CYFIRMA

DECODING THREATS

CHCETE VĚDĚT V PŘEDSTIHU KDY, KDE A JAK MŮŽE BÝT VAŠE ORGANIZACE Nnapadena?

LUKÁŠ ŽIDLICKÝ

COUNTRY MANAGER CZECH REPUBLIC – PRIANTO GMBH

PROČ DĚLÁME TO, CO DĚLÁME

KDYSI DÁVNO...

Každý okamžik má svou historii

- Koncept kybernetické bezpečnosti má své kořeny v 70. letech 20. století a od 90. let 20. století se stává stále viditelnějším.
- Jednoduché metody přerostly v sofistikované metody útoku a obrany.

Správné nastavení mysli vám může pomoci

- Byl jsi napadem ať už to víš nebo nikoliv
- Bezpečnostní kontroly umožňují zabezpečit vaši organizaci
  - Používání přístupových práv s automatizovanou správou
  - Přesnější strukturování infrastruktury pomocí oddělení sítí
  - Implementujte zabezpečení koncových bodů
  - Identifikujte společné bezpečnostní parametry: Identity a jejich přístupová oprávnění

Budoucnost bohužel začíná vždy dnes

- Změna infrastruktury, např. zavedením SaaS, PaaS a základního cloudu, vede ke složitějším bezpečnostním výzvám.
- Interoperabilita mezi různými organizacemi vede k odhalení kybernetického prostoru.

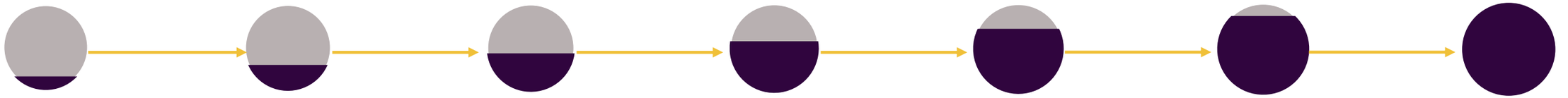
Bezpečný "vnitřek" vás neochrání před zlem z "venku".

CYFIRMA
DECODING THREATS

PROČ DĚLÁME TO, CO DĚLÁME

IDENTIFIKOVALI JSME MOŽNOSTI, JAK ZABRÁNIT ÚTOKŮM.

Struktura útoku



1. Rozpoznávání

Skenování prostředí nebo získávání informací z různých zdrojů.

2. Vyzbrojování

Spojení škodlivého kódu s exploitem za účelem vytvoření zbraně (Piece of Malware)

3. Doručení

Přenos zbraně/malwaru k cíli (např. prostřednictvím e-mailu, vniknutí, spoofingu, phishingu atd.).

4. Operace

Po doručení se zbraně/malware spustí při nějaké akci. Ten následně zneužije zranitelnost.

5. Instalace

Zbraň nainstaluje do systému malware.

6. Velení a řízení

Příkazový kanál pro vzdálenou manipulaci s obětí

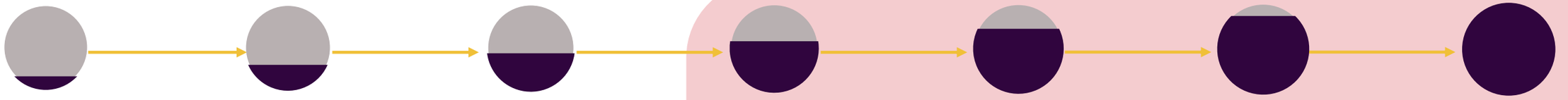
7. Opatření k cílům

S rukama na vstupu dosáhne útočník svého cíle

PROČ DĚLÁME TO, CO DĚLÁME

IDENTIFIKOVALI JSME MOŽNOSTI, JAK ZABRÁNIT ÚTOKŮM.

Struktura útoku



1. Rozpoznávání

Skenování prostředí nebo získávání informací z různých zdrojů.

2. Vyzbrojování

Spojení škodlivého kódu s exploitem za účelem vytvoření zbraně (Piece of Malware)

3. Doručení

Přenos zbraně/malwaru k cíli (např. prostřednictvím e-mailu, vniknutí, spoofingu, phishingu atd.).

4. Operace

Po doručení se zbraně/malware spustí při nějaké akci. Ten následně zneužije zranitelnost.

5. Instalace

Zbraň nainstaluje do systému malware.

6. Velení a řízení

Příkazový kanál pro vzdálenou manipulaci s obětí

7. Opatření k cílům

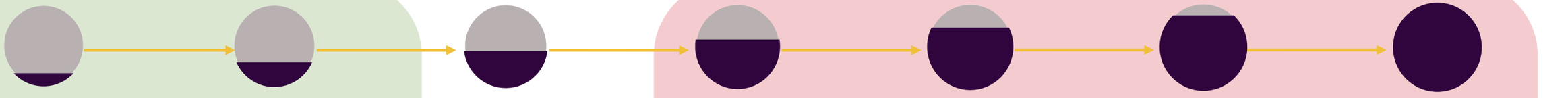
S rukama na vstupu dosáhne útočník svého cíle

Tradiční přístupy k reakci na identifikované kybernetické hrozby

PROČ DĚLÁME TO, CO DĚLÁME

IDENTIFIKOVALI JSME MOŽNOSTI, JAK ZABRÁNIT ÚTOKŮM.

Struktura útoku



1. Rozpoznávání

Skenování prostředí nebo získávání informací z různých zdrojů.

2. Vyzbrojování

Spojení škodlivého kódu s exploitem za účelem vytvoření zbraně (Piece of Malware)

3. Doručení

Přenos zbraně/malwaru k cíli (např. prostřednictvím e-mailu, vniknutí, spoofingu, phishingu atd.).

4. Operace

Po doručení se zbraně/malware spustí při nějaké akci. Ten následně zneužije zranitelnost.

5. Instalace

Zbraň nainstaluje do systému malware.

6. Velení a řízení

Příkazový kanál pro vzdálenou manipulaci s obětí

7. Opatření k cílům

S rukama na vstupu dosáhne útočník svého cíle

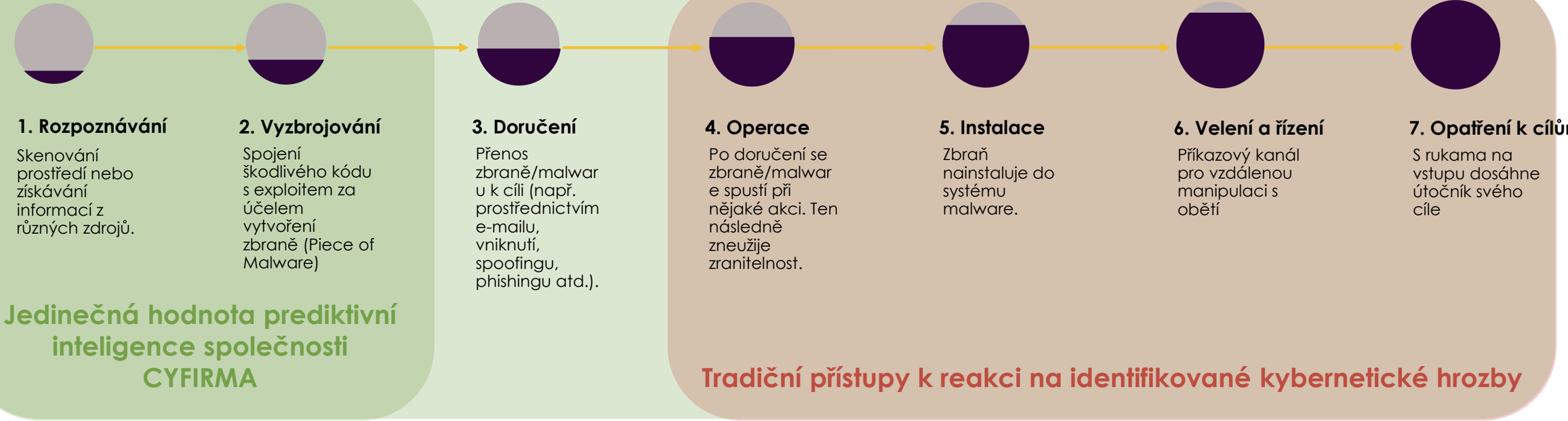
Jedinečná hodnota prediktivní inteligence společnosti CYFIRMA

Tradiční přístupy k reakci na identifikované kybernetické hrozby

PROČ DĚLÁME TO, CO DĚLÁME

IDENTIFIKOVALI JSME MOŽNOSTI, JAK ZABRÁNIT ÚTOKŮM.

Struktura útoku



CYFIRMA - UNIKÁTNÍ MODEL ŘÍZENÍ VNĚJŠÍCH HROZEB

6 POHLEDŮ NA JEDNOTNOU PLATFORMU PRO ŘÍZENÍ KYBERNETICKÝCH HROZEB A RIZIK

1

ZJIŠŤOVÁNÍ míst ÚTOKŮ

Identifikujte "dveře" a "okna" do organizace.

Obchodní výstup: Průběžné monitorování v reálném čase s cílem identifikovat stínové IT nebo děravé systémy, ke kterým mohou získat přístup kyberzločinci. **Povědomí o ploše útoku vám umožní provést realistickou analýzu nákladů a přínosů jednotlivých prostředků a rozhodnout se, jak plochu útoku zmenšit.**

2

ZPRAVODAJSTVÍ KOLEM ZRANITELNOSTI

Klíče ke "dveřím" a "oknům", které mohou kybernetičtí zločinci zneužít.

Obchodní výstup: Zranitelnosti jsou mapovány na aktiva a související zneužití a seřazeny podle kritičnosti. **To umožňuje podniku optimalizovat zdroje a zaměřit se na nejdůležitější a nejnaléhavější nedostatky.**

3

ZPRAVODAJSTVÍ KOLEM ZNAČKY

Poznejte, kdy je vaše značka napadena

Obchodní výstup: Zjistěte, kdo, proč a jak se na vaši značku zaměřuje, a získejte kompletní přehled o porušování značky. **Chraňte značku a udržujte si loajalitu zákazníků tím, že zajistíte, aby ji nepošpinila firemní špionáž, hrozby zevnitř nebo jiní škodliví aktéři.**

4

OCHRANA PŘED DIGITÁLNÍMI RIZIKY

Jasné informace o digitálním profilu, úniku dat, narušení bezpečnosti a vydávání se za někoho jiného.

Obchodní výstup: Odhalte digitální stopy a případy vydávání se za někoho jiného a úniku dat. Získejte téměř v reálném čase upozornění na únik vašich dat ve volné přírodě. **S těmito znalostmi můžete mezeru zacelit a zabránit dalším škodám na pověsti a financích.**

5

POVĚDOMÍ O SITUACI

Získejte kontrolu nad vyvíjejícím se prostředím hrozeb tím, že porozumíte novým hrozbám, jejich zmírňování a potenciálním scénářům útoků.

Obchodní výstup: Rychlý přehled o kybernetických útocích, incidentech a narušeních, ke kterým došlo ve vašem odvětví, technologii, kterou používáte, a zeměpisné oblasti, ve které působíte. **Tyto poznatky a dopady mohou být vodítkem pro důležitá obchodní rozhodnutí, včetně investic do kybernetického prostoru.**

6

KYBERNETICKÁ ROZVĚDKA

Prediktivní, personalizované, vícevrstvé a kontextualizované zpravodajství rozebírá kybernetickou útočnou kampaň a odpovídá na otázky KDO, PROČ, CO, KDY a JAK připravuje kybernetickou útočnou kampaň.

Obchodní výstup: Získejte kompletní přehled a informace o externích hrozbách. **Udržte nepřítele na uzdě, získejte včasné varování a odvraťte kybernetické útoky, abyste se vyhnuli narušení, které by mohlo ohrozit podnikání.**

CYFIRMA
DECODING THREATS

THE CYFIRMA UNIQUE CYBER–INTELLIGENCE MODEL

ZPRAVODAJSKÝ MODEL CYFIRMA JE VODÍTKEM PRO VÝVOJ DECYFIR A DETCT.

ODHALENÍ POVRCHU ÚTOKU
Identifikujte "dveře" a "okna" do organizace.

ZPRAVODAJSTVÍ O ZRANITELNOSTI
Klíče ke "dveřím" a "oknům", které mohou kybernetičtí zločinci zneužít.

ZPRAVODAJSTVÍ KOLEM ZNAČKY
Poznejte, kdy je vaše značka napadena

OCHRANA PŘED DIGITÁLNÍMI RIZIKY
Jasné informace o digitálním profilu, úniku dat, narušení bezpečnosti a vydávání se za někoho jiného

DETCT BY CYFIRMA

Personalizované | Realizovatelné | Komplexní

Průběžné monitorování a monitorování v reálném čase

Poznejte své prostředí útoku

Vystavení na sociálních sítích a na webu

Vydávání se za osobu a protiprávní jednání

Dark Web Exposure

Vulnerabilities Exposure

Monitorování narušení bezpečnosti dat

Monitorování rizik třetích stran

POVĚDOMÍ O SITUACI
Získejte kontrolu nad vyvíjejícím se prostředím hrozeb tím, že porozumíte novým hrozbám, jejich zmírňování a potenciálním scénářům útoků.

KYBERNETICKÁ ROZVĚDKA
- Prediktivní
- Personalizované
- Vícevrstvé
- Kontextové zpravodajství rozebírá kampaň kybernetického útoku - KDO, PROČ, CO, KDY, JAK

DECYFIR BY CYFIRMA

Prediktivní | Personalizované | Pohled hackerů | Vícevrstvé | Kontextualizované

Třívrstvá inteligence

Strategic
Understand Hackers' and their motivation (Who, Why)

Management
Understand Hackers' interest and attack readiness (What, When)

Tactical
Methods, techniques and tools of attack (How)

CYFIRMA
DECODING THREATS

NAVŠTIVNE NÁS NA STÁNKU PRIANTO GMBH

PRIANTO STÁNEK Č. 2 V PRVNÍM PATŘE

PRIANTO

Váš distributor užitečného software

Softwarová Distribuce

Macriumsoftware *Your image is everything*

ONE IDENTITY™

control UP

sugarcrm

UNITRENDS A Kaseya COMPANY

TeamViewer

FLEXERA

nitro Quest™

CYFIRMA DECODING THREATS

ENDPOINT PROTECTOR by CoSoSys

SMARTBEAR

solarwinds

Runecast

deepnet SECURITY