Forcepoint

Jak chránit data před krádeží a zneužitím?

Filip Bednář
Business Development Manager
CLICO Česká republika & Slovensko

CLICO

Forcepoint

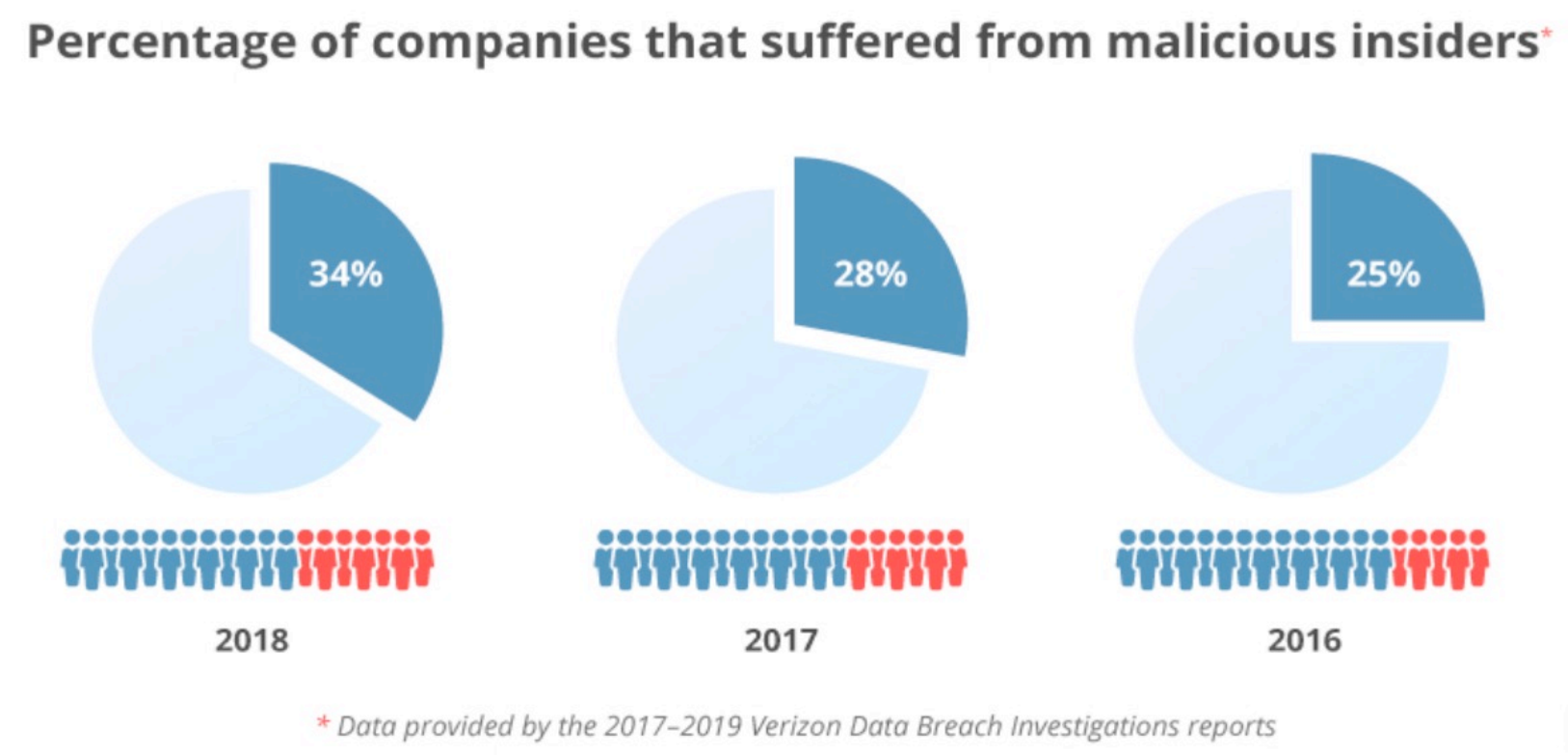
O společnosti Forcepoint

- Integrace firem Raytheon, Websense, Stonesoft Corporation a RedOwl Analytics
- Forrester´s leader v oblasti zabezpečení uživatelů a dat!
- Přes 10 tisíc zákazníků po celém světě
- Necelých 3 tisíce zaměstnanců
- Zastoupení v ČR, distribuce, partnerská síť

CLICO

Forcepoint

Trochu statistiky

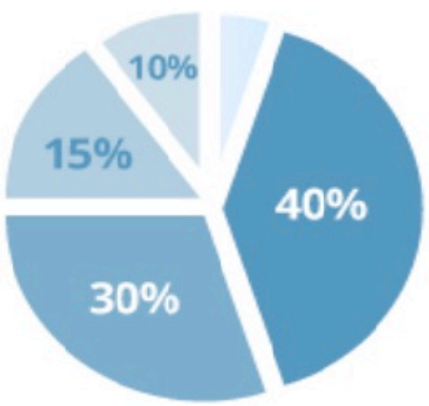


CLICO

Forcepoint

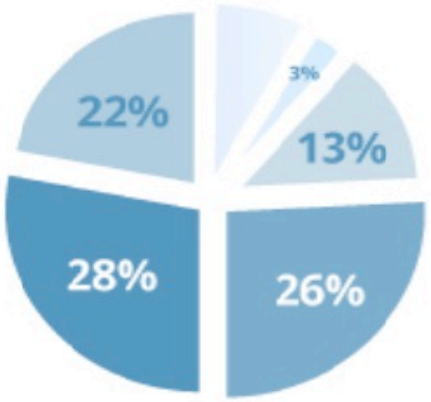
Trochu statistiky

Insider-related data breach detection time



40% - years
30% - months
15% - weeks
10% - days

* *Data provided by Verizon 2019 Insider Threat Report: Executive Summary*



28% - hours
26% - one day
22% - minutes
13% - one week
3% - one month

* *Data provided by Crowd Research Partners 2018 Insider Threat Report*

CLICO

Forcepoint

Je třeba začít klasifikací dat – **Jak na to?**

- Scan statických dat i dat v pohybu
- Regulární výrazy, klíčová slova, slovníky
- Machine learning tool
- Třetí strany, tj. Boldon James, Microsoft AIP a další

CLICO

Forcepoint DLP – 4 hlavní moduly

FORCEPOINT DLP – ENDPOINT

- Ochrání data a uživatele na koncových stanicích, statická data, data v pohybu
- Windows, MacOS, Linux
- Web Security, E-mail Security

FORCEPOINT DLP – NETWOK

- Ochrání data v pohybu, integrace s vaší e-mail a web proxy gateway

FORCEPOINT DLP – CLOUD APPS

- Ochrání data v cloudu, O365, Dropbox, Google apps, Salesforce a další

FORCEPOINT DLP – DISCOVER

- Ochrání statická data, strukturovaná data v databázích

Forcepoint

Některé principy, které používáme pro ochranu vašich dat

FINGERPRINTING

- Umožní vytvořit unikátní segmenty celého dokumentu nebo jeho části
- Ta konkrétní data následně ochrání

OCR

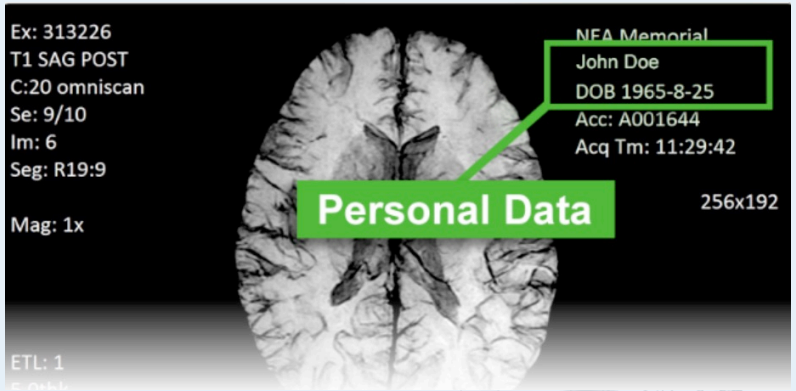
- Nalezne citlivá data v obrázcích, PDF souborech atp.

MACHINE LEARNING

- Naučí se kontext, dobré a špatné příklady a následně si je nacvičí

INCIDENT RISK RANKING

- řadí DLP incidentům skóre, vyzdvihne to nejpodstatnější!

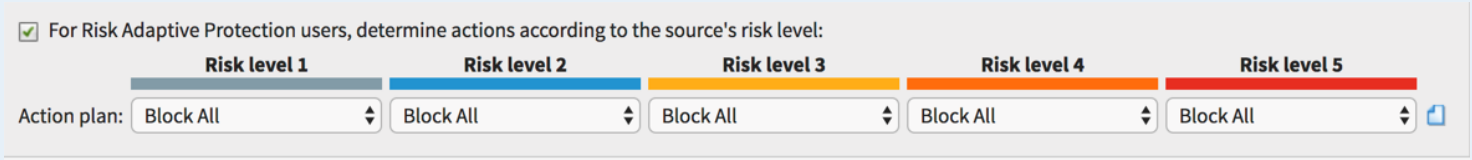


CLICO

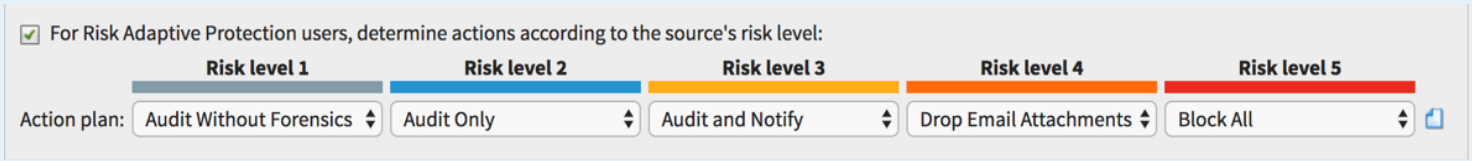
Politiky se vynutí na základě risk profilu uživatele

Pro kritické informace a účely naplnění shody s předpisy (compliance) může být varianta „Block All“

tím správným řešením



U incidentů, kterým je potřeba dodat širší kontext je možné risk levels odstupňovat

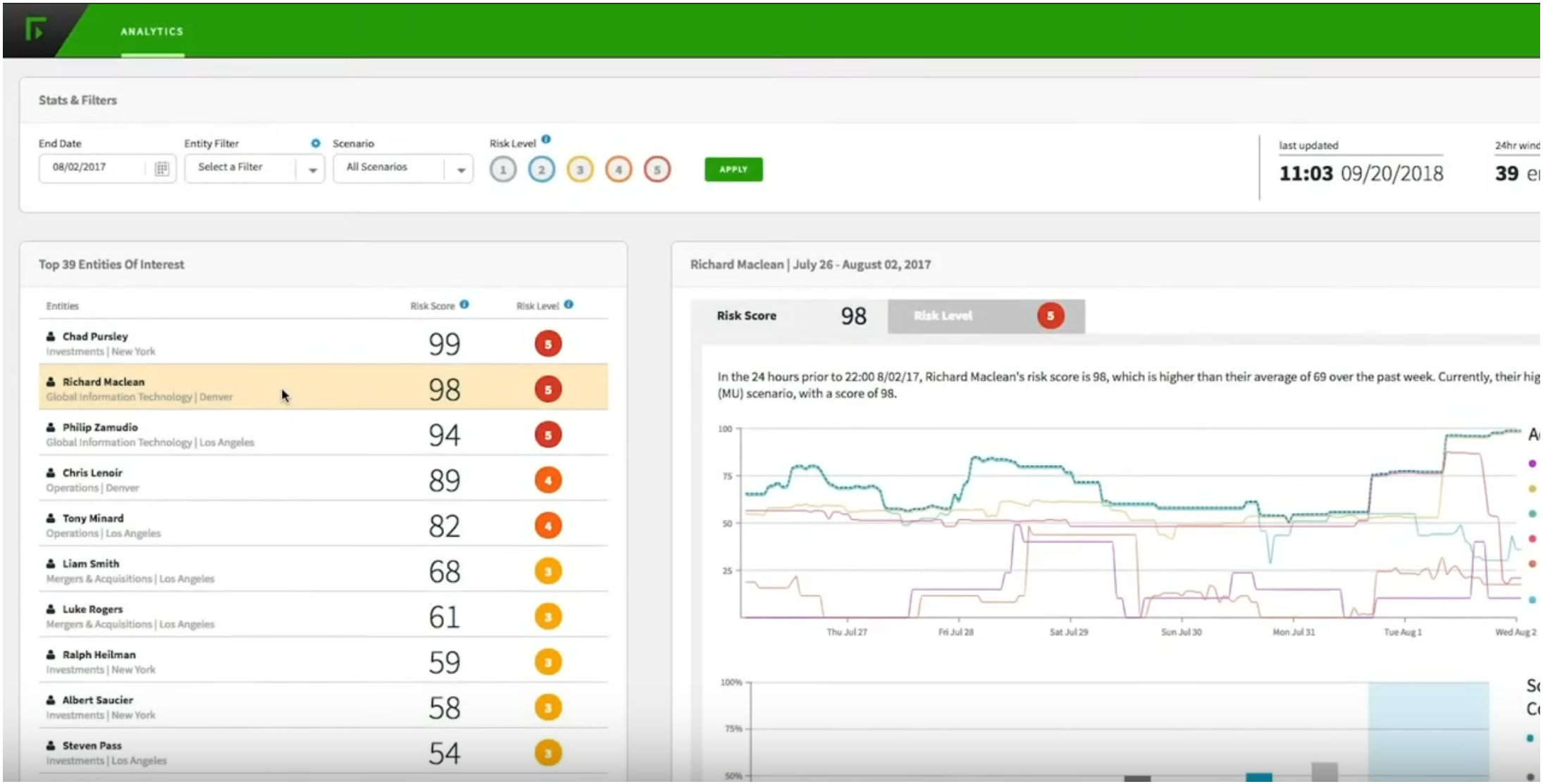


Forcepoint

Tradiční přístup vs. UEBA

CLICO

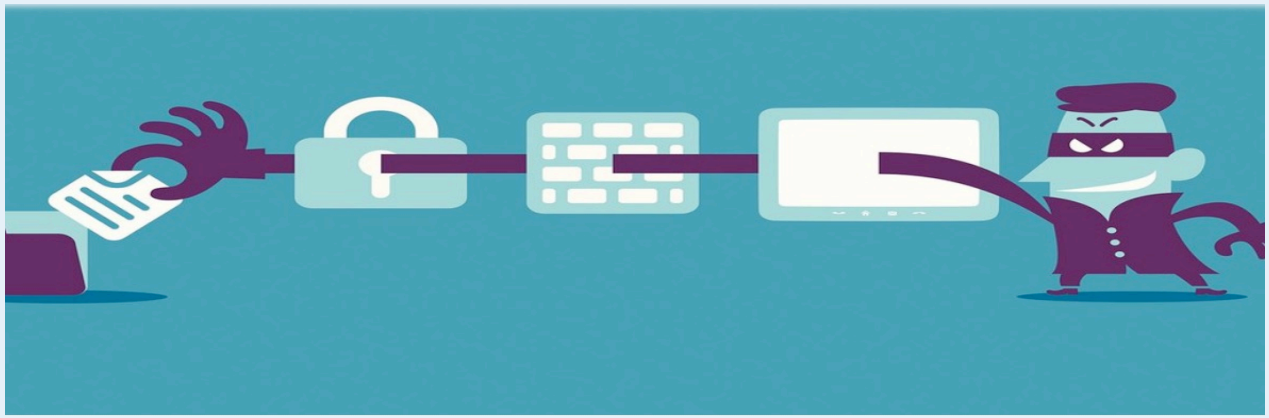
Forcepoint


ANALYTICS
Stats & Filters
End Date
08/02/2017
Entity Filter
Select a Filter
Scenario
All Scenarios
Risk Level
1 2 3 4 5
APPLY
last updated
11:03 09/20/2018
Top 39 Entities Of Interest
Entities
Risk Score
Risk Level
Chad Pursley
Investments | New York
99
5
Richard Maclean
Global Information Technology | Denver
98
5
Philip Zamudio
Global Information Technology | Los Angeles
94
5
Chris Lenoir
Operations | Denver
89
4
Tony Minard
Operations | Los Angeles
82
4
Liam Smith
Mergers & Acquisitions | Los Angeles
68
3
Luke Rogers
Mergers & Acquisitions | Los Angeles
61
3
Ralph Heilman
Investments | New York
59
3
Albert Saucier
Investments | New York
58
3
Steven Pass
Investments | Los Angeles
54
3
Richard Maclean | July 26 - August 02, 2017
Risk Score
98
Risk Level
5
In the 24 hours prior to 22:00 8/02/17, Richard Maclean's risk score is 98, which is higher than their average of 69 over the past week. Currently, their hig
(MU) scenario, with a score of 98.
100
75
50
25
Thu Jul 27
Fri Jul 28
Sat Jul 29
Sun Jul 30
Mon Jul 31
Tue Aug 1
Wed Aug 2
100%
75%
50%

Forcepoint

Příklad – **RICHARD / IT ADMIN**

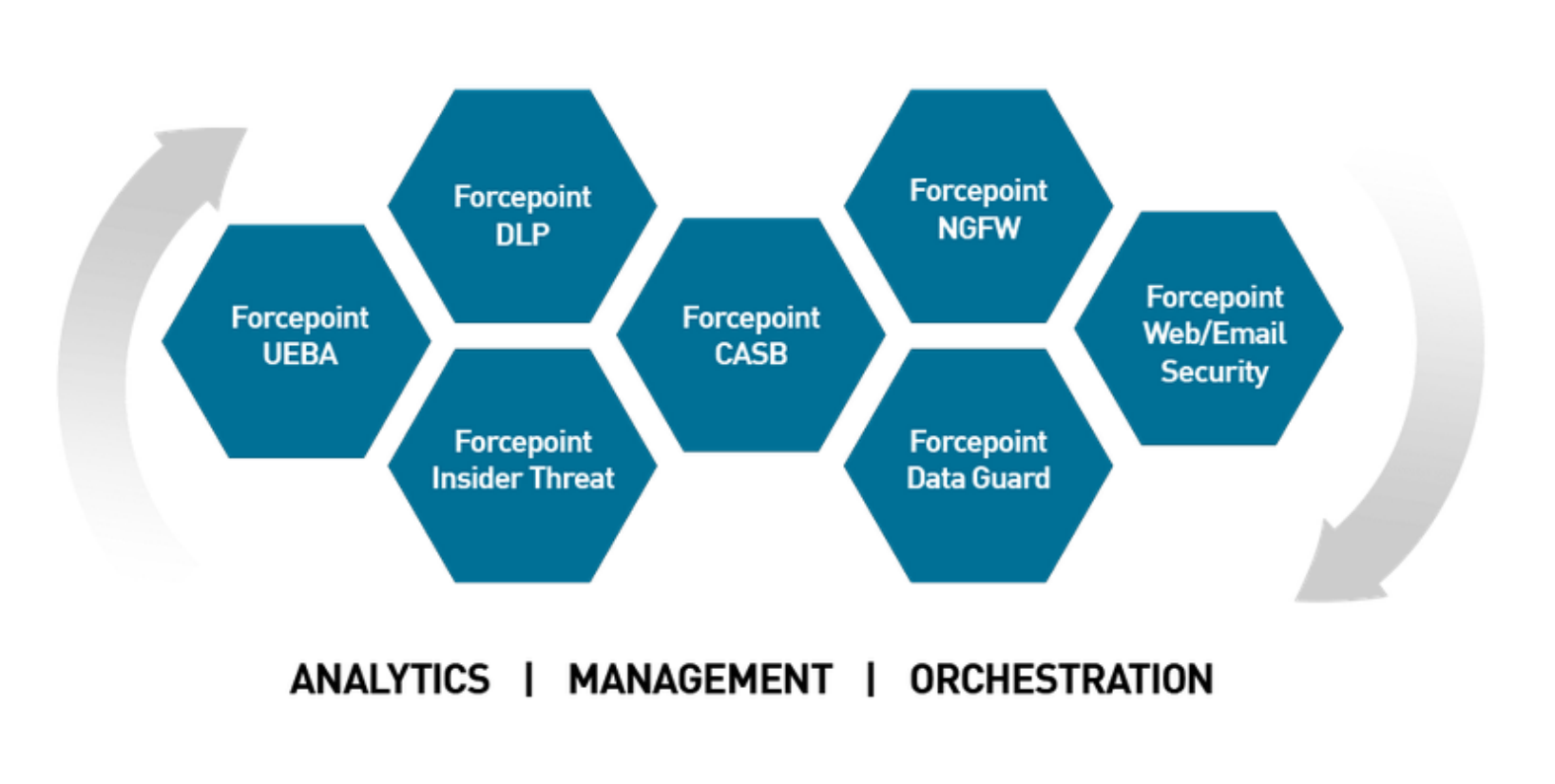
- Risk skóre se zvýšilo poté, co Richard provedl sérii úkonů mimo jeho běžné chování
- Dashboard mě upozorní na náhlou změnu a umožní mi zareagovat
- Kompletní přehled činností, které vedly ke zvýšení risk skóre
- UEBA dodá informace DLP modulu a ten zareaguje podle nastavené politiky



CLICO

Forcepoint

Forcepoint ECOSYSTEM



CLICO

Forcepoint

DĚKUJI ZA VAŠI POZORNOST

CLICO s.r.o.

Antala Staška 2027/77

Budějovická alej, Blok B

140 00 Praha 4

www.clico.cz

www.clico.sk

CLICO