Zákazník

Obor činnosti

Vzdělání a výzkum

Výzvy

- Vysoký výkon
- Rozsáhlá celoevropská síť
- Potřeba získávat detailní a přesné informace v reálném čase s možností historického náhledu
- Vývoj dodatečných detekčních metod
- Integrace s ticketovacím nástrojem třetí strany

Přínosy řešení

- Získání viditelnosti do síťového provozu a zvýšení bezpečnosti infrastruktury
- Možnost poskytovat službu Security as a Service uživatelům sítě GÉANT
- Snížení času a nákladů potřebných na reportování a zvládání provozních a bezpečnostních incidentů
- Doživotní licence, jejímž omezením je pouze výkon HW zařízení

Nasazené produkty

- Flowmon kolektory
- Flowmon ADS ISP

GÉANT

GÉANT je mezinárodní organizace propojující evropské národní sítě pro výzkum a vzdělávání (tzv. NRENy), a to pomocí panevropské datové komunikační infrastruktury. Její páteřní síť poskytuje vědeckým a vzdělávacím institucím po celé Evropě také internetovou konektivitu prostřednictvím až 100G linek. Celkově infrastrukturu této organizace, operující až na rychlostech 500 Gbps, využívá přes padesát milionů uživatelů. S napojením na více jako 100 národních sítí se jedná o největší a zároveň i nejmodernější vědeckou a vzdělávací infrastrukturu na světě.

Situace

Vysoká dostupnost a řízení kvality služeb jsou pro infrastrukturu GÉANTu naprosto klíčové. Každý den je prostřednictvím jeho celoevropské páteřní sítě přeneseno více jak tisíc terabytů dat. Tato infrastruktura poskytuje zákazníkům konektivitu o rychlostech až 100G, a to na páteřní síti, která je designována pro rychlost až 8 Tbps. To zajišťuje, že služby sítě zůstávají v předstihu před potřebami zákazníků a růstem objemu dat. GÉANT v této infrastruktuře využívá řadu různorodých typů routerů s různými verzemi firmwaru, a proto je celé prostředí velmi citlivé na precizní integraci.

Nasazení řešení Flowmon

Cílem nasazení řešení Flowmon bylo získat nástroj pro reporting bezpečnostních událostí, který bude využíván uživateli sítě GÉANT (43 národních výzkumných a vzdělávacích institucí). Řešení umožňuje svým rozsahem odhalovat útoky na síťové služby, botnety, útoky typu port scan, zranitelnosti služeb, zařízení infikovaná malwarem a ostatní nežádoucí aktivity. Řešení Flowmon bylo do infrastruktury GÉANTu nasazeno s tím, že bude sbírat flow data exportovaná z již existujících prvků páteřní sítě (routerů).

Pro zajištění redundance byly paralelně nasazeny dva kolektory, oba vybaveny softwarovým modulem Flowmon ADS pro detekci anomálií a nežádoucího chování v datové síti. Výstupy tohoto systému ve formě bezpečnostních incidentů jsou automaticky předávány ticketovacímu softwaru, který upozorňuje dotčené NRENy, že byla v jejich síti zaznamenána nežádoucí událost narušující bezpečnost. Celé řešení bylo nasazeno v řádu hodin. Následné testování na straně zákazníka, integrace a dovývoj zákaznicky-specifických detekčních metod zabraly dva měsíce. Tyto aktivity se poté odrazily v pilotním programu a celá služba byla oficiálně spuštěna v produkčním prostředí o tři měsíce později.

Hodnocení zákazníka

Nasazení řešení Flowmon hodnotí Wayne Routly, Head of Information & Infrastructure Security organizace GÉANT, následovně:

„Řešení Flowmon jsme si vybrali ve výběrovém řízení, kterého se účastnilo dvanáct konkurenčních produktů. Po třech měsících intenzivního testování jsme si potvrdili, že je to ten pravý produkt pro naši síť, a to díky jeho výkonnosti, schopnostem detekovat anomálie, škálovatelnosti a jednoduchosti správy a konfigurace řešení. Jsem rád, že uživatelé naší sítě vidí v reportingu bezpečnostních incidentů důležitý přínos a mají enormní zájem o tuto naši novou platformu v rámci projektu NSHaRP.“