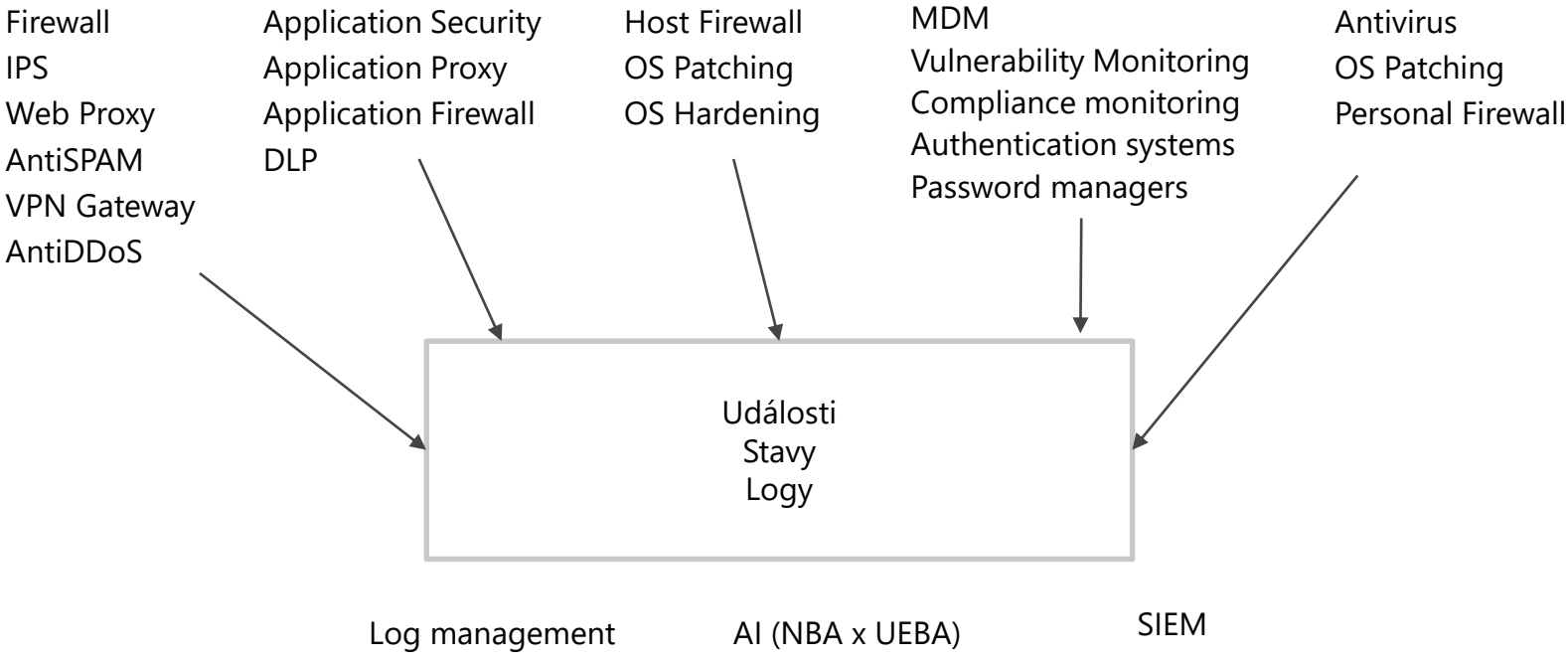
ÚVOD DO AUTOMATIZACE BEZPEČNOSTI

DALIBOR SOMMER, CISA
17. DUBNA 2019

CONSULTING

TECHNICKÁ OPATŘENÍ

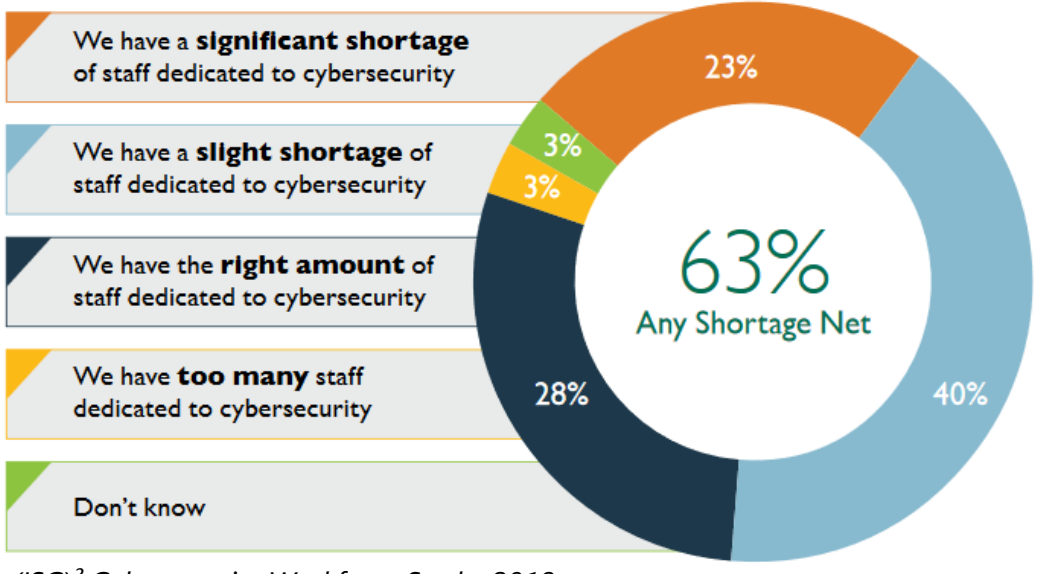


Bezpečnostní akce téměř vždy závisí na lidském faktoru!

ZÁSADNÍ PROBLÉM?

The tech talent gap persists, with 80% of security professionals having trouble finding talent.
Dimensional Research, 2019

Almost all (96%) respondents have trouble keeping security teams staffed because of the everchanging tech landscape.
Dimensional Research, 2019



(ISC)² Cybersecurity Workforce Study, 2018

Lack of Skilled Information Security Professionals Is the Biggest Challenge for Cyber Security
dynamicsCISO.com

CO S TÍM?

INTEGRACE

CONSULTING

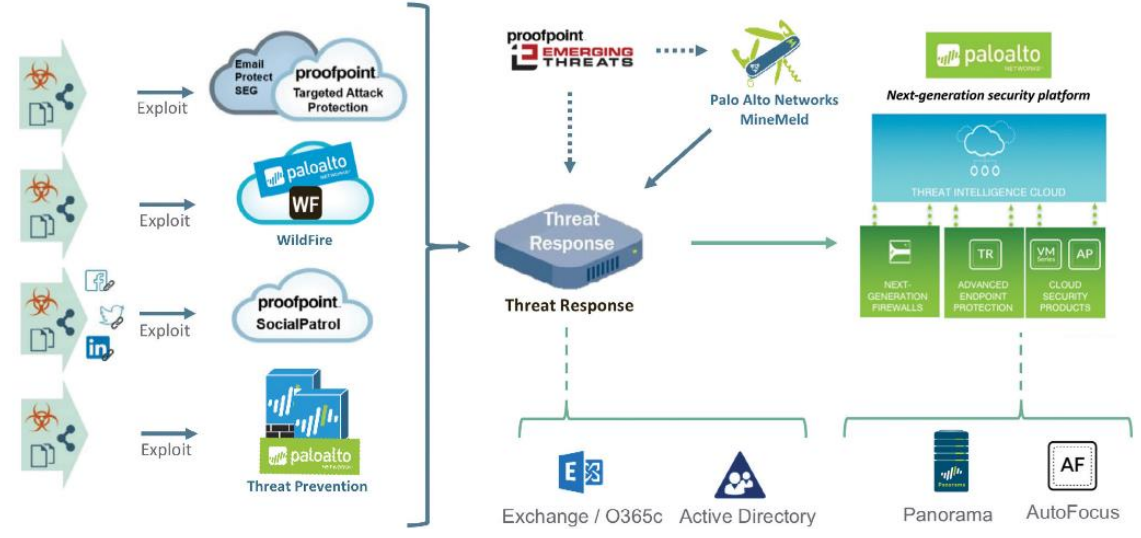
Ochrana síťového perimetru

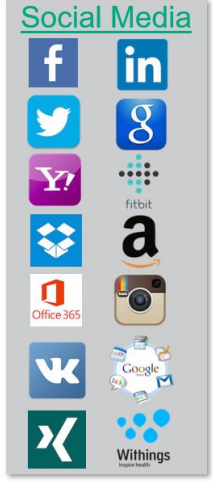
- Firewall + IPS + Application Control
- LAN + WiFi + VPN Access
- User Profiling and Authentication
- Endpoint Security
- UEBA
- …

Ochrana aplikací

- Application Delivery Controller
- SSL decryption
- Application Firewall
- IPS
- AntiDDoS
- Vulnerability monitoring
- …

API





AUTOMATIZACE A ORCHESTRACE

Automatizace

Provedení (původně lidského) úkonu počítačem

- Instalace OS z image
- Evidence serveru v CMDB
- Založení deníku změn
- Přidělení IP adresy z IPAM
- Přidělení jména a aktualizace DNS
- Vytvoření admin účtu a uložení hesla v trezoru hesel
- Zavedení serveru do Compliance management nástroje
- Hardening OS
- Zavedení serveru do Vulnerability monitoring nástroje
- …

Orchestrace

Provádění jednoho či více automatizovaných úkonů přes více prvků nebo platforem

- Instalace více serverů
- Založení více uživatelů
- …

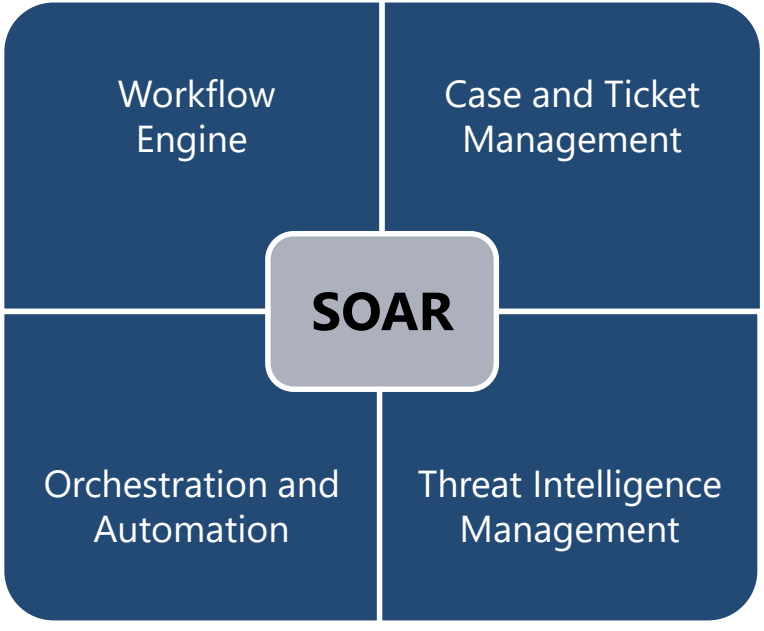
- Založení uživatele do více systémů
- Provedení kontroly Compliance na všech síťových prvcích
- Změna nastavení přístupových pravidel na více serverech
- …

CONSULTING

SOC AUTOMATIZACE - SOAR

- Automatizace opakujících se úkonů pro vyhodnocování/posuzování a odstraňování nálezů/nápravy
- Implementace workflow pro vyhodnocování a zavírání incidentů
- Integrace interních a externích zdrojů threat intelligence
- Zavedení systému pro pravidelné monitorování a vyhodnocování administrátorských/uživatelských aktivit

Security Orchestration, Automation and Response (SOAR)



Gartner: Prepare Your Security Operations for Orchestration and Automation Tools, 2018

CONSULTING

DOPORUČENÍ NA ZÁVĚR

- Řešit problematiku bezpečnostních specialistů
- Optimalizovat pracovní postupy a nástroje
- Vzájemně integrovat vhodná řešení
- Automatizovat a orchestrovat ☺

DĚKUJI ZA POZORNOST

CONSULTING

dalibor.sommer@xconsulting.cz