COMGUARD

cyber security masters

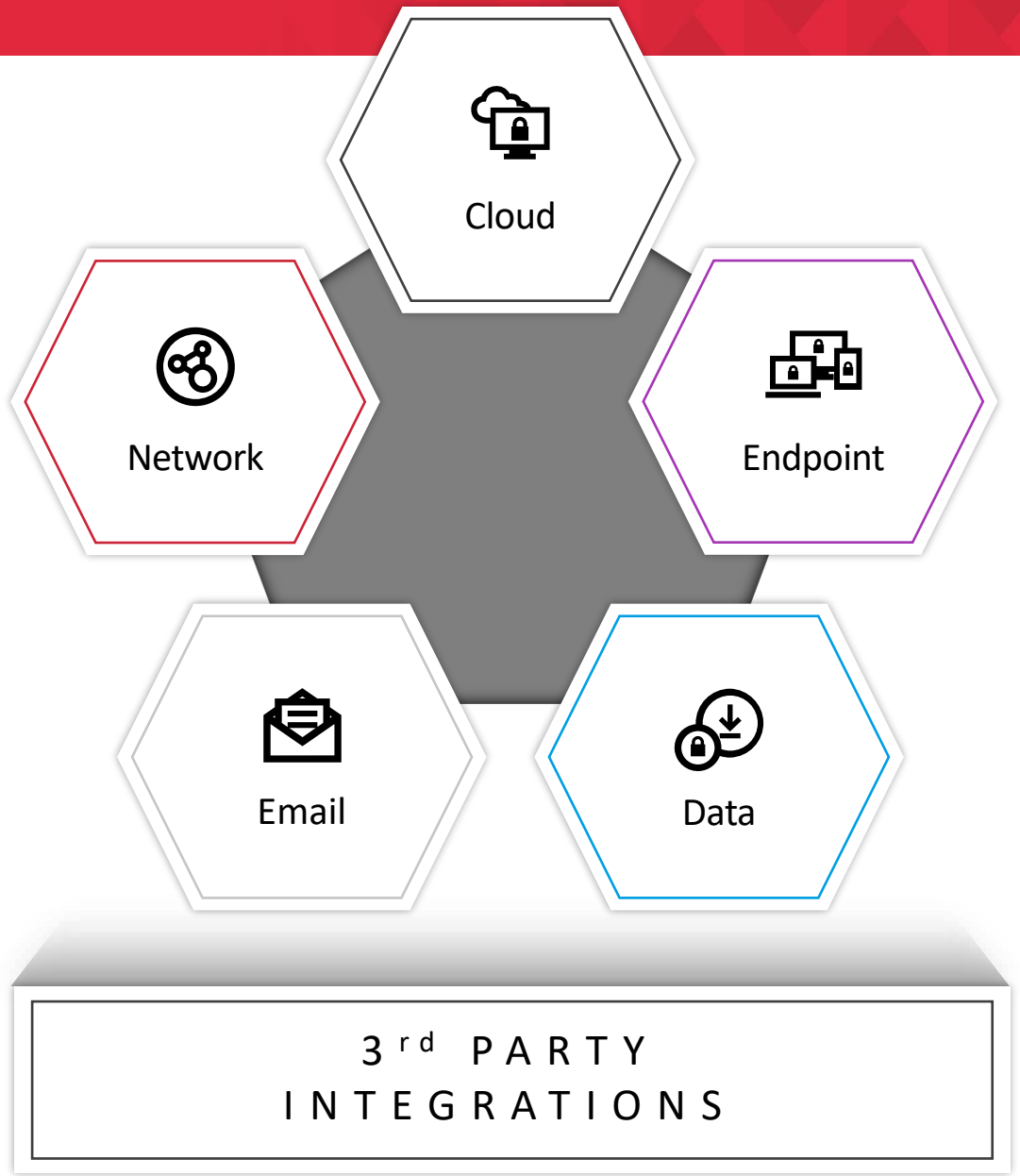
XDR 1. díl skládačky

Endpoint protection (HX)

Thorsten Merz | Solutions Engineer | Trellix

Martin Votava | Sales Director | COMGUARD

Trellix Product Lines



COMGUARD

Trellix XDR Platform

XConsole

Core Engines

- Endpoint Security – unified agent, HX, M EDR
- Data Security – ex M DLP
- Cloud Security – CASB Skyhigh
- Email Security – ex F (on prem, cloud)
- Network Security – IPS, NX, mix
- Secops – ESM SIEM, Helix
- 3rd Party Engine

Advanced Research Center

- Product Research
- Threat Intelligence
- Adversarial Resilience & Advocacy
- Data Science ML / AI
- Research Engineering

Data Lake

COMGUARD

Moderní Endpoint Security

EPP + EDR = Moderní Endpoint Security

Endpoint Protection

- Legacy technologie
- Základní signature-based ochrana
- Důležité pro compliance, audity, …

Endpoint Detection and Response

- Pokročilá technologie
- Detekuje hrozby bez pomoci signatur
- Nasazeno převážně v enterprise prostředí
- Možnosti pro Forenzní analýzu a threat hunting

COMGUARD

Proč Trellix Endpoint Security?

Professional

Persistent

Sophisticated

Systematic

70% DETEKOVANÉHO MALWARE SE OBJEVÍ POUZE JEDENKRÁT *1

68% DETEKOVANÉHO MALWARE JE POUŽITO POUZE PRO KONKRÉTNÍ ÚTOK

Aktuální stav u zákazníků

Pokročilé hrozby nejsou detekovány

Nejsou prostředky pro forenzní analýzu

Vícero agentů různých technologií

Velké množství alertů

Nepřehlednost

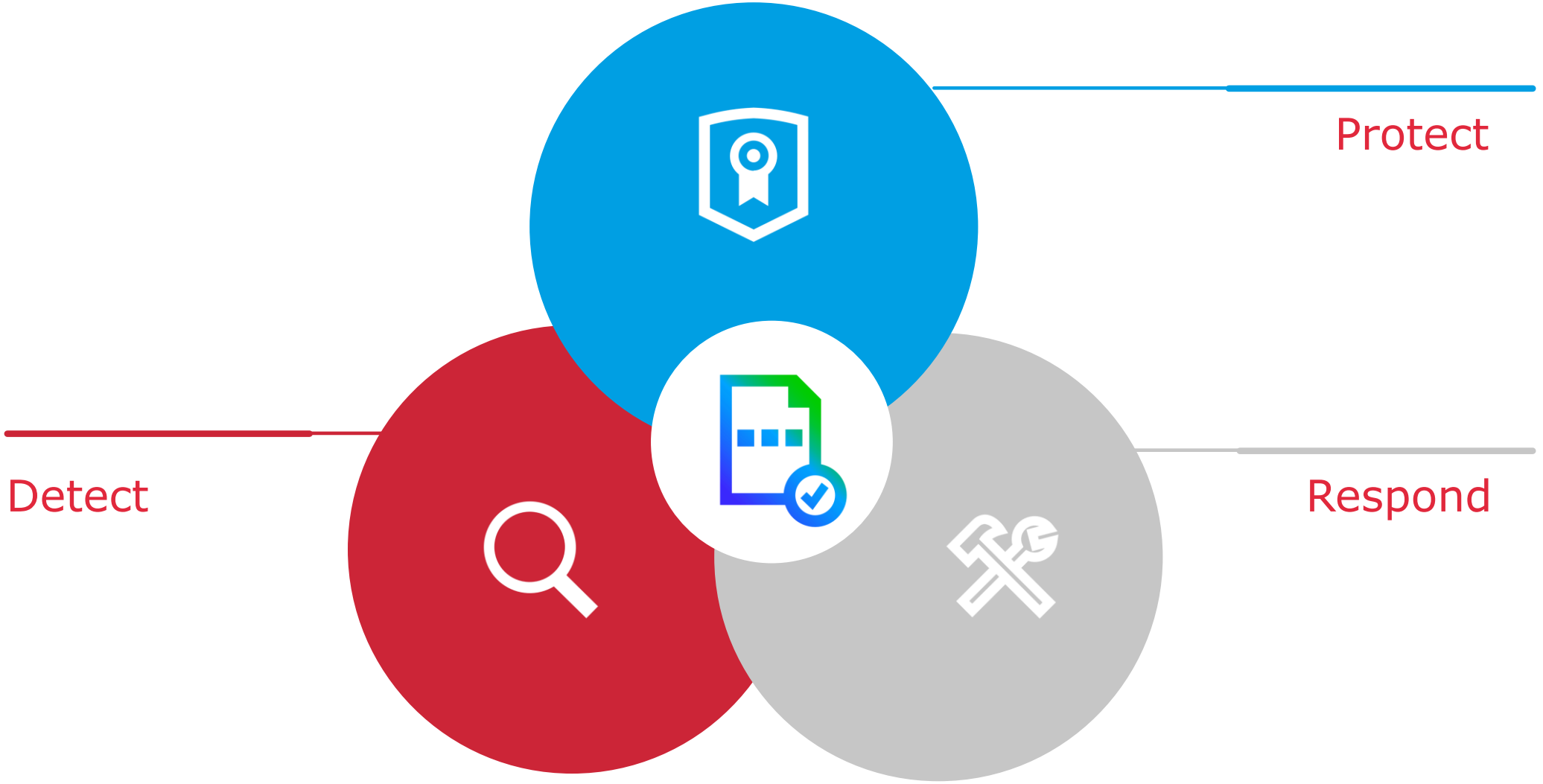
Negativní důsledky

Organizace jsou zranitelné

Nedodržení předpisů může vést k pokutám a ztrátě dobrého jména

Čas strávený sledováním alertů a logů, aniž by byla viditelná hlavní příčina problému

Trellix Endpoint Security (HX)



COMGUARD

cyber security masters

Děkujeme za pozornost!