Příloha č. 2

**Systém SIEM (Security Information and Event Management) pro ICT ČSÚ**
- technický popis předmětu plnění

| Požadované funkce | Parametr |
|---|---|
| Příjem/stahování dat z požadovaných zařízení | Ano |
| Univerzální podpora pro všechny IP zařízení a aplikace | Ano |
| Varování na možné bezpečnostní hrozby | Ano |
| Možnost sledování cílů v oblasti Bezpečnosti | Ano |
| Možnost analýzy dat v reálném čase a jejich zobrazení pomocí Event Exploreru | Ano |
| Nonstop provoz | Ano |
| Instalace bez klientských agentů | Ano |
| Grafický přehled o výkonu systému a bezpečnostních událostech | Ano |
| Přehledné webové rozhraní pro správu | Ano |
| Analytický nástroj pro intuitivní ovládání a pokročilé analýzy | Ano |
| Ukládání dat, rozpoznávání trendů a tvorba výkazů | Ano |
| Počet trvale sledovaných událostí za vteřinu | min 1000 |
| Počet sledovaných systémů | min 150 |
| Počet současných uživatelů SIEM | min 8 |
| Počet současných uživatelů Exploreru | min 5 |
| Interní úložiště logů | min 300 GB |
| Možnost připojení externí úložiště | Ano |

Pořízený systém SIEM musí umožnit vysílat výstrahy, monitorovat, produkovat výkazy a bezpečně ukládat logy. Musí umožnit administrátorům, tzn. vybraným pracovníkům ČSÚ (IT bezpečnosti a IT podpory) zkoumat uložené logy pomocí intuitivního ovládacího rozhraní – musí to být pokročilý analytický software, který převádí rozsáhlou nestrukturovanou masu prvotních dat do podoby strukturovaných informací, které poskytnou důležité poznatky v těchto třech hlavních oblastech:

- zjednodušení shody s předpisy;
- zdokonalení bezpečnosti a řízení rizik;
- optimalizace IT a sítových operací.

Předpokládá se, že součástí pořízení systému SIEM bude příprava dostatečného počtu výstupů/výkazů systému, zajišťujících shodu s platnými předpisy – požaduje se, aby byla zaručena průběžná rozšiřitelnost/aktualizace těchto výkazů na základě postupného zavádění nových předpisů.

Systém musí být připraven na soulad s předpisy, které se mohou v rámci ČSÚ objevit = ukládání dat bez filtrování, normalizace, chránit data před zfalšováním v podobě autentizovaného, ověřitelného zdroje uchovávaných dat.

Systém musí disponovat výstrahami v reálném čase, monitorovat a disponovat forenzními funkcemi, aby administrátoři měli jasný pohled na důležité informace a mohli je tak lépe chápat a účinně předcházet a zmírňovat rizika.

Systém musí být využitelný ke sledování a správě logů síťových zařízení a úložišť, a současně k monitorování hardwaru a používaných aplikací. Systém musí poskytovat inteligentní forenzní nástroj pro odhalování problému s infrastrukturou, pomáhat administrátorům a poskytovat detailní přehled o konkrétním chování konkrétních koncových uživatelů, které následně umožní vyhodnotit a optimalizovat IT a síťové operace.