



FORCEPOINT

Přínos analýzy chování uživatelů v
kyberprostoru pro ochranu citlivých
dat.

Vladimír Špička
FORCEPOINT

BEZPEČNOSTNÍ TECHNOLOGIE

Technologie a výsledky v oblasti kybernetické bezpečnosti.

\$81mld

- vydáno na bezpečnost v roce 2016
- četnost bezpečnostních incidentů narostla

< 50%

organizací souhlasí, že technologie zvýší bezpečnost

Chování uživatelů v kybernetickém prostoru.

80%

organizací se domnívá, že při porozumění chování uživatelů dosáhne lepších výsledků

<1/3

organizací se domnívá, že dostatečně rozumí chování uživatelů v kyber. prostoru

LIDÉ JSOU SOUČÁSTÍ INCIDENTŮ

TECHNOLOGIE SE MĚNÍ

LIDÉ JSOU SOUČÁSTÍ INCIDENTŮ



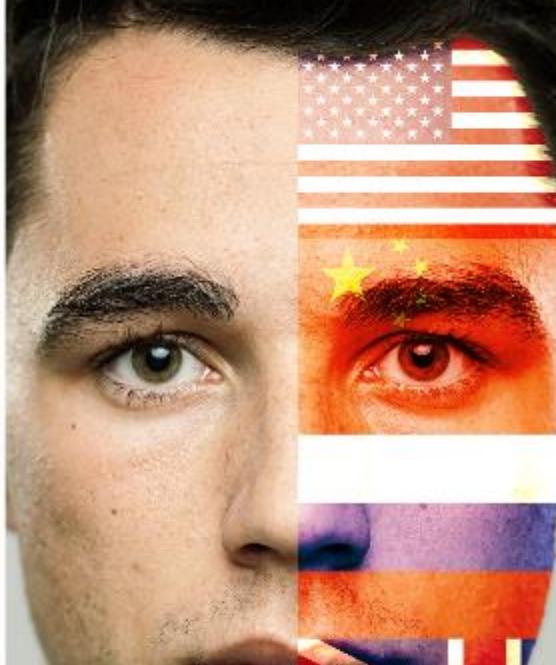
Neúmyslné chování

Špatně komunikovaná pravidla a nízké povědomí uživatelů



Nesprávné procesy

Data tam, kde by neměla být, ne kde by měla být



Škodlivý kód

Phishingové útoky, pokročilé hrozby, zabezpečení BYOD

Zneužití identity

Odcizení přihlašovacích údajů, sociální inženýrství



Nespokojený zaměstnanec

Odcházející zaměstnanec



Kriminální činnost

Firemní špináž, národní špináž, organizovaný zločin

PROTECTING THE HUMAN POINT

Where critical data and IP are most valuable –
and most vulnerable

PROTECTING THE HUMAN POINT

Zvyšme kybernetickou bezpečnost tím, že použijeme systémy, které analyzují a interpretují chování uživatelů při práci s citlivými daty a duševním vlastnictvím.

VYJÁDŘENÍ ZÁKAZNÍKŮ

Jako CISO potřebuji vědět, které osoby v mé organizaci se chovají způsobem, který představuje největší bezpečnostní riziko a proč. Pak mohu riziku porozumět a správně na ně reagovat.

Jako CISO, který identifikoval konkrétního uživatele v mé organizaci jako zdroj potenciálního rizika, potřebuji rychle a důkladně pochopit potenciálně rizikové chování uživatele a kontext, abych mohl podniknout rychlé a účinné kroky ke zmírnění potenciálního rizika.

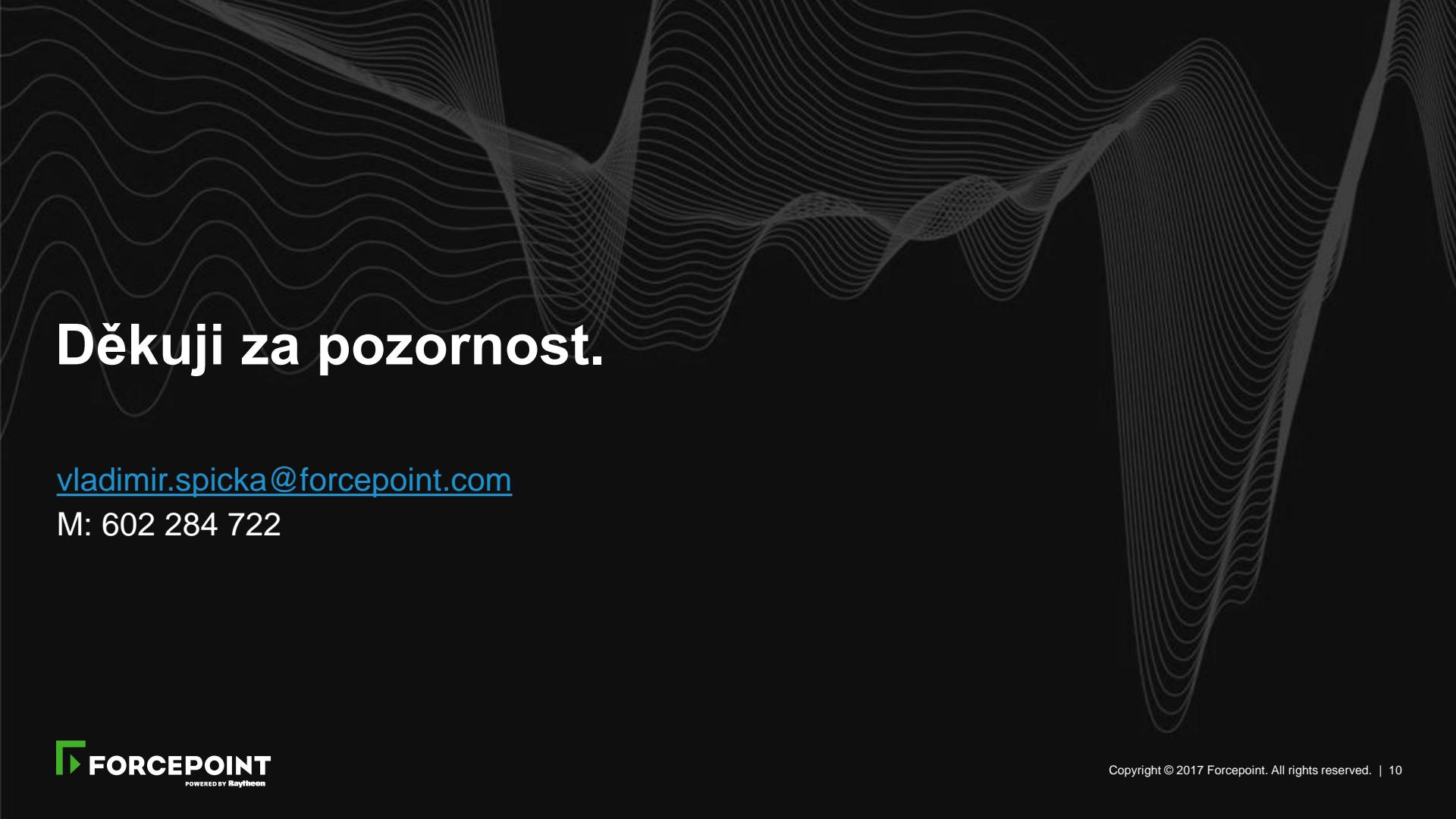
RIZIKOVÉ CHOVÁNÍ UŽIVATELŮ A MOŽNÝ ÚNIK DAT FORCEPOINT INSIDER THREAT A DLP

The image shows two screenshots of security management software. The left screenshot is for 'SureView® INSIDER THREAT' and includes sections for 'COMMAND CENTER', 'ORGANIZATIONAL RISK SCORE TREND', 'TOP RISK SCORES', and 'HIGH RISK EMPLOYEES'. The right screenshot is for 'FORCEPOINT TRITON® APX' and shows a 'Main' menu with options like 'Status', 'Reporting', 'Policy Management', 'Logs', 'Settings', and 'Deployment'. A modal window titled 'Incident Risk Ranking - Top Cases' is open, listing several incidents of suspected data theft. Each incident entry includes a timestamp, score, case ID, and a detailed description of the violation.

Case ID	Date	Score	Description
ID: 197126	08 Oct, 2016, 11:31 AM	8.1	Suspected data theft James Brown, Principle Engineer sent password content to a personal acquaintance, gu@gmail.com.
ID: 196526	08 Oct, 2016, 09:31 AM	7.6	Suspected data theft Linda Jackson, Showing 1 sources of 1 James Brown, Principle Engineer Department: R&D jbrown@mycompany.com +001 (312) 345-0711
ID: 197141	08 Oct, 2016, 09:00 AM	7.0	Suspected data theft Barbara White, Sales Manager Copied credit card content (500 matches) to a removable media.
ID: 197132	08 Oct, 2016, 00:21 AM	6.5	Suspected data theft Mark Smith, Security Administrator Sent credit card content (100 matches) to 3 common destinations.
ID: 197135	08 Oct, 2016, 12:31 PM	6.2	Suspected data theft PublicServer 10.0.12.34 Sent 4 shadow files to a personal acquaintance, sam@gmail.com.
ID: 197164	08 Oct, 2016, 07:20 AM	6.2	Suspected data theft Dave Black, Sr. Marketing Manager Uploaded credit card and financial content (2 matches) to labose.eu
ID: 197116	08 Oct, 2016, 11:00 AM	4.1	Suspected personal communication Bob Davidson, Developer Sent content of various violated policies to 2 email addresses.
ID: 197144	08 Oct, 2016, 06:20 AM	4.0	Suspected personal communication SharedServer 11.2.32.12 Sent credit card and financial content (2 matches) to 2 email addresses.
ID: 197187	08 Oct, 2016, 11:25 AM	2.8	Broken business process Dana Brown, Principle Engineer Uploaded credit card content (4 matches) to internal.org.com.

PROTECTING THE HUMAN POINT

Analýza aktivity uživatele umožní včasné varování a tedy prevenci úniku nebo ztráty dat, způsobené napadenými systémy nebo nesprávným chováním uživatelů.



Děkuji za pozornost.

vladimir.spicka@forcepoint.com

M: 602 284 722