Lovecká sezóna

RNDr. Ján Kromel, PhD.

Základné informácie o spoločnosti

- Pôsobenie na trhu od roku 1991
- Viac ako 100 zamestnancov
- Sídla spoločnosti v Bratislave a v Košiciach
- Certifikácia spoločnosti podľa noriem: ISO 9001, ISO 14001, ISO/IEC 27001, ISO/IEC 20000-1, ISO 45001 a ISO 10006
- Ponúkame špičkové služby v oblasti projektovania, výstavby, prevádzkovania a bezpečnosti informačných systémov, networkingu, komplexnej bezpečnosti organizácií a špeciálnych aplikácií.

whoami

- Vedúci oddelenia Forenzných analýz a penetračného testovania
- Sun Certified System Administrator
- Certified GIAC Mobile Device Security Analyst
- Certified GIAC Reverse Engineering Malware
- **Najpodstatnejšie**: celoživotný začiatočník v oblasti kybernetickej bezpečnosti, keďže je toľko veľa čo je potrebné sa naučiť a tak málo času… ☺

Upozornenie: Informácie uvedené v prezentácii nie sú „zákonom“, ale námetmi na zamyslenie ☺

Obsah

- Threat Hunting? Huh...?
- Marketing náš každodenný...
- Threat Hunter: lovec alebo lovná zver ..?
- Lov začína ... ☺

Threat Hunting? Huh…?

Threat Hunting? Huh...?

- **Proaktívny proces** zvýšenia ochrany aktív ☺
- Realizovaný pomocou kontinuálneho prehľadávania aktív
- Ďalšie zbytočné výdaje?! Veď máme AV (host sec), DLP, FW a podobne...
  - Cieľom Threat Huntingu je identifikácia a izolácia pokročilých hrozieb, ktoré obchádzajú implementované bezpečnostné riešenia.
- Threat Hunting je **iteratívny proces**, kde prvotným vstupným údajom môže byť napr. výstup Threat Intelligence > IOC a IOA > Threat Hunting
- Analytik pracuje s prvotnou hypotézou (hypotézami)

Marketing náš každodenný...
(alebo „Nikto Vám nemôže dať toľko, koľko Vám s naším produktom vieme sľúbiť!“)

Marketing náš každodenný...

- Marketing
  - Vyhliadka „krajšej“, „bezpečnejšej“ budúcnosti ;)
  - Produkty (napr. EDR/XDR) často predstavované ako plnoautomatizované „magické všelieky na bolesti bezpečákov“
  - Ohromujúce prezentačné videá a demo ukážky na „živých“ prostrediach
- Realita
  - Implementácia ako podľa manuálu až do doby, pokiaľ zákazník nepožaduje „neštandardné“ konfigurácie
  - Z automatizovaného procesu sa stáva nočná mora bezpečnostného tímu = od nefunkčnosti deklarovanej „magickej“ funkcionality až po „novovzniknutý“ problém nedostatku ľudských zdrojov

Threat Hunter: lovec alebo lovná zver ..?

Threat Hunter: lovec alebo lovná zver ..?

- Threat Hunter: lovec (analytik poľuje na útočníka)
  - Zavedený proces Threat Huntingu
    - Zabezpečený zber potrebných údajov
    - Dostatočný počet ľudských zdrojov (interných, alebo externých ako služba)
  - Implementovaný nástroj pre Threat Hunting
    - Dedikované ľudské zdroje pre **správu nástroja aj analýzu údajov**
- Threat Hunter: lovná zver (manažment poľuje na analytika)
  - Nezavedený proces Threat Hunting
    - Činnosti vykonávané kamikadze štýlom „Veď na to máte TEN nástroj, tak robte!“
    - Nezabezpečený zber potrebných údajov
    - Nedostatočný (vo veľa prípadoch nulový) počet dedikovaných ľudských zdrojov
  - Zakúpený a implementovaný nástroj Threat Hunting
    - Neexistencia dedikovaných ľudských zdrojov, nástroj si žije vlastným životom a vo veľa prípadoch sa stáva zbraňou proti bezpečnostnému teamu

Lov začína...

Lov začína

- Threat Hunting je **proces, nie technológia/softvér/a podobne**!
- Analytik (Threat Hunter) je najkritickejším „komponentom“ procesu Threat Huntingu, nie softvér!
  - Je dobré zvážiť možnosť využitia špecializovaných externých služieb
- Softvérové nástroje „napomáhajú a uľahčujú život“ analytikom, ale je potrebné k nim pristupovať realisticky
- Threat Hunting je potrebné budovať od základov, nie od strechy a preto:

Pozor, aby sa pod nátlakom vonkajších faktorov z lovca nestala korisť

Ďakujem za pozornosť

Tel: +421 55 727 17 17 | E-mail: lynx@lynx.sk

LYNX - spoločnosť s ručením obmedzeným Košice

www.lynx.sk