# Technická specifikace plnění

**Dodávka, implementace a podpora řešení pro síťovou visibilitu a ochranu koncových bodů**

Předmětem plnění je nasazení technologie Aktivního XDR, tedy kombinace síťového systému NDR, systému pro ochranu koncového bodu EDR. Produktově je řešení založeno na platformě Fidelis Elevate, které zmíněné funkcionality pokrývá moduly Fidelis Network a Fidelis Endpoint, které jsou integrovány do jednotné detekční, vyšetřovací a reakční platformy.

Fidelis Network bude monitorovat síťový provoz a detekovat hrozby pohybující se po síti. Současně také poskytne údaje – historický popis provozu – které budou využívány při vyšetřování incidentů.

Fidelis Endpoint bude nasazen na koncových bodech a bude monitorovat dění na nich. Současně se záznamem chování aplikací a operačního systému bude provádět nad těmito údaji behaviorální analýzu s cílem rozpoznat hrozby, které zasáhly koncový bod.

V analýze síťového provozu bude pomáhat systém kategorie packet-broker, který je schopný ze síťového provozu odstranit tu část, kterou nemá smysl analyzovat (typicky backupy, video streamy) ze strany NDR, shromáždit všechen provoz z různých zdrojů (síťové prvky, virtualizační paltformy), provést jeho deduplikaci případně další pokročilé filtrování a odeslat výsledný provoz do senzorů systému NDR. Další funkcionalitou tohoto systému může být také dešifrování síťového provozu s cílem umožnit jeho analýzu.

Výše popsané řešení bude sloužit bezpečnostním specialistům pro včasné rozpoznání hrozeb, které vznikly přímo v prostředí školy, nebo se do školy snaží dostat přes jejích bezpečnostní perimetr.

V kvantitativní rovině bude řešení pokrývat:

- 2 Gbps monitorovaného provozu
- 2500 koncových bodů (stanic a serverů)

Retence ukládaných vyšetřovacích dat (metadat) bude 30 dní

Dodávka licencí SW / HW

| **popis licence / HW** | **Qty** |
|---|---|
| **Fidelis Elevate** | |
| FNL-2G-30D-INT - Fidelis Network Software Perpetual License for up to 2 Gbps of aggregate peak monitored bandwidth and 30 days of metadata storage.<br>* Annual Premium Software Support and Threat feed included | 1 |
| FNL-2G-30D-SUP-INT - FNL-2G-30D Annual Premium Software Support and Threat feed | 2 |
| FSS-SW-R1-SE-INT - Fidelis Endpoint agent software, perpetual license.<br>* Annual Premium Software Support and Threat feed included | 2500 |
| FSS-SW-R1-SE-SUP-INT - Fidelis Endpoint agent software, annual premium support for perpetual software license. Includes phone support, software upgrades and threat feed. For 2500 Endpoints | 2 |
| **Gigamon Fabric Manager (GigaVUE-FM)** | |
| GigaVUE-FM, manage 1 Physical Visibility Fabric Node (Promotion/Evaluation 1 seat license)<br>* Annual Software support included | 2 |
| Annual Software support program fo GigaVUE-FM for 2 seat licences | 2 |
| **Gigamon GigaVUE-HC1** | |
| GigaVUE-HC1 chassis, 12 1G/10G cages, 4 10/100/1000M Copper, fan tray, 2 power supplies, AC power. Hardware only. Must pair with appropriate GigaVUE-OS Software License. Gigamon Advance Hardware Replacement with direct Gigamon support, available with Subscription enabled hardware products at time of product purchase.<br>* Annual HW support included | 2 |
| Annual HW support for GigaVUE-HC1 chassis, 12 1G/10G cages for 2 HW appliances | 2 |
| GigaVUE-OS Term Software License for GigaVUE-HC1 (GVS-HC101-HW or GVS-HC102-HW). Includes Elite-Plus Software Support Program.<br>*Annual Elite-Plus Software Support included | 2 |
| Annual Elite-Plus Software Support Program for GigaVUE-OS Term Software License for GigaVUE-HC1 for 2 licences | 2 |
| **GigaSMART licenses for Advanced Traffic processing** | |
| CoreVUE GigaSMART software bundle for GigaVUE-HC1. Capabilities included: Advanced Tunneling, Header Stripping, Slicing, Masking, Advanced Load Balancing, Source Port Labeling. Includes bundled Elite-Plus Support | 2 |
| Annual subscription license for GigaSMART, GigaVUE-HC1 license, De-Duplication feature. Includes embedded Elite-Plus Support. This is a Gen 2 license. For 2 GigaSMART, GigaVUE-HC1 license | 2 |
| 20 pack of 10Gb SFP+, Multimode SR. Not TAA Compliant. | 1 |

**Měsíční technická správa platformy Fidelis Elevate**

Služba měsíční technické správy platformy **Fidelis Elevate** zahrnuje kompletní údržbu, dohled a správu systémových komponent s cílem zajistit stabilní, výkonný a aktuální provoz platformy. Zaměřujeme se na správné fungování infrastruktury Fidelis, jejích modulů a integrací, s důrazem na dostupnost, výkon a konzistenci konfigurace.

**Obsah služby:**

- **Zdravotní kontrola systému**
    - Kontrola dostupnosti a výkonu jednotlivých komponent (Collector, Decoder, CommandPost, DataVault, atd.)
    - Ověření komunikace mezi komponentami a stavů systémových služeb
- **Správa systémových aktualizací**
    - Nasazování doporučených verzí softwaru a bezpečnostních záplat (patch management)
    - Aktualizace pravidel a signatur bez zásahu do detekčních politik
- **Správa konfigurace a systému**
    - Kontrola integrity konfiguračních souborů a systémových parametrů
    - Údržba a úprava nastavení (např. logování, úložiště, limity a timeouty)
    - Správa připojení na externí systémy (SIEM, LDAP, SMTP, syslog)
- **Monitorování systémových zdrojů**
    - Dohled nad využitím CPU, RAM, diskového prostoru a síťové propustnosti
    - Detekce a řešení potenciálních problémů s výkonem nebo kapacitou
- **Zálohování a obnova konfigurací**
    - Pravidelné zálohování konfigurací jednotlivých komponent
    - Možnost obnovy do funkčního stavu v případě poruchy nebo výpadku
- **Technická podpora a konzultace**
    - Diagnostika a řešení systémových chyb nebo výpadků
    - Konzultace ohledně rozšíření infrastruktury, upgradu či změn konfigurace
- **Reporting technického stavu**
    - Měsíční technický report s přehledem provedených úkonů, stavu systému a doporučeními

**Měsíční technická správa platformy Gigamon**

Měsíční správa zařízení **Gigamon GigaVUE-HC1** zahrnuje kompletní údržbu a technickou správu fyzického zařízení i softwarové platformy **GigaVUE-OS**, včetně pokročilých funkcí modulu **GigaSMART**. Cílem služby je zajistit vysokou dostupnost, výkon a správnou distribuci síťového provozu pro analytické a bezpečnostní nástroje.

---

**Rozsah služby**

**1. Zdravotní a provozní dohled**

- Monitoring provozního stavu a dostupnosti všech fyzických rozhraní (1G/10G SFP+, 1G RJ45)

**2. Správa GigaVUE-OS**

- Audit aktuální verze GigaVUE-OS a posouzení potřeby aktualizace
- Nasazení schválených aktualizací včetně ověření kompatibility s GigaSMART licencemi

**3. Zálohování a konfigurace**

- Pravidelné zálohy běžící i uložené konfigurace zařízení
- Dokumentace topologie připojení (TAP/SPAN zdroje, tool porty, inline nástroje)
- Správa přístupových účtů, SSH certifikátů a SNMP konfigurací

**4. Správa GigaSMART modulů**

- **Deduplikace provozu**
    - Nastavení a ladění deduplikace (time-based, sequence-based) pro snížení zátěže downstream nástrojů
- **Tunneling a de-tunneling**
    - Konfigurace GRE/ERSPAN de-tunnelingu pro rozbalení provozu ze vzdálených lokací
    - Podpora VXLAN, MPLS, GTP stripping dle aktivovaných funkcí
- **NetFlow generace (GigaSMART NetFlow)**
    - Aktivace a správa NetFlow exportu (v5, v9, IPFIX) přímo ze zařízení
    - Směrování flow záznamů na kolektory, optimalizace šablon
- **Packet Slicing**
    - Nastavení ořezávání paketů podle typu provozu nebo délky hlaviček pro snížení objemu dat
- **TLS/SSL Metadata Extraction**
    - Aktivace sběru metadat z TLS handshake (verze, SNI, certifikáty) bez dešifrování obsahu
- **Latency/Timing Analysis**
    - Aktivace časových značek pro latency analýzu v rámci vybraných tool portů

**Rozsah možných ad hoc prací na platformách Fidelis Elevate a Gigamon**

Tato část stanoví příklady ad hoc (jednorázových, nestandardních) prací, které lze vykonávat na bezpečnostních a monitorovacích platformách Fidelis Elevate a Gigamon GigaVUE-HC1. Tyto účely nespadají do pravidelné měsíční správy a jsou prováděny na základě zvláštních požadavků, incidentů nebo změn v infrastruktuře.

**1. Ad hoc práce na platformě Fidelis Elevate**

**1.1 Rozšíření a integrace**

- Nasazení nových komponent (Collector, Decoder, CommandPost)
- Integrace s externími systémy (SIEM, SOAR, EDR, threat intel)
- Zavedení TLS dešifrovacích bodů

**1.2 Migrace a změna infrastruktury**

- Migrace na nové servery nebo lokace
- Změna adresace, routovací topologie
- Virtualizace nebo fyzická konsolidace

**1.3 Ladění a troubleshooting**

- Diagnostika chyb nebo výpadků služeb
- Vyčistění nebo obnovení databází
- Reset komponent po závazné chybě

**1.4 Pokročilé detekční funkce**

- Tvorba vlastních pravidel (PCRE, YARA)
- Nastavení vlastních alertovacích mechanismů

**2. Ad hoc práce na platformě Gigamon**

**2.1 Architektonické změny**

- Zavedení nových TAP/SPAN zdrojů
- Redesign FlowMaps, ToolMaps a distribuce provozu
- Přidání nových portů nebo nástrojů

**2.2 Aktivace GigaSMART funkcí**

- NetFlow generace a export (v5/v9/IPFIX)
- GRE/ERSPAN/VXLAN de-tunneling
- Deduplikace, slicing, TLS metadata extrakce

**2.3 Reakce na změny v síti**

- Rekonfigurace portů a map
- Přesměrování provozu po změně architektury

**2.4 Upgrade a problémové stavy**

- Asistence při upgradu GigaVUE-OS
- Diagnostika výkonnostních úzkých hrdel