ALEF

ALEF OctoShield

Powered by Cisco

Jiří Herzig

Presales Engineer, Security

Jiri.Herzig@alef.com

Cisco Partner

Cloud and Managed Service Provider

Řešení OctoShield

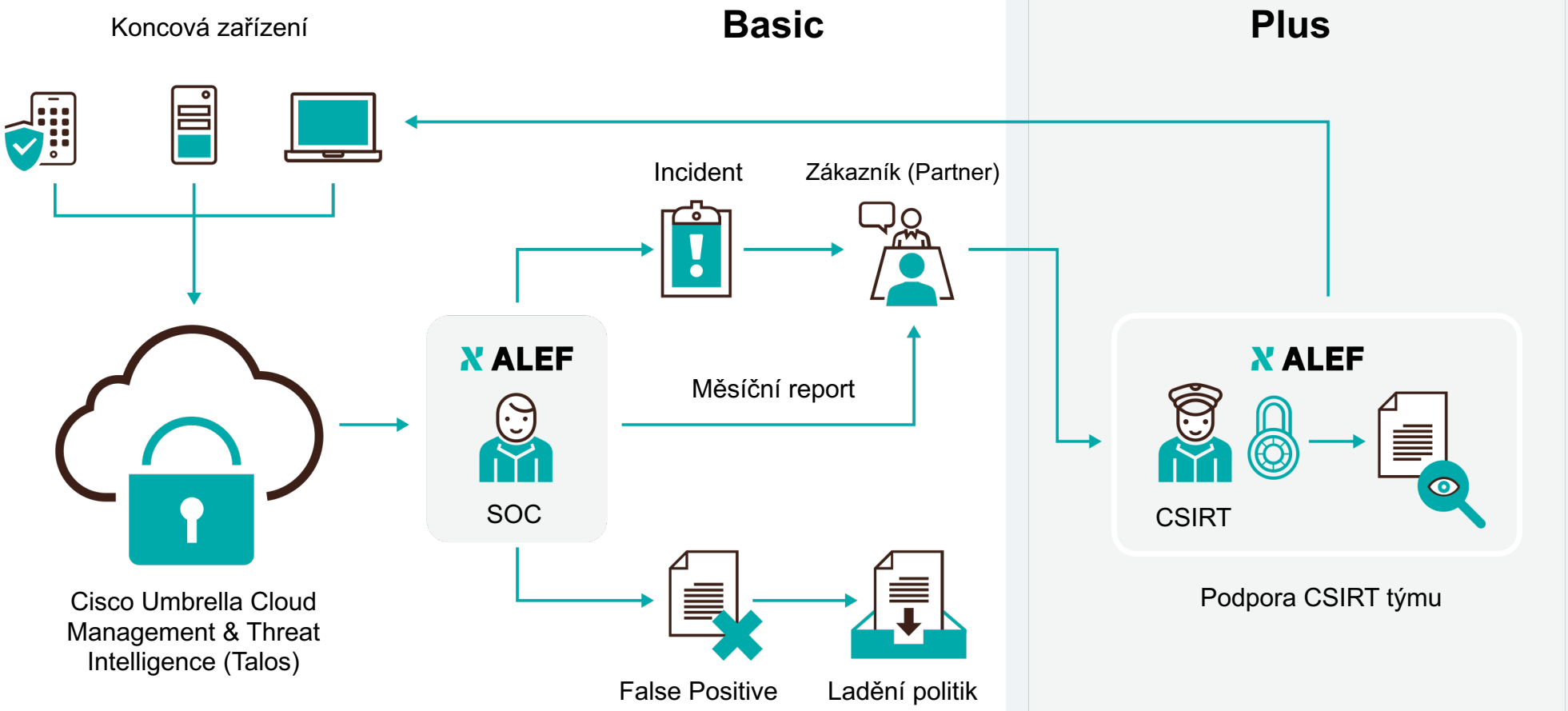
- Obsahuje cloudové produkty od Cisco Systems - Secure Endpoint (AMP4E) a Umbrella
- Ochrana kdekoliv díky největší databázi počítačových hrozeb na světě TALOS od Cisco Systems
- Kombinace dvou produktů přesahuje běžné antivirové programy
- Součástí je i bezpečnostní dohled, vykonávaný lidmi – experty na cybersecurity

Služby v rámci OctoShield

- Aktivace Cloud Management Portálu
- Počáteční nastavení
- Pomoc s instalací
- Zaškolení
- 8x5 bezpečnostní dohled
- Kontaktovaní v případě nálezu malware s doporučeními

ALEF

Koncept služby - OctoShield



OctoShield – jiný produkt než antivirus

Cisco Umbrella v první linii obrany **zablokuje** pokus o stažení malware na základě porovnání **DNS domény** oproti největší reputační databázi na světě – **Cisco TALOS**.
I v případě nakažení malwarem **Cisco Umbrella zablokuje komunikaci na řídicí server (C&C)** a znemožní tak vzdálené ovládání zařízení a díky tomu se **malware nikdy neaktivuje**

cisco Umbrella

- Kontrola souborů pomocí stažených signatur
- Heuristická analýza
- Emulace nativního výpočetního prostředí
- Detekce a analýza odchozí komunikace

Tradiční Antivirová Ochrana

- **Detekce malware** na základě **reputace souborů** získané z jejich analýzy v Cisco Threat Grid (Malware Analytics)
- **Blokace** nezávadných **souborů** které jsou součástí **malware kampaně** (downloader, connector)
- **Retrospektivní analýza** – při změně hodnocení souboru ukáže trajektorii jeho šíření a zablokuje všechny jeho výskyty.
- **Trajektorie zařízení** – kompletní přehled chování zařízení
- **IoC** – možnost hromadného hledání artefaktů malware na zařízeních
- **Behaviorální analýza**

cisco Secure Endpoint

Managed Services

Cena

Cena OctoShield

Cena OctoShield na měsíc pro jedno zařízení

=

Cena jednoho šálku dobré kávy

ALEF

Děkuji za pozornost