ELLIO a ntop zpřesňují monitorování síťového provozu

29.5.2024 - Jana Tomášiková | PROTEXT

Díky integraci ELLIO: Feedu do řešení ntopng, tj. řešení pro vysokorychlostní 360° monitorování sítě, získají uživatelé hlubší vhled do svého síťového provozu prostřednictvím informací o zdrojích hromadných exploitů, aktivitě botnetů a dalších oportunistických útocích, a to ještě před dostupností tradičních detekčních pravidel na ochranu před známými zranitelnostmi.

"*Blocklisty jsou účinným nástrojem pro blokování útočníků, ale pouze za předpokladu, že jsou podloženy vysoce kvalitními, často aktualizovanými daty s minimálním výskytem False Positives. Používání ELLIO: Feedu v živé produkci nám ukázalo, že ELLIO je díky své analýze a zpracování dat velmi efektivní v odhalování hrozeb. Ve srovnání s jinými bezpečnostními řešeními, jako jsou IDS, ELLIO nevyžaduje neustálý dohled a mnohem lépe zvládá útoky typu zero-day,*" řekl Luca Deri, zakladatel ntop.

ELLIO: Feed je seznam hrozeb, který se dynamicky aktualizuje a obsahuje v průměru až 200.000 IP adres propojených v danou chvíli s útočníky, skeny a dalšími záškodnými aktivitami hromadného zneužití na Internetu. Za spolehlivostí dat stojí vysoce výkonné kombo: rozsáhlá síť internetových senzorů provozovaná ELLIO, pokročilé algoritmy strojového učení a unikátní zpracování dat v reálném čase.

Zkušební verze zdarma

Uživatelé s nejnovější verzí ntopng mají možnost vyzkoušet výhody ELLIO: Feedu zdarma po dobu 30 dní na https://ellio.tech/ntop-feed-trial.

O ntop

ntop je technologická společnost, která poskytuje software pro analýzu síťového provozu, capture-to-disk a traffic generation aplikace, optimalizující výkon komerčně dostupného hardwaru (COTS). Ntop je považovaný za lídra ve své oblasti a představuje standard ve vysokorychlostním monitoringu sítí. Více na https://www.ntop.org/.

O ELLIO

ELLIO Technology je kyberbezpečnostní společnost, která zefektivňuje práci bezpečnostních týmů tím, že eliminuje výstrahy z generických útoků a kybernetického šumu. Prostřednictvím své rozsáhlé sítě internetových senzorů a honeypotů ELLIO sbírá a analyzuje internetový provoz, identifikuje útoky a označuje exploity a zranitelnosti. ELLIO nabízí spolehlivé a plně automatické filtrování kyberšumu a generických útoků na úrovni síťového perimetru. Pomáhá snižovat dopady "alert fatigue", tj. zátěže způsobené nadměrným počtem alertů a eventů v nástrojích SIEM a SOAR. Více na https://ellio.tech/

https://www.ceskenoviny.cz/tiskove/zpravy/ellio-a-ntop-zpresnuji-monitorovani-sitoveho-provozu/2524901