COMGUARD

SCADAfence

SCADAfence – Kybernetická bezpečnost v průmyslovém prostředí

S kybernetickými útoky v průmyslovém prostředí se budeme setkávat stále častěji. Provozní technologie jsou mnohem zranitelnější než informační technologie a bezpečnostní incidenty jsou destruktivnější a většího rozsahu.
OT zařízení zpravidla nemají dostatečný výkon pro implementaci bezpečnostních mechanismů jako je šifrování a pokročilé autentizační protokoly. Mnoho OT zařízení bylo navrženo před desítkami let a nepočítalo se z provázanosti do IT světa. Avšak dnes v důsledku konvergence IT&OT, digitalizace a spolupráce jsou čím dál propojenější.

Účelem IT prostředí je přenos velkého množství dat a zpracování informací. Jejich hlavní prioritou je důvěrnost dat. Naopak OT prostředí zajišťuje správné řízení průmyslových procesů. Vzhledem k tomu, že byly navrženy nezávisle na jednotlivých provozech, nebyly tyto sítě nijak zvlášť zabezpečeny, protože jejich ochrana byla řešena na úrovni politik dané společnosti. Pro OT prostředí je podstatná dostupnost systémů, která musí být v režimu 24/7. Z toho vyplývá limitace bezpečnostních záplat, které je možné aplikovat pouze při plánované odstávce, která bývá např. pouze jednou ročně. V případě kompromitace systému je navrácení zařízení do původního stavu také možné pouze v období plánované odstávky. Pokud by došlo k samotné kompromitaci systému, je značně náročnější navrátit zařízení do původního stavu.

Abychom předešli kybernetickému útoku, potřebujeme detekovat zranitelnosti a anomálie v síti. Také potřebujeme monitorovat všechna zařízení a indikovat náznaky útoku.

SCADAfence Platform

Systém pro monitorování průmyslových sítí, který poskytuje jejich kompletní viditelnost. Automaticky monitoruje, jaká zařízení se nachází v síti, detekuje hrozby a zranitelnosti. Využívá širokou škálu algoritmů strojového učení a umělé inteligence a díky tomu dokáže detekovat anomálie v síti, které mohou ohrozit dostupnost systémů a jejich bezpečnost.

SCADAfence Governence Portal

Centrálně definuje a monitoruje dodržování bezpečnostních compliance, které souvisí s OT prostředím. Governance Portal agreguje informace z několika lokalit a sbírá informace z ostatních bezpečnostních systémů.

Reporting – Zobrazuje real-time reporty a automaticky generuje compliance reporty.

Průmyslové standardy – ISO27001, IEC62443, NIST, NERC CIP

SCADAfence Multi-Site Portal

Centrální management pro více SCADAfence Platform nebo pro sledování jednotlivých lokalit.

Klíčové vlastnosti SCADAfence Platform

- **Přehled o OT sítích**, komunikačních vzorcích, odhalení potencionálních útoků
- **Asset Management**
- Monitoring síťového provozu
- Analýza konektivity
- **Monitoruje aktivitu** vzdáleně připojených uživatelů
- **Proaktivně upozorňuje** na zranitelnosti a rizika v OT síti
- Automatické reporty určené pro management
- **Nejmenší false positives nálezy**
- **Risk Reduction** – Pasivně detekuje IoC (Indicators of Compromise) v reálném čase a poskytuje tak včasné informace o náznacích útoku
- **Velké možnosti integrací** se stávajícími IT nástroji
- **Nasazení a základní nastavení je hotovo v rámci jednoho dne**

Integrace

RAPID7 · cybereason · Barracuda · CYBERARK · splunk> · CHECK POINT · KEYSIGHT · FORTINET · paloalto NETWORKS · BELDEN · Gigamon · SIEMENS · IBM Radar · ORACLE · SKYBOX SECURITY · CISCO · GARLAND TECHNOLOGY · zscaler · Secureworks

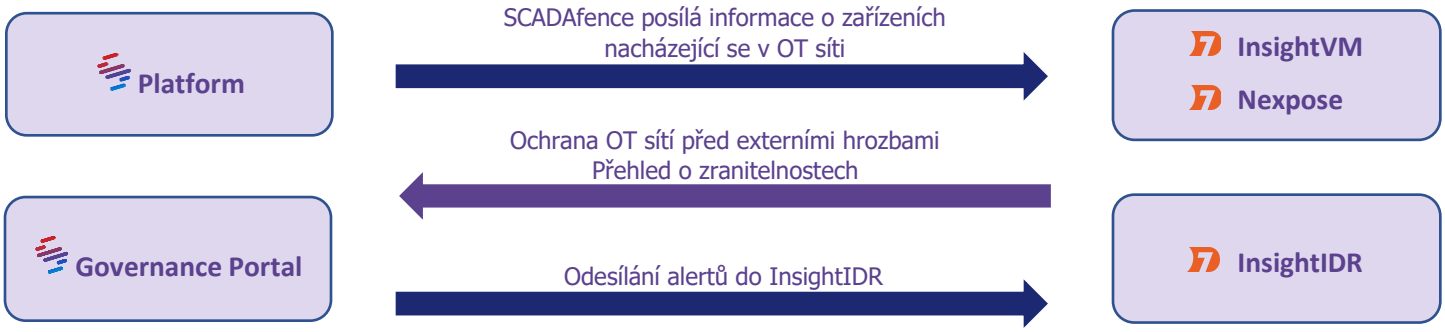
COMGUARD communication security

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz

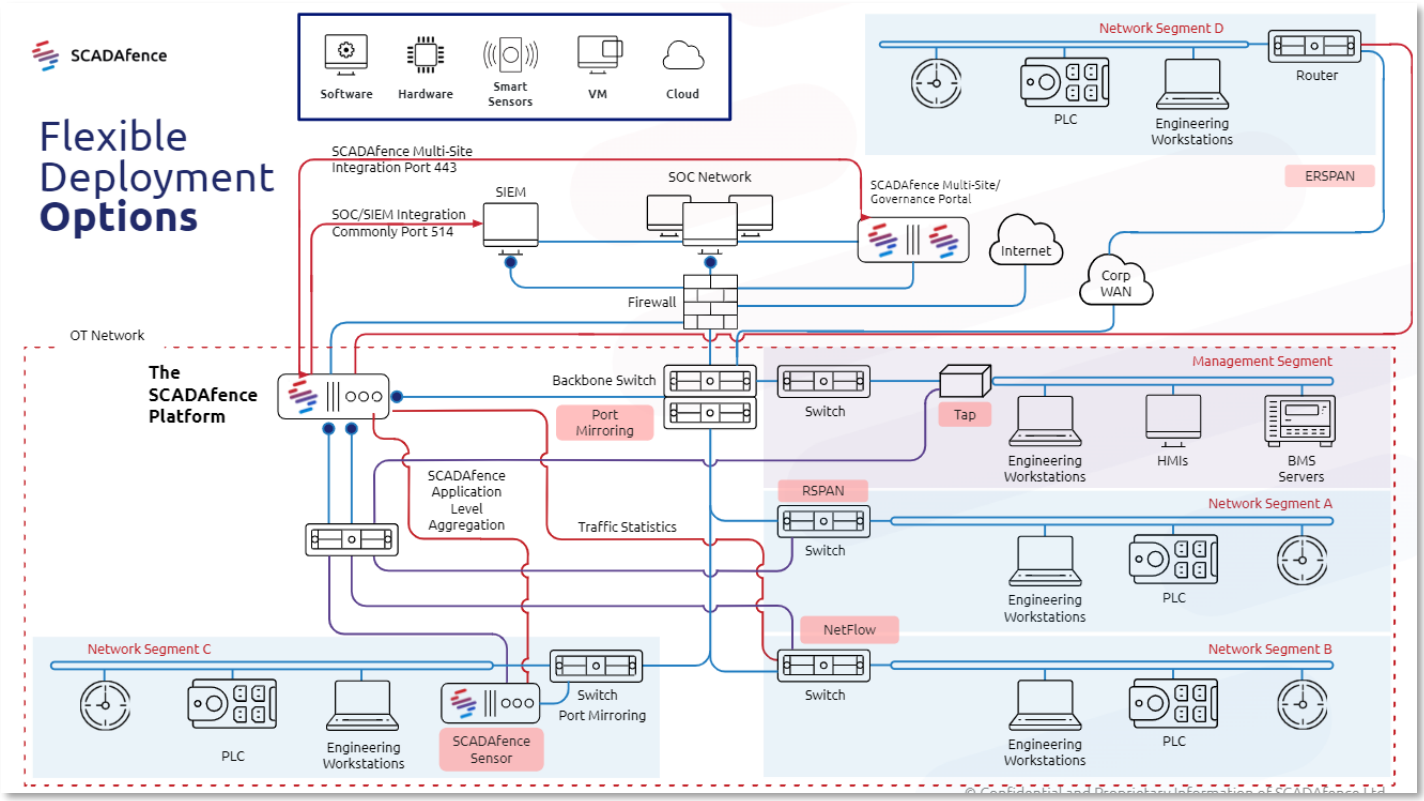
SCADAfence – Kybernetická bezpečnost v průmyslovém prostředí

Integrace SCADAfence Platform a Rapid7

Díky integraci s Rapid7 má stávající admin InsightVM přístup k informacím o **assetech v OT prostředí**, dokáže **prioritizovat zranitelnosti** a plánovat skenování na konkrétní zařízení. Naproti tomu správce OT sítí získá podrobnější přehled o zranitelnostech nacházející se v OT síti a může využívat funkcionality InsightVM. V případě incidentu, SCADAfence **generuje alerty**, které mohou být odeslány do InsightIDR.



Referenční architektura



COMGUARD
communication security

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz