BEHAVIORÁLNÍ ANALÝZA S VYUŽITÍM STROJOVÉHO UČENÍ

ARUBA INTROSPECT: USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)

Ondřej Krabec | security consultant

CONSULTING

SIEM NEBO UEBA ?

- **SIEM - Security Information and Event Management**
  - SIEM řešení je auditní a monitorovací nástroj pro zajištění a garanci úrovně bezpečnosti provozovaného segmentu IT.
  - Zaměřeno na obecné vyhodnocování událostí ze zařízení, přístupu k datům, aktivitě aplikací, apod. a na **uchování auditní stopy**.
  - **Vyhodnocování založené především na agregačních a korelačních pravidlech**.

- **UEBA - User and Entity Behavior Analytics**
  - Zaměřeno na vyhodnocování chování entit (uživatelů / zařízení)
  - Párování aktivit s konkrétní entitou
  - **Vyhodnocování založené na strojovém učení a hledání anomálií v typickém chování**

PŘÍKLAD: BEZPEČNOST NA LETIŠTI

Pravidla

Jednoduché statické kontroly

→ **Rule based**

Učení se z dat

Dynamické kontroly založené na kontinuelním monitorování a určování podezřelých aktivit cestujících (entit)

→ **Anomaly based**

CONSULTING

JAK SI V TĚCHTO PŘÍPADECH STOJÍ STANDARDNÍ BEZPEČNOSTNÍ IT NÁSTROJE?

Firewall

IDS a IPS

Web/Mail brány

SIEM a log management

UEBA principy
a
Strojové učení

ÚTOKY VYUŽÍVAJÍCÍ PLATNÉ INTERNÍ PŘÍSTUPOVÉ ÚDAJE

KOMPROMITACE

40 millionů kreditních karet ukradeno ze serverů firmy Target

UKRADENÉ PŘÍSTUPY

ZLÉ ÚMYSLY

Edward Snowden ukradl více než 1.7 milionu klasifikovaných dokumentů

ÚNIK INFORMACÍ JAKO CÍL

NEZODPOVĚDNOST

DDoS útok z 10M+ haknutých domácích zařízení odstavilo hlavní weby

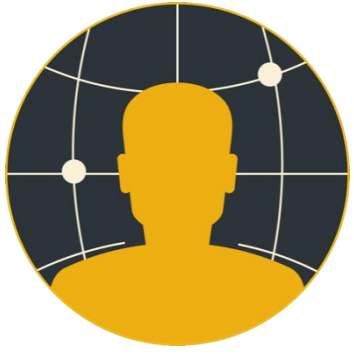
VŠICHNI POUŽÍVALI STEJNÉ HESLO

NÁSTROJE UEBA ŘEŠÍ DVĚ HLAVNÍ OBLASTI

ÚTOKY A NEBEZPEČNÉ CHOVÁNÍ

uvnitř sítě

Jeden z hlavních cílů protivníků je získat přístup k platným interním přístupovým údajům. Útok tak získá klíčové nástroje.



EFEKTIVITA

bezpečnostních týmů

80% těchto úniků je detekováno za měsíce či roky místo týdnů či ještě kratších období

➡ Detekce založená na **strojovém učení (ML)**

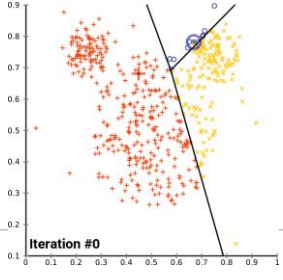
OBECNĚ: TECHNIKY STROJOVÉHO UČENÍ

Supervizované strojové učení

Nesupervizované strojové učení
(Neověřené)

Např. Bayesův klasifikátor (učící se a založený na pravděpodobnosti)

Např. algoritmus pro shlukovou analýzu K-means



PŘÍKLAD HROZBY DETEKOVATELNÉ POMOCÍ STROJOVÉHO UČENÍ

Detekce DNS exfiltrace

Útočník vezme soubor, naseká ho na malé kousky, každý z nich zakóduje a tento řetězec použije jako subdoménové pole v DNS dotazu. Jakmile se všechny kousky dostanou k DNS serveru data jsou ukradena!

DNS exfiltraci nelze detekovat běžnými statickými pravidly na firewallu či SIEM.

STROJOVÉ UČENÍ - DETEKCE ANOMÁLIÍ

- To co není chyceno přímou shodou s cílenými modely je odhalováno skrze detekci anomálií
- Využíváme dvojí ”baselining” – historický a skupinový

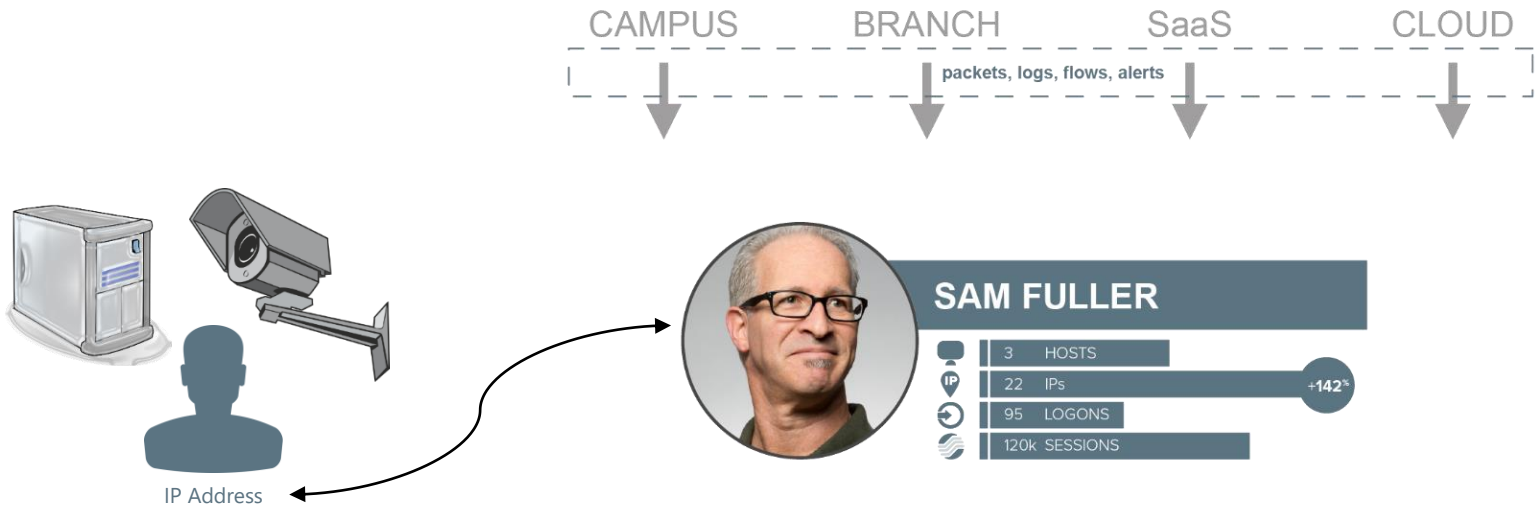
CONSULTING

UEBA

Aruba Introspect

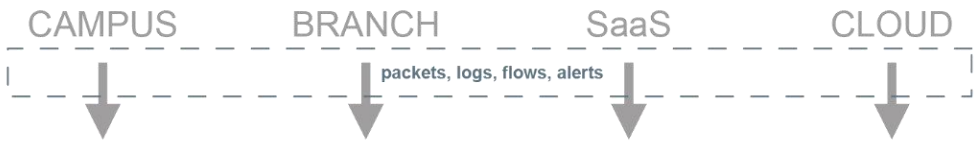
aruba
a Hewlett Packard
Enterprise company

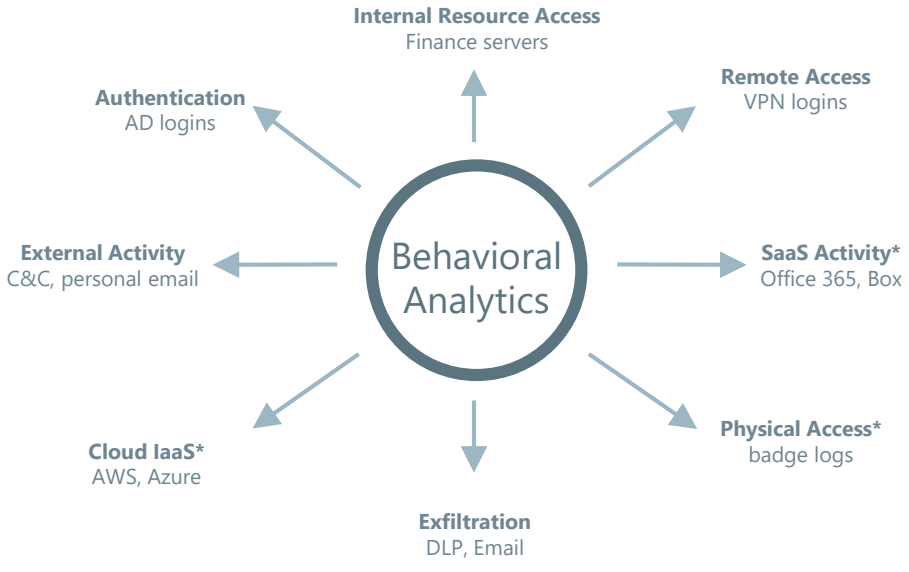
ZÁKLAD: PÁROVANÍ ÚDÁLOSTÍ A PŘENOSŮ NA UŽIVATELE/ENTITU

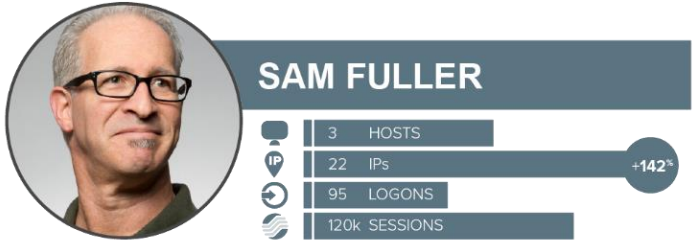


Entity jsou přebírány z AD/LDAP, vč. dalších atributů (skupina/oddělení, atd.)

ANALÝZA CHOVÁNÍ NAPŘÍČ MNOHA DIMENZEMI

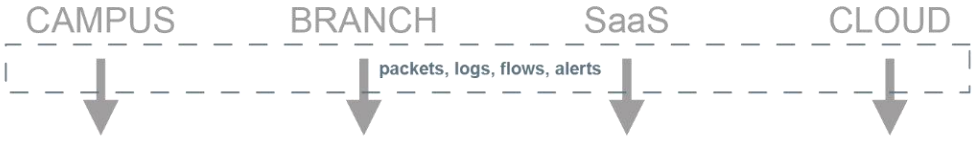






Vytváření tzv. Behavioral Baselines pro každou entitu

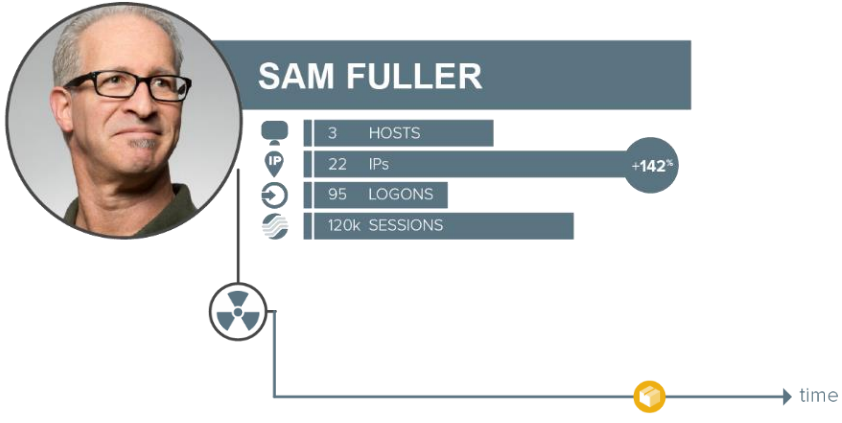
ZÁKLADNÍ ANALÝZA CHOVÁNÍ



Strojové učení
NESUPERVIZOVANÉ
(auto-učící se)

ANALÝZA CHOVÁNÍ

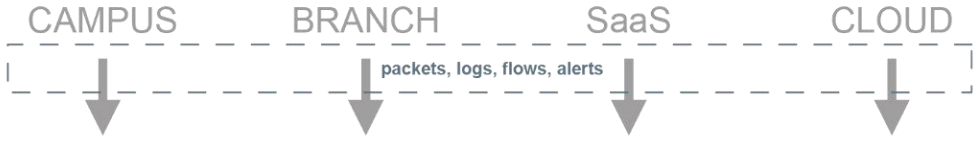
BASELINES
HISTORIE
+
SROVNÁNÍ SE SKUPINOU



Využíváme dvojí "baselining" – historický a skupinový

ABNORMÁLNÍ PŘÍSTUP K INTERNÍM DATŮM

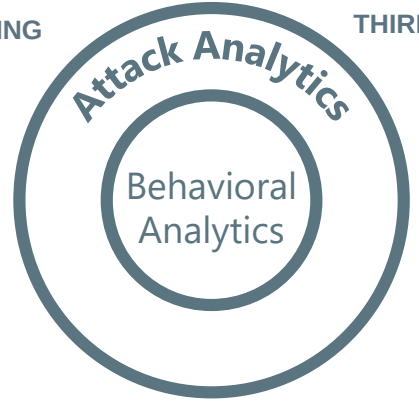
HLEDÁNÍ ŠKODLIVÉHO MEZI ANOMÁLIEMI



BUSINESS CONTEXT
High Value Assets
High Value Actors

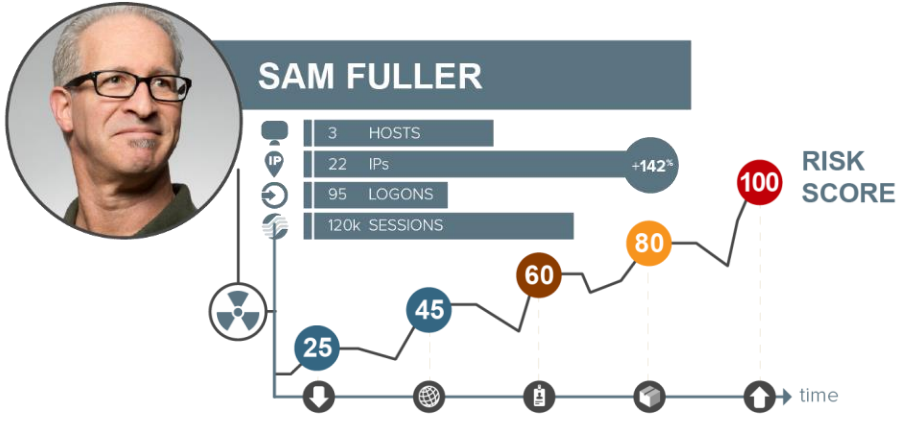
MACHINE LEARNING

SUPERVISED
UNSUPERVISED



THIRD PARTY ALERTS

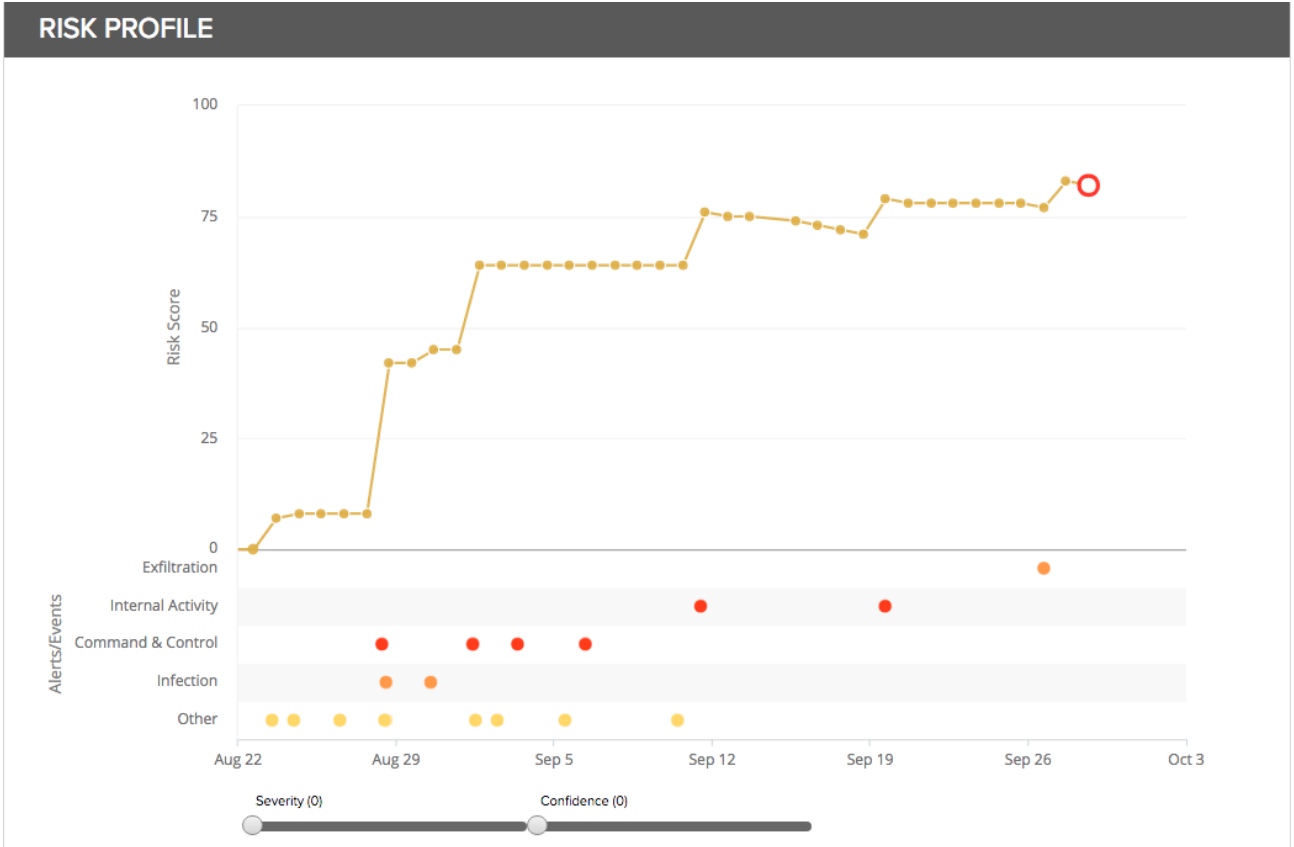
DLP
Sandbox
Firewalls
STIX
Rules
Etc.



Posloupnosti detekovaných anomálií jsou dále vyhodnocovány pomocí ML a hledá se tzv. kill chain.

Řetězení anomálií → vyšší pravděpodobnost vnitřního útoku a vyšší risk score entity

UŽIVATELSKÝ RISK SCORING



- Skrytý Markovův Model (HMM) sleduje dočasný pohyb přes různé scénáře útoků (kill-chains)

CONSULTING

UŽIVATELSKÝ RISK SCORING

Type	Name	Risk Score	Risk Percentile	Change
	mjohnson-pc.niara.com	78	100%	▲ 78
	10.22.3.101	68	100%	▲ 68
	mjohnson	100	100%	▲ 100
	sshetty-pc.niara.com	66	97%	▲ 66
	10.22.3.106	55	95%	▲ 55
	karthik-pc.niara.com	61	95%	▲ 61
	uhenry-mbp.niara.com	53	93%	▲ 53
	jordanrachel-mbp.niara.com	53	93%	▲ 53
	robert58-mbp.niara.com	53	93%	▲ 53

UŽIVATELSKÝ RISK SCORING

100
RISK SCORE
100
CHANGE

mjohnson

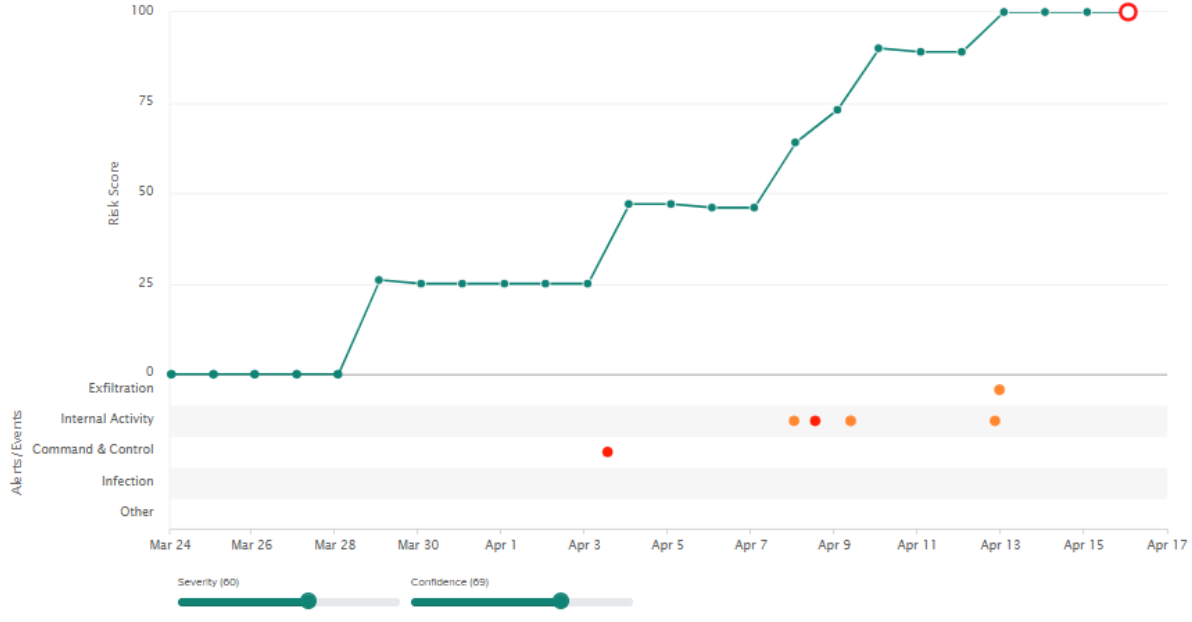
FULL NAME: **Michelle Johnson**
TITLE: **Finance Manager**
EMAIL: **mjohnson@niara.com**

ASSOCIATIONS

DEPARTMENT: **Finance**
MANAGER: **Hari Seldon**
GROUPS:
Domain Users

WATCHLISTS
Executive Team Domain Admins Users under Investigation

RISK PROFILE



ALERTS IN TIME RANGE

Apr 12	11:32 pm	Suspicious Data Exfiltration	SEVERITY 60 CONFIDENCE 100
Apr 12	11:32 pm	Large Data Upload to External	SEVERITY 60 CONFIDENCE 100
Apr 12	9:13 pm	Large Internal SMB Download	SEVERITY 60 CONFIDENCE 100
Apr 09	9:58 am	Excessive Hosts Failed Logons by User	SEVERITY 70 CONFIDENCE 99
Apr 09	9:58 am	Excessive Failed Logons	SEVERITY 60 CONFIDENCE 99
Apr 08	1:05 pm	Global Admin Escalation	SEVERITY 70 CONFIDENCE 80
Apr 03	1:38 pm	DNS DGA	SEVERITY 80 CONFIDENCE 81

KONKRÉTNÍ PŘÍKLAD: EXFILTRACE DAT

Indikátory

Přístup k interním kritickým datům

Přesun dat na externí zdroje

UEBA vyhodnocení:

- Abnormální přístup k interním datům

- Abnormální USB zápis dat(*)
- Abnormální upload na Dropbox, FTP či cokoliv relevantního

Vysoké risk skóre pro uživatele XY

KONKRÉTNÍ PŘÍKLAD: RYCHLOST

Nov 26, 2017
8:16:00 PM

LAND SPEED VIOLATION
ALERT-42 | HISTORY BASELINE

60
SEVERITY

100
CONFIDENCE

User **bsmith** remotely logged on using **188.166.236.164** from **Singapore, Singapore** on **Nov 26, 2017** within **1min 0s** of logon using **138.197.137.156** from **Toronto, Canada** at speed of **560145 MPH**

OPEN	UNCLASSIFIED	UNASSIGNED	INTERNAL ACTI...	N/A	MORE CARDS
STATUS	LABEL	ASSIGNEE	ATTACK STAGE	BASELINE	DEEP DIVE

CONSULTING

PRAVIDLA, STROJOVÉ UČENÍ– A CO DÁL?

	Obecné, nesnadno kvantifikovatelné	Snadno aplikovatelné organizační pravidla	Nízký výskyt false positives
Statická pravidla *Uživatel se připojil v už 5:00 a odpojil až v 22:00.*	✗	✓	✗
Strojové učení *Uživatel přistupuje k neobvykle velkému počtu kritických aplikací, ve srovnání s jeho historií za posledních 30 dní.*	✓	✗	✗
Pravidla + Strojové učení *Uživatel nahrál nezvykle vysoký počet souborů na Dropbox a zároveň je v AD ve skupině propuštěných pracovníků.*	✓	✓	✗
Postupné sledování (řetězení detekcí) *Uživatel ze seznamu propuštěných pracovníků provedl nezvykle vysoký počet nahrání na Dropbox a zároveň v následujících 8 hodinách provedl neobvykle vysoký počet tisků na tiskárně.* ***→ Zvýšení skóre pro danou entitu (uživatele)***	✓	✓	✓

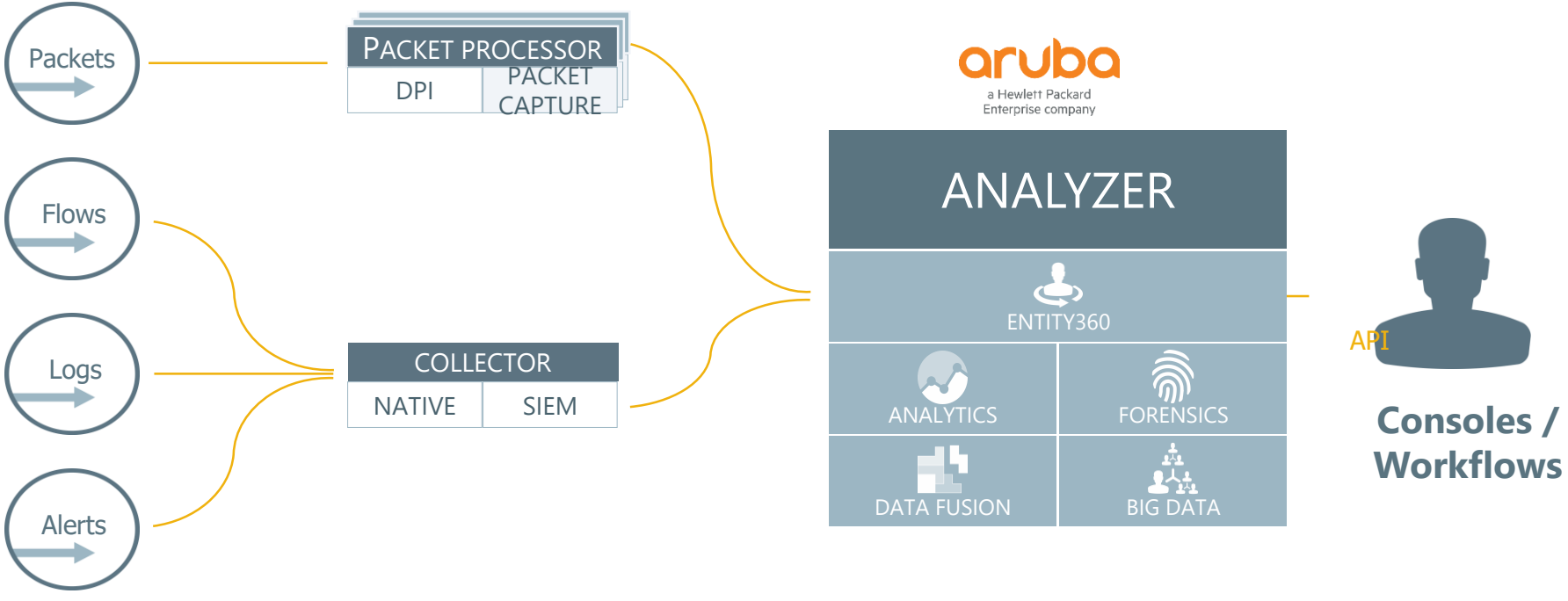
CONSULTING

Nasazení a integrace

Aruba Introspect

aruba
a Hewlett Packard
Enterprise company

KOMPONENTY ŘEŠENÍ



DĚKUJI ZA POZORNOST

Ondřej Krabec | security consultant

M: +420 728 157 388
@: ondrej.krabec@xconsulting.cz