NÚKIB se zahraničními partnery spolupodepsal dokumenty zaměřené na platformy SIEM a SOAR

27.5.2025 - | Národní úřad pro kybernetickou a informační bezpečnost

Tato série publikací se skládá ze tří dokumentů:

Tento dokument definuje SIEM a SOAR platformy, vysvětluje jejich přínosy i výzvy a nabízí doporučení na vysoké úrovni pro jejich implementaci. Je určen především pro vedení organizací, ale může posloužit jakékoli organizaci, která zvažuje, zda a jak platformy SIEM a/nebo SOAR zavést.

Příručka poskytuje obecná doporučení pro odbornice a odborníky na kybernetickou bezpečnost a popisuje, jak mohou platformy SIEM/SOAR zlepšit viditelnost, detekci a reakci na incidenty. Zabývá se také principy výběru, zavádění a údržby těchto platforem.

Tento dokument přináší podrobná doporučení k logování pro různé typy zdrojů dat – například nástroje pro detekci a reakci na koncových bodech (EDR), operační systémy Windows/Linux, síťová zařízení či cloudová prostředí.

„Jsem rád že se NÚKIB mohl podílet na druhé sérii dokumentů spolupodepsaných pod vedením ASD zaměřených na platformy SIEM a SOAR – technologie, které jsou stále častěji využívány i v České republice. Doporučené principy odrážejí dlouhodobé bezpečnostní standardy, které náš úřad systematicky prosazuje. Je nezbytné, aby se organizace zavazovaly nejen k počátečním investicím do bezpečnostních technologií, ale také k trvalé podpoře lidí a procesů, které tyto systémy provozují. Řešení typu SIEM nebo SOAR, které nezpracovává relevantní data a není aktivně sledováno a laděno, pravděpodobně nebude schopné efektivně detekovat ani reagovat na hrozby“ uvedl ředitel NÚKIB Lukáš Kintr.

https://nukib.gov.cz/cs/infoservis/aktuality/2260-nukib-se-zahranicnimi-partnery-spolupodepsal-dokumenty-zamerene-na-platformy-siem-a-soar