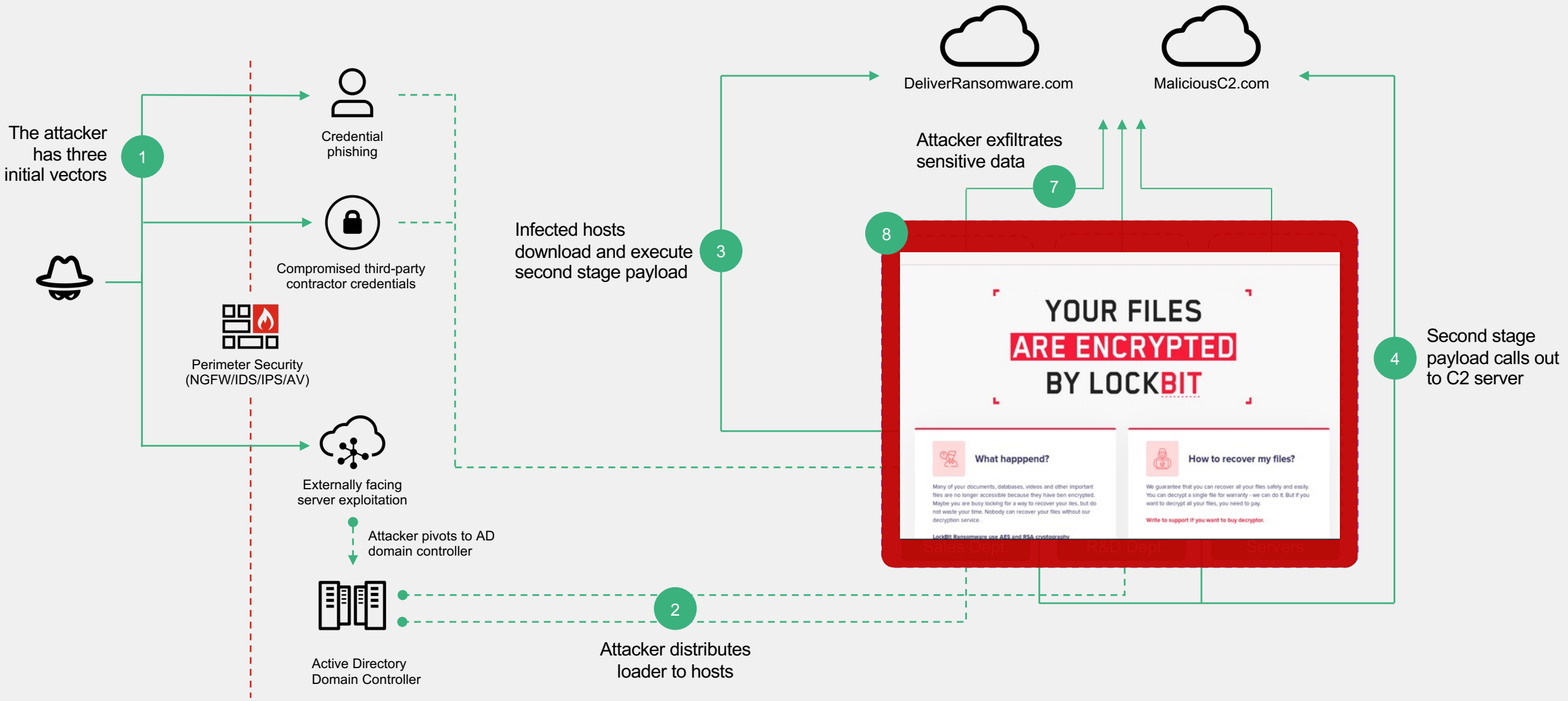
Začíname cestu k integrovanej kybernetickej bezpečnosti

Systems Engineer /
Juraj Belko

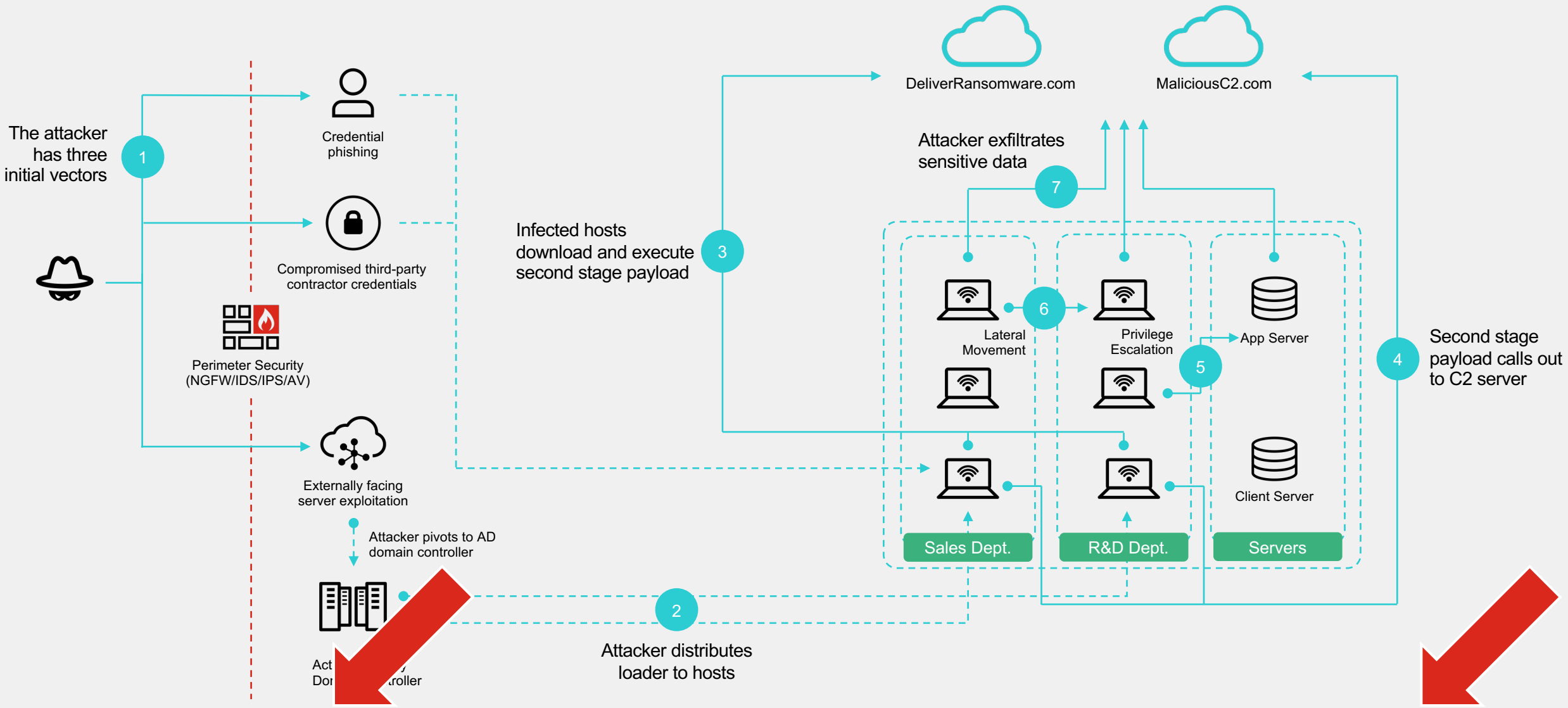
Juraj Belko

Systems Engineer

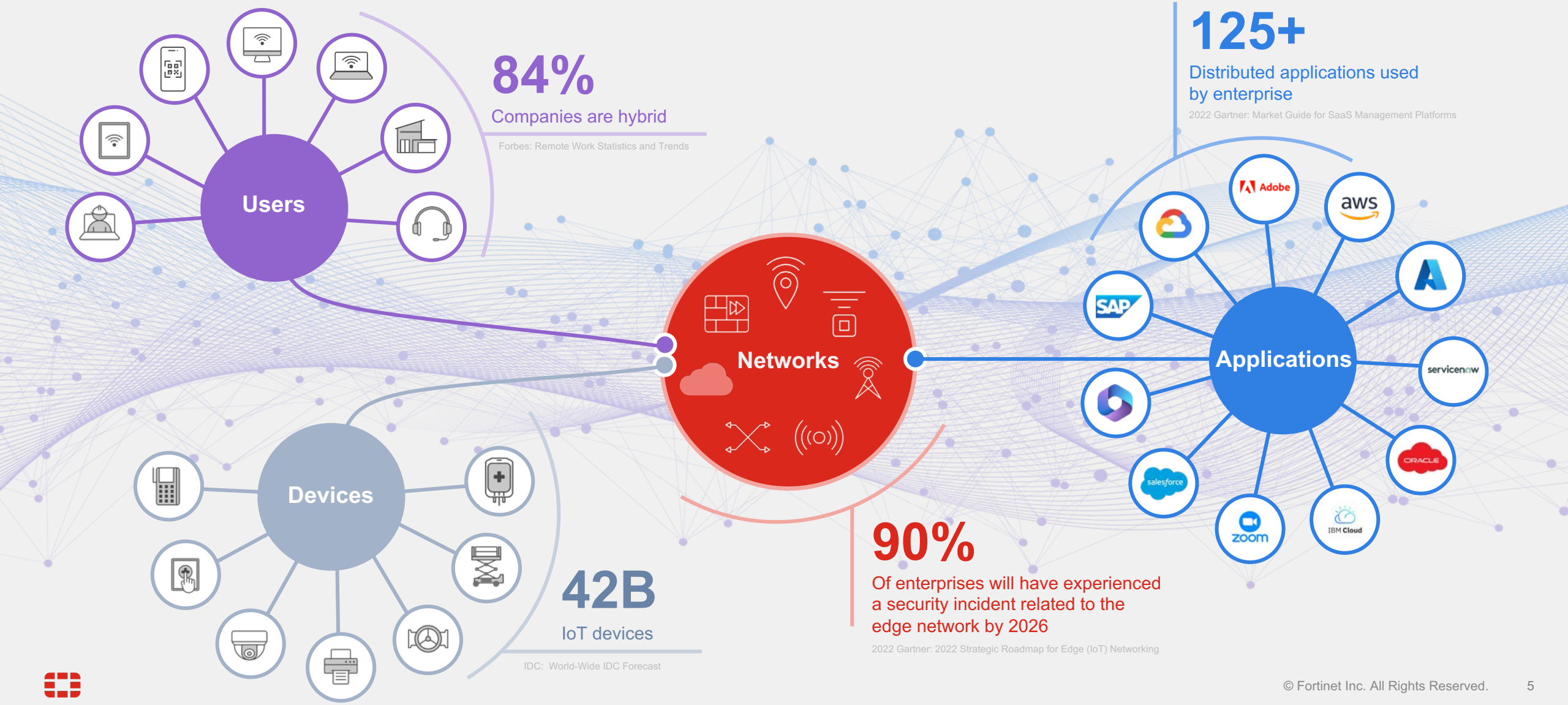
Anatomy of a Ransomware Attack



Anatomy of a Ransomware Attack



Infraštruktúra sa stáva zložitejšou a zraniteľnejšou

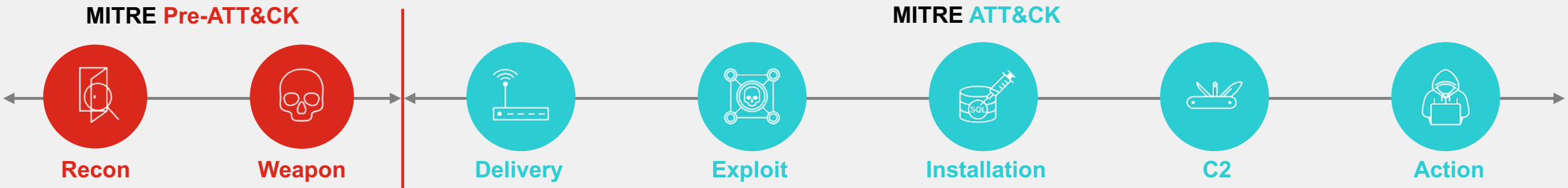


Problém Mačky


FORTINET

Krok číslo jeden – Endpoint Security

How to Break the Attack Sequence



Products & Solutions

Recon	Weapon	Delivery	Exploit	Installation	C2	Action
FortiRecon	FortiRecon	FortiGate (HW/VM/CN/SASE)	FortiGate (HW/VM/CN/SASE)	FortiGate (HW/VM/CN/SASE)	FortiGate (HW/VM/CN/SASE)	FortiAnalyzer Event handlers & reports
FortiDeceptor	FortiDeceptor	FortiProxy	FortiProxy	FortiClient	FortiClient	FortiSIEM Rules Engine & Threat Hunting
		FortiClient	FortiClient	FortiEDR Defuse exploit	FortiEDR Defuse compromised endpoint	FortiSOAR Playbooks
		FortiEDR	FortiEDR Defuse compromised endpoint	FortiDeceptor Defuse Lateral Movement	FortiNDR	IOC Threat hunting
		FortiADC	FortiADC	FortiCWP	FortiSIEM UEBA	Outbreak Detection
		FortiWeb	FortiWeb Web application	FortiSIEM UEBA		ZTNA Auto tagging
		FortiNDR AV+ANN	FortiDeceptor Threat detection, analysis, and response			FortiClient Endpoint search
		FortiMail	FortiSIEM UEBA			FortiEDR | XDR
		FortiCASB				FortiDeceptor Threat intelligence, & attack isolation
		FortiCWP				

FGD AI-Powered Security

	Credential Stuffing Prevention Service	Anti-malware, AV pre-Filter, SBX, Endpoint Vulnerability Protection, App Control, IL CASB, Credentials	IPS, Application, FW, IOT, OT	URL, AV	Botnet, C2, DNS	
		AV, IL SBX, IL CASB	IPS, IoT, OT	URL, AV	C2, DNS	

SOC Augmentation By FortiGuard

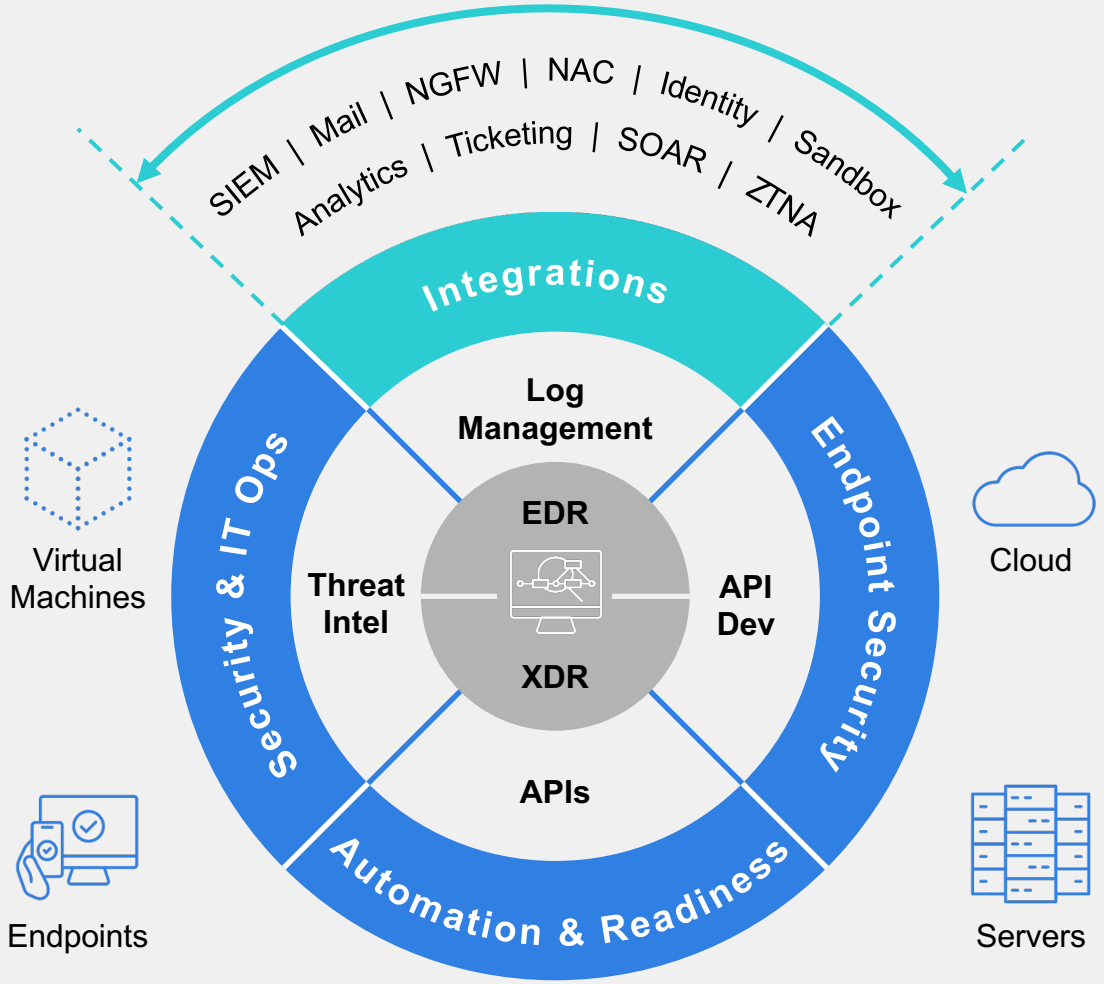
Know Your Risks & Vulnerabilities	Train Your SOC	Managed Detection & Response	Augment Your SOC	Respond Faster and More Effectively
Security Assessments	**IRR, Playbooks, Training**	**MDR**	**SOC as a Service**	**Incident Response**

Viditeľnosť a zmenšovanie priestoru pre útok

FortiEDR/XDR Design Principles

Cloud-native endpoint protection, detection and response

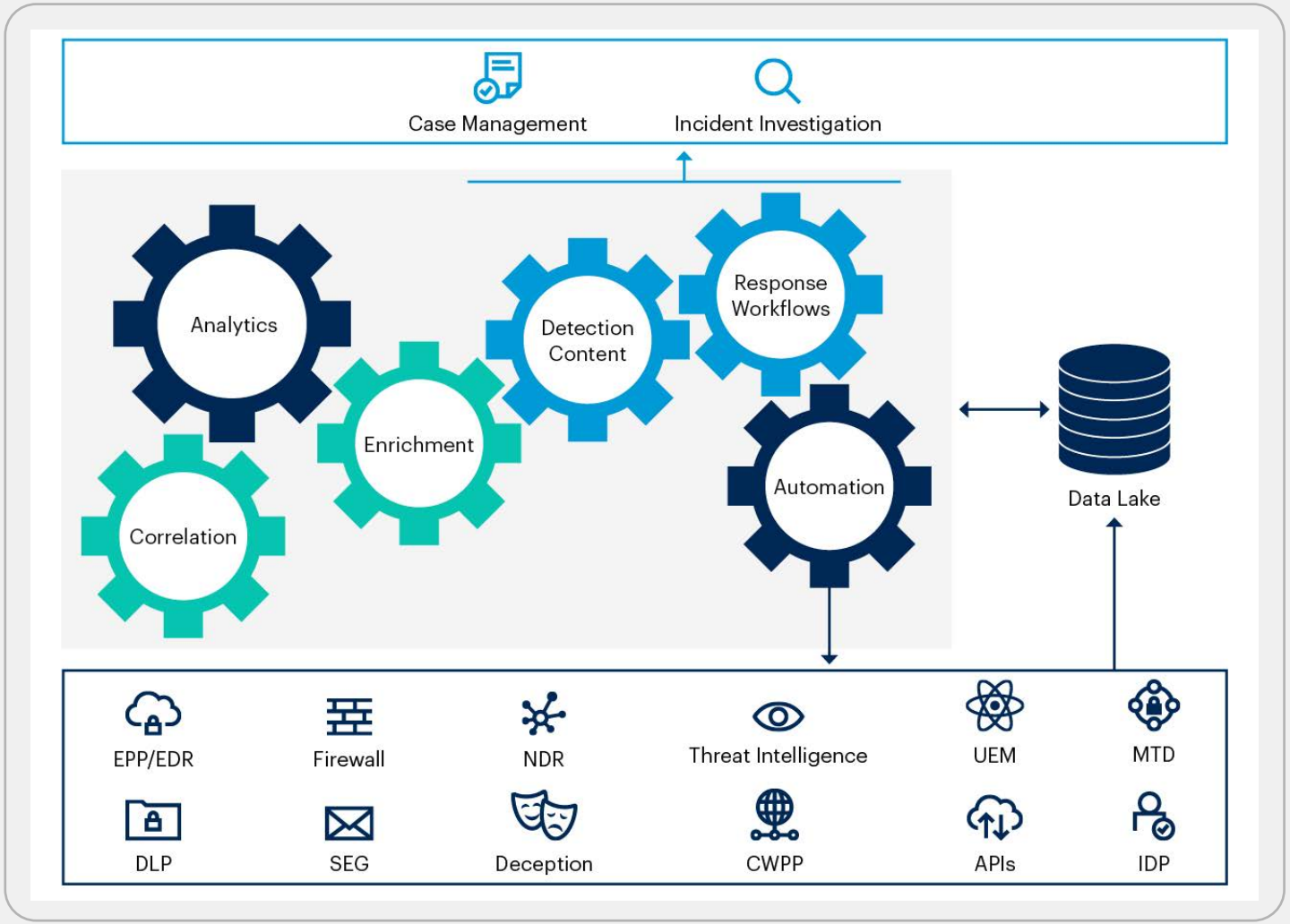
- Kernel-based EPP/EDR client
- ML and behavior-based protection
- Ransomware-proof code tracing
- Lightweight agent
- Support for legacy OSes and hybrid environments with feature parity
- Tamper-proof and evasion resistant
- Complemented by managed services



Odlišnosti
XDR vs EDR

Extended Detection and Response

A perfect principle for vendor consolidation



Source: Gartner Market Guide for Extended Detection and Response. August 17, 2023. Thomas Lintemuth, Peter Firstbrook, Ayelet Heyman, Craig Lawson, Jeremy D'Hoinne

EDR/XDR
Integrácia a automatizácia

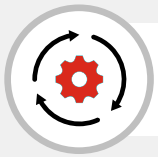
FortiEDR/ForitXDR - Fabric Integration

FortiGate
- Telemetry sharing, automatic blocking of malicious destination IP

FortiNAC
- Extended response - move endpoints to remediation VLAN

FortiSandbox
- Threat intelligence sharing

FortiAnalyzer / FortiSIEM
- Alerts and logs



FortiSOAR
- Extended workflow automation

FortiClient/EMS
- Ingesting endpoint status from EDR for ZTNA posture check

User Access - ZTNA
- Share and assign TAG to hosts following a security posture change

3rd Party Firewall
- Palo Alto, Check Point, Cisco

3rd Party Identity
- Active Directory

3rd Party Mail Security
- ProofPoint

3rd Party SIEM
- Splunk App

3rd Party Event Management
- ServiceNow

3rd Party Access Management
- Microsoft AD, Azure

3rd Party Cloud
- Google SCC, Amazon GuardDuty


SECURITY MANAGERS BE LIKE
SPENT $100K ON A NEW SECURITY TOOL
JUST REALIZED TEAM IS TOO BUSY TO USE IT

FortiGuard Managed Detection and Response

Managed Detection and Response (EDR and XDR)

FortiGuard
Managed Detection & Response

Provides organizations with 24x7 continuous threat monitoring, analysis event triage, and incident handling by experienced analysts using the FortiEDR (XDR) platform.

Threat Detection, Hunting, and Analysis

Containment and Remediation

Notifications and Reporting

Forensics Escalation Requests

Reakcia na incidenty

Intuitive AI Assistance

FortiAI: Built-in GenAI capabilities for proactive threat management and automation

- **Assessment:** Utilize FortiAI to evaluate network anomalies within FortiAnalyzer's data streams.
- **Prediction:** Anticipate potential breaches by applying FortiAI's predictive capabilities to analytics.
- **Best Practices:** Continuously receive recommendations and guidance

Prompts:

- Analyze this incident and tell me what action to take.
- Tell me about this malware and the attackers who use it.
- What response playbooks do you recommend for this alert?
- Create a report of events per critical incident of the last 30 days.

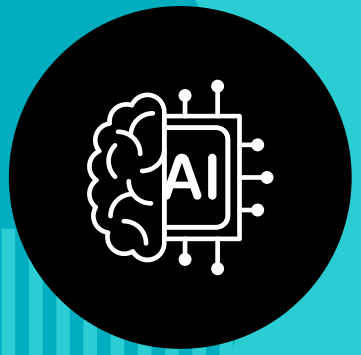
Your Beyond The Fabric Story

Enabling Seamless Investigation Experience and Detection To Response Story

elastic ANOMALI Symantec.
McAfee MySQL LogRhythm CISCO paloalto NETWORKS
Radar RSA ArcSight An HP Company CYLANCE amazon web services
{REST API} IMAP Active Directory Carbon Black. SentinelOne
Check Point SOFTWARE TECHNOLOGIES LTD. FORTINET PHISHME PostgreSQL f5
IBM splunk> tenable Nessus Tor JIRA
QUALYS servicenow cuckoo slack Microsoft virustotal
Microsoft System Center Operations Manager Exchange NETWITNESS REVERSING LABS
';--have i been pwned? MISP Threat Sharing THREATQ HYBRID ANALYSIS

AI Powered Incident Response

Separate the Wheat (Valuable alerts) from the Chaff (noise of false positives)



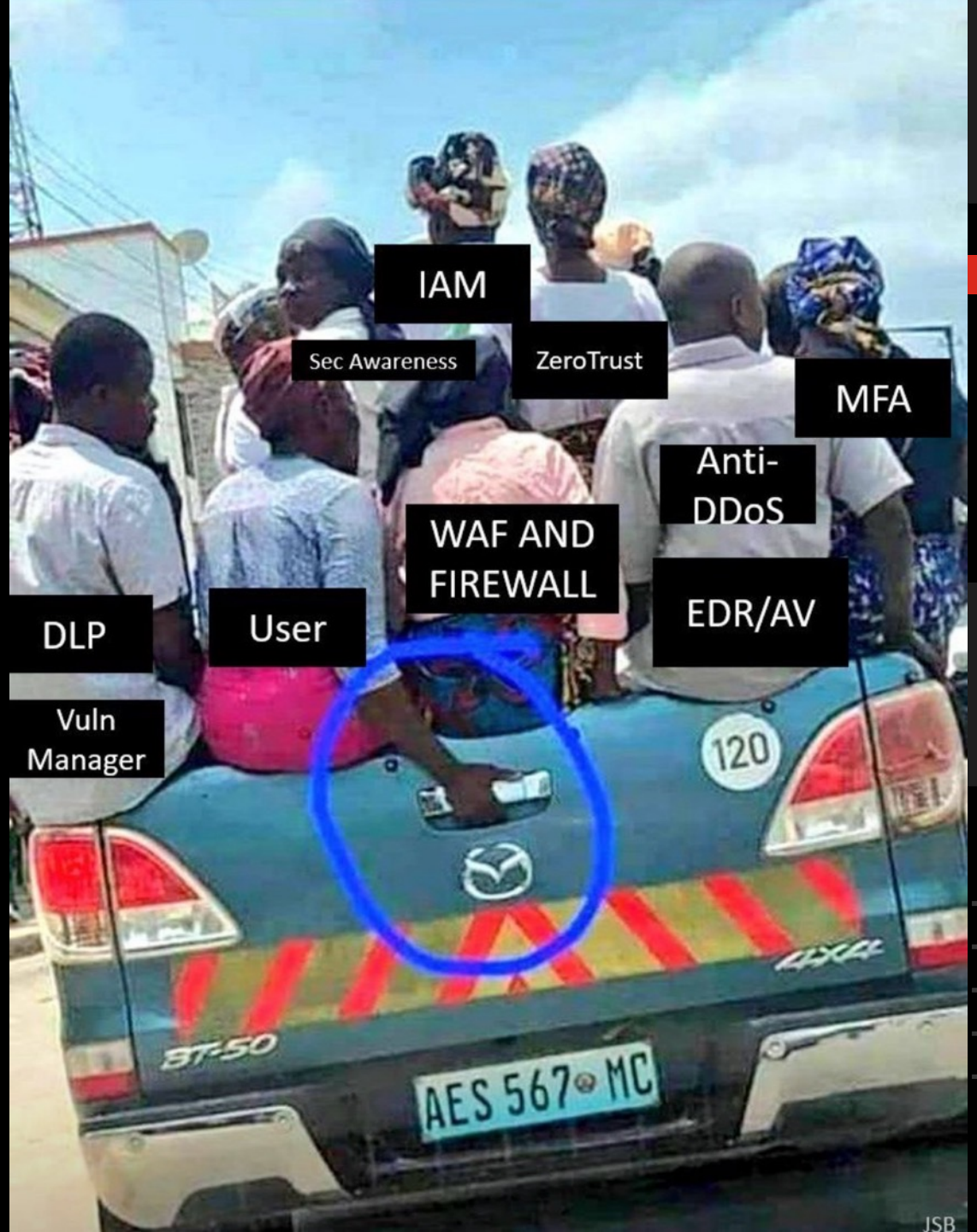
Utilizovať AI pri vyhodnocovaní logov a incidentov

SecOps aj bez Security znalostí vďaka AI

Firewall nieje všetko

”R” v EDR/XDR znamená Response

Automatizácia a integrácia


IAM
Sec Awareness
ZeroTrust
MFA
Anti-DDoS
WAF AND FIREWALL
EDR/AV
DLP
User
Vuln Manager
120
BT-50
AES 567 MC
4X4
JSB