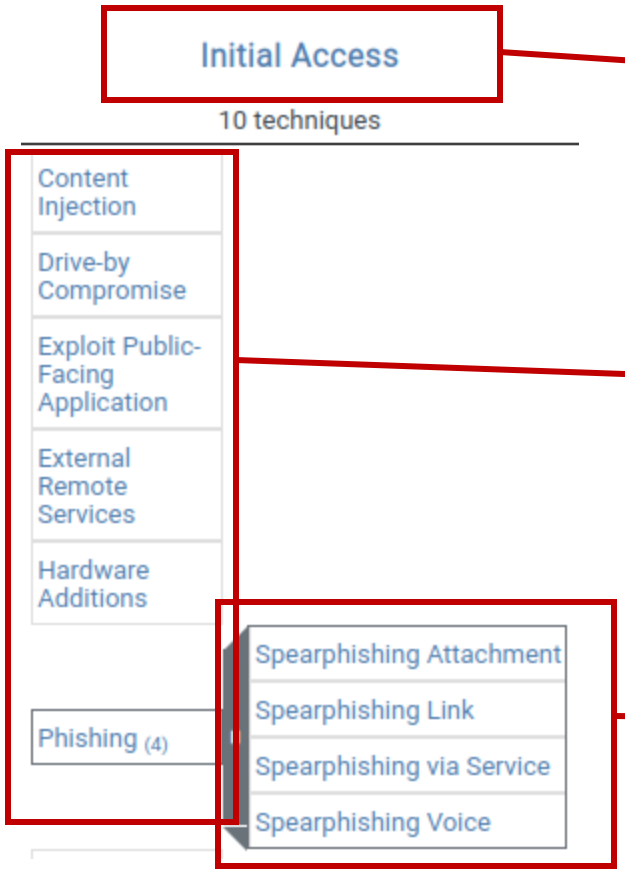
MITRE ATT&CK

- Taktike su prikazane unutar ATT&CK matrice.
  - ATT&CK matrica je vizualni prikaz taktika i tehnika koje napadači koriste u različitim fazama kibernetičkog napada.
- Prikaz taktika unutar ATT&CK matrice:



MITRE ATT&CK

ATT&CK®



TAKTIKA – Zašto? - Inicijalni pristup

TEHNIKA – Kako? - npr. Phishing

PODTEHNIKE - specifične implementacije tehnike – npr. putem zloćudne poveznice ili zloćudne datoteke

Threat Hunting – Stvarni primjer

- Povreda osobnih podataka – Uber 2022.

- Primjećeni sumnjivi pokušaji prijave u sustav te sumnjivi pokušaji pristupa podatcima unutar sustava. --> Hipoteza: Okidač je bila phishing kampanja.
- Prikupljeni su postojeći logovi elektroničke pošte, aplikacijski logovi te podatci o mrežnom prometu. --> Analiza: Fokus stavljen na identifikaciju postojanja žrtava kampanje.
- Analizom je utvrđeno postojanje kompromitiranih računa zaposlenika Uber-a. Identificirane su phishing poruke e-pošte te zlonamjerne poveznice.
- Opozvana su prava koja su imali kompromitirani računi te su im resetirane lozinke. Uvedena je višefaktorska autentifikacija unutar cijele kompanije.
- Osvježena je baza znanja unutar kompanije, ali i zajednice koja se bavi kibernetičkom sigurnosti. Također je provedena odgovarajuća edukacija unutar kompanije od strane tima za kibernetičku sigurnost.

Threat Hunting – Potencijalni primjer

- Automatizirani alati primijetili su neuobičajeni mrežni promet i potencijalno preuzimanje zlućudnih datoteka unutar sustava. --> Hipoteza: U tijeku je sofisticirani napad.
- Korištena su YARA pravila kako bi se pokušali pronaći potencijalni znakovi prisutnosti zlućudnih datoteka. --> Analiza: Pronađeni su tragovi izbrisanih datoteka koje upućuju na moguću prisutnost zlućudnih programa za udaljeni pristup na nekom od računala u sustavu.
- Daljnjim istraživanjem (korištena je metoda *backtrack*-inga) otkriveno je da su na određeno računalo preuzeti brojni alati za pokušaj napada grubom silom, u svrhu dobivanja vjerodajnica za *Remote Desktop Protocol* (napad je bio uspješan, s obzirom na preuzimanje zlućudnih datoteka na računalo).
- Opozvane su sve vjerodajnice povezane sa napadnutim računalom te je ono stavljeno u izolaciju od ostatka sustava.
- Predloženo je korištenje višefaktorske autentifikacije za sve sustave koji koriste vjerodajnice te blokiranje svih upita prema nekorištenim RDP vratima.

Zaključak

- Postojanje vještine kao što je Threat Hunting od iznimne je važnosti u današnjem svijetu.

- Proaktivan pristup omogućava otkrivanje naprednih prijetnji prije nego što one uzrokuju nepopravljivu štetu organizacijama te, nama bitnije, korisnicima njihovih usluga.

- Kao temelj uspješnog lova na kibernetičke prijetnje ponajviše se izdvaja ažurnost i informiranost samog lovca o aktualnim i već korištenim napadima.

Literatura

- Mahboubi, Arash, et al. "Evolving techniques in cyber threat hunting: A systematic review." Journal of Network and Computer Applications (2024): 104004.
  - https://www.sciencedirect.com/science/article/pii/S1084804524001814
- Strom, Blake E., et al. "Finding cyber threats with ATT&CK-based analytics." The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202 (2017).
  - https://www.mitre.org/news-insights/publication/finding-cyber-threats-attck-based-analytics
- Jadidi, Zahra, and Yi Lu. "A threat hunting framework for industrial control systems." IEEE Access 9 (2021): 164118-164130.
  - https://ieeexplore.ieee.org/document/9638634
- Ajmal, Abdul Basit, et al. "Offensive security: Towards proactive threat hunting via adversary emulation." IEEE Access 9 (2021): 126023-126033.
  - https://ieeexplore.ieee.org/document/9511495
- IBM | What is Threat Hunting? | siječanj 2025.
  - https://www.ibm.com/think/topics/threat-hunting
- MITRE | ATT&CK | siječanj 2025.
  - https://attack.mitre.org/
- Syscomm | Threat Hunting Real World Examples | siječanj 2025.
  - https://www.syscomm.co.uk/cyber-security/the-essentials-of-threat-hunting-real-world-examples/
- Sentiel One | Revolutionizing Adaptive Threat Hunting | siječanj 2025.
  - https://www.sentinelone.com/blog/chained-detections-revolutionizing-adaptive-threat-hunting

Hvala!