# Siemens Xcelerator: Nový software Siemens automaticky identifikuje zranitelná výrobní zařízení

**16.4.2024 - | Siemens**

**Výrobní zařízení jsou stále častěji terčem kybernetických útoků. Průmyslové podniky proto musí identifikovat a řešit potenciální zranitelnosti svých systémů. S cílem řešit potřebu co nejrychlejší identifikace zranitelných míst v oblasti kybernetické bezpečnosti ve výrobních halách uvede společnost Siemens na trh nový software jako službu z oblasti kybernetické bezpečnosti, který bude poprvé představen na veletrhu Hannover Messe 2024.**

Cloudový systém SINEC Security Guard nabízí automatizované mapování zranitelností a správu zabezpečení optimalizovanou pro průmyslové provozovatele v prostředí OT (Operation Technology). Software dokáže automaticky přiřadit známé kybernetické bezpečnostní zranitelnosti k výrobním prostředkům průmyslových podniků. To umožňuje průmyslovým provozovatelům a odborníkům na automatizaci, kteří nemají specializované odborné znalosti v oblasti kybernetické bezpečnosti, identifikovat rizika kybernetické bezpečnosti mezi OT aktivy ve výrobě a získat analýzu hrozeb založenou na rizicích. Software pak doporučuje a prioritizuje opatření k jejich zmírnění. Definovaná opatření lze také plánovat a sledovat pomocí integrované správy úkolů. SINEC Security Guard je k dispozici jako služba („SaaS“), hostuje jej společnost Siemens a zakoupit jej bude možné v červenci 2024 na Siemens Xcelerator Marketplace a na Siemens Digital Exchange.

Zvýšení ochrany snížením manuálních zásahů

"*Se systémem SINEC Security Guard mohou zákazníci soustředit své zdroje na nejnaléhavější a nejrelevantnější zranitelnosti a zároveň mají ve svém závodě plnou transparentnost rizik. Jde o jedinečný systém, protože zohledňuje specifickou situaci provozního prostředí zákazníka a zároveň poskytuje informace důležité z hlediska bezpečnosti v oblasti OT,*" říká Dirk Didascalou, ředitel pro technologie (CTO) společnosti Siemens Digital Industries. "*Při vývoji SINEC Security Guard jsme vycházeli z našich rozsáhlých zkušeností s kybernetickou bezpečností v našich vlastních továrnách.*"

V současné době mají provozovatelé výrobních technologií (OT) v průmyslu za úkol nepřetržitě zabezpečovat svá výrobní zařízení. Musí analyzovat bezpečnostní doporučení dodavatelů, manuálně je porovnávat s inventářem aktiv v závodě a stanovit priority pro zmírňování dopadů. Protože je tento proces při použití stávajících nástrojů časově náročný a náchylný k chybám, hrozí, že správci přehlédnou kritické zranitelnosti svých aktiv nebo dojde k falešně pozitivním výsledkům. To může vést k nesprávné konfigurací technických prostředků, například síťových komponentů, a neadekvátnímu rozdělení lidských zdrojů. S nástrojem SINEC Security Guard mohou provozovatelé průmyslových provozů tyto problémy řešit, aniž by potřebovali hluboké znalosti v oblasti kybernetické bezpečnosti.

Detekce útoků ve velkém měřítku společně s nástrojem Microsoft Sentinel

Pro komplexní pohled na kybernetickou bezpečnost IT a OT bude SINEC Security Guard nabízet také propojení s Microsoft Sentinel, řešením společnosti Microsoft pro správu bezpečnostních informací a událostí (SIEM – Security Information and Event Managment) pro proaktivní detekci hrozeb, jejich vyšetřování a reakci. Po připojení může SINEC Security Guard odesílat do Sentinelu upozornění na

bezpečnostní události včetně útoků, což umožní bezpečnostnímu analytikovi začlenit poznatky a závěry SINEC Security Guard do vyšetřování a reakcí pomocí center bezpečnostních operací s podporou Microsoft Sentinel. "*Vzhledem k tomu, že informační technologie a provozní technologické systémy se nadále sbližují, je ucelená architektura kybernetické bezpečnosti klíčem k ochraně jak IT, tak OT kapacit. Spojením našich doménových znalostí Siemens a Microsoft usnadňují průmyslovým provozovatelům efektivní odhalování a řešení kybernetických bezpečnostních hrozeb ve velkém měřítku,*" říká Ulrich Homann, korporátní viceprezident pro Cloud + AI ve společnosti Microsoft.

SINEC Security Guard podporuje také ruční nahrávání existujících informací o majetku za účelem jeho inventarizace. Společnost Siemens však doporučuje, aby provozovatelé průmyslových firem používali Industrial Asset Hub, cloudové řešení společnosti Siemens pro správu aktiv, které umožňuje průběžnou automatizovanou správu inventáře aktiv. Mezi funkce patří také detekce narušení sítě a útoků na základě signatur prostřednictvím senzoru SINEC Security Guard, aplikace Industrial Edge, která uživatelům poskytuje živé informace o jejich průmyslové síti. Aplikace SINEC Security Guard Sensor je k dispozici na obchodní platformě Industrial Edge Marketplace společnosti Siemens.

V první verzi aplikace SINEC Security Guard budou pouze prostředky Siemens OT, v budoucnu se plánuje podpora zařízení třetích stran. SINEC Security Guard rozšíří stávající portfolio softwaru Siemens pro zabezpečení OT sítí, které tvoří SINEC Security Inspector a SINEC Security Monitor.

https://www.siemenspress.cz/siemens-xcelerator-novy-software-siemens-automaticky-identifikuje-zranitelna-vyrobni-zarizeni