1. számú melléklet

Műszaki leírás

AI alapú IT védelmi és hálózati forgalomelemző rendszer

Az Országgyűlés Hivatala, mint Vevő egy Mesterséges Intelligenciát (Artificial Intelligence, a továbbiakban AI) alkalmazó hálózatbiztonsági védelmi és hálózati forgalom elemző rendszert, illetve a bevezetéséhez szükséges hardver eszközöket, szoftver licence-eket és azokhoz szükséges implementációs szolgáltatásokat kíván beszerezni. Az AI-t alkalmazó hálózatbiztonsági védelmi és hálózati forgalom elemző rendszer beszerzésének célja, hogy jelentősen megerősítse a jelenlegi hálózatbiztonsági védelmi infrastruktúrát, illetve olyan képességekkel egészítse ki azokat, amelyekkel jelenleg nem rendelkeznek, valamint, hogy a meglévő infrastruktúra elemekkel való integrációja révén lehetővé tegye a nemkívánatos, vagy egyértelműen rosszindulatúnak nyilvánított hálózati forgalmak igény szerinti automatizált blokkolását.

Továbbá a rendszernek biztosítania kell a hálózati adatforgalom és kommunikáció folyamatos, valós idejű és több hónapra való historikus jellegű követését is, az azonnali, vagy utólagos hibaelemzésekhez és hibafeltárásokhoz egyaránt, valamint a rendszer fejlett hálózati biztonsági forgalomelemző és riporting képességekkel kell rendelkezzen.

Beszerzendő termékek és szolgáltatások:

- hálózati forgalom analitikai eszközök,
- hálózati forgalom anomália detektáló eszköz,
- hálózati forgalom rögzítő modul,
- az összes szükséges szoftvert örökös licence-el kell leszállítani,
- telepítési és jótállási szolgáltatások.

Az AI-t alkalmazó IT védelmi és hálózati forgalom elemző rendszer kapcsán a megadott specifikáció szerinti következő eszközöket kérjük leszállítani:

Virtuális adatgyűjtő (collector) eszköz műszaki specifikációja

- legalább 6 TB háttértárkapacitású hálózati forgalom tárolására alkalmas licence-el kell rendelkeznie.

- virtuális szoftver eszköz legyen (VMware, Hyper-V, KVM, AWS, Azure, Google Cloud támogatás),
- Támogatott virtualizációs platform: VMware ESXi (8.x), Microsoft Hyper-V (2012 R2 vagy magasabb verzió), KVM (KVM 3.10.0, QEMU 1.5.3, libvirt 4.5.0 vagy magasabb verziók),
- legalább 2 db menedzsment port támogatás,
- legalább 2 db 1Gbps Ethernet monitorozó (NetFlow/IPFIX) port támogatása,
- parancssoros, WEB-GUI és virtuális konzol vezérelhetőség támogatása,
- legalább 150.000 flow/sec feldolgozó képesség,
- NetFlow, IPFIX, sFlow, jFlow, NetStream, CFLOWD típusú adatok fogadása és feldolgozása,
- beépített flow gyűjtés és analitikai képesség, megjelenítés és riporting képesség, automatizált riporting képesség,
- hálózatforgalom vizualizáció, dashboard képesség, „Top N" statisztikák, egyedi felhasználói profilok, hibakeresési képesség,
- aggregáció L2-L7 paraméterek alapján – pl. DNS válaszkódok, HTTP URL 2/3 szintjei, TLS változatok, JA3 fingerprint.

„A" típusú hálózati forgalom monitorozó eszköz műszaki specifikációja

- hardver eszköznek kell lennie,
- legalább 2x10/25 Gbit Ethernet monitor port támogatás – line rate feldolgozás (legalább 1,5 Mpps monitor port teljesítmény, legalább 3Mpps eszköz teljesítmény; Flow cache: legalább 4M flow/monitor port),
- 1 U kiépítésű legyen,
- legalább 12 processzormag, Hyper Threading támogatás,
- legalább 64 GB RAM memóriakapacitás,
- hálózatforgalom monitorozás és IP flow generálás képesség,
- legalább 2 db 10/100/1000 Mbps Ethernet menedzsment port
- Netflow/IPFIX statisztika készítése, L2-L4 (protokollok: legalább VLAN, MPLS, GRE, OTV, ESP, and VxLAN, SRT, RTT, jitter stb.), L7 (legalább hostnevek, URL, böngésző információk HTTP/S protokolloknak, DNS, DHCP, SQL, SMTP, Samba/CIFS, VOIP, SSL/TSL, CoAP, IEC104).

- beépített legalább 500 GB flow analizátor collector-onként,
- built-in geolokáció és autonomous system megfeleltetés.

„B" típusú hálózati forgalom monitorozó eszköz műszaki specifikációja

- hardver eszköz legyen,
- legalább 4x1 Gbit Ethernet monitor port támogatás (legalább 1,48 Mpps monitor port teljesítmény, legalább 3Mpps eszköz teljesítmény; Flow cache: legalább 0,5M flow/monitor port).
- 1 U kiépítésű legyen,
- legalább 8 processzormag, Hyper Threading támogatás,
- legalább 32 GB RAM memóriakapacitás,
- hálózatforgalom monitorozás és IP flow generálás képesség,
- legalább 2 db 10/100/1000 Mbps Ethernet menedzsment port,
- Netflow/IPFIX statisztika készítése, L2-L4 (legalább protokollok VLAN, MPLS, GRE, OTV, ESP, VxLAN, SRT, RTT, jitter stb.) L7 (legalább hostnevek, URL, böngésző információk HTTP/S protokolloknak, DNS, DHCP, SQL, SMTP, Samba/CIFS, VOIP, SSL/TSL, CoAP, IEC104),
- beépített legalább 500 GB flow analizátor collector-onként,
- built-in Geolokáció és Autonomous System megfeleltetés.

„C" típusú hálózati forgalom monitorozó eszköz műszaki specifikációja

- virtuális eszköz legyen,
- legalább 1x10 Gbit Ethernet monitor port támogatás (legalább 0,7 Mpps monitor port teljesítmény, legalább 0,7 Mpps eszköz teljesítmény; Flow cache: legalább 4M flow/monitor port.
- támogatott virtualizációs platform: VMware ESXi (8.x), Microsoft Hyper-V (2012 R2 vagy magasabb verzió), KVM (KVM 3.10.0, QEMU 1.5.3, libvirt 4.5.0, vagy magasabb verziók),
- hálózatforgalom monitorozás és IP flow generálás képesség,
- Netflow/IPFIX statisztika készítése, L2-L4 (protokollok legalább VLAN, QinQ, MPLS, GRE, OTV, ESP, VxLAN, SRT, RTT, jitter stb.) L7 (legalább hostnevek,

URL, böngésző információk HTTP/S protokolloknak, DNS, DHCP, SQL, SMTP, Samba/CIFS, VOIP, SSL/TSL, CoAP, IEC104)

- Geolokáció és Autonomous System megfeleltetés.

„D" típusú hálózati forgalom monitorozó eszköz műszaki specifikációja

- virtuális eszköz legyen,
- 1x1 Gbit Ethernet monitor port támogatás (legalább 0,3 Mpps monitor port teljesítmény, legalább 0,3 Mpps eszköz teljesítmény; Flow cache: 0,5M flow/monitor port),
- támogatott virtualizációs platform: VMware ESXi (8.x), Microsoft Hyper-V (2012 R2 vagy magasabb verzió), KVM (KVM 3.10.0, QEMU 1.5.3, libvirt 4.5.0 vagy magasabb verziók).
- hálózatforgalom monitorozás és IP flow generálás képesség,
- Netflow/IPFIX statisztika készítése, L2-L4 (protokollok legalább VLAN, MPLS, GRE, OTV, ESP, VxLAN, SRT, RTT, jitter stb.) L7 (legalább hostnevek, URL, böngésző információk HTTP/S protokolloknak, DNS, DHCP, SQL, SMTP, Samba/CIFS, VOIP, SSL/TSL, CoAP, IEC104),
- Geolokáció és Autonomous System megfeleltetés.

Anomália detektációs modul műszaki specifikációja

- NetFlow v5/v9, IPFIX, NetStream, jFlow, cflowd stb. belső flow adatforrás feldolgozó képesség,
- Threat Intelligence (reputációs adatbázisok), whois, IP tools, weblinks – külső adatforrás feldolgozó képesség,
- anomália detekciós képesség: gépi tanulás, „adaptive baselining", viselkedés alapú analitika, heurisztika. MITRE v15 megfeleltetés. Beépített forensics/triage eventlog, kapcsolatok, packet és szignatúra,
- legalább 20.000 flow/sec feldolgozó képesség, egyszerre legalább 20 adatforrásból,
- riportolás és riasztás: e-mail, PDF/CSV, syslog, SNMP, packet capture trigger, script trigger,
- SIEM támogatás: CEF (syslog), SNMP trap,

- esemény vizualizációs képességek: esemény analitika, „timeline", „evidence" nézet, interaktív nézetek,
- integrációs képességek: LDAP/AD, FortiGate, Checkpoint, Veeam

Hálózati forgalom rögzítő és protokollelemző szoftvermodul műszaki specifikációja

- Hálózati forgalom rögzítés képesség – PCAP formátumban,
- 1, 10, 40, 100 Gbit monitor port támogatás,
- legalább 2 Probe eszköz egyidejű támogatása,
- REST API, integrációs lehetőség biztosítása,
- Forgalom rögzítés szűrés alapján: legalább IP cím, CIDR, MAC cím, protokoll, port, VLAN címke, MPLS,
- rögzített PCAP fájlok analízise; támogatott protokollok: legalább ARP, CoAP, DHCP, DNS, FTP, GOOSE, HTTP, ICMP, IEC104, IMAP, IMF, IP, MMS, MQTT, NTP, POP, SIP, SLAAC, SMB, SMTP, SSL, TCP.

Implementációs szolgáltatások – feladatok listája

- Collector deployment és alapkonfiguráció,
- Probe-ok üzembehelyezései és alapkonfigurációi,
- Flowmon Anomaly Detection System alapkonfigurációhoz információgyűjtés és konzultáció,
- szerverek és szolgáltatások "leltárja", szolgáltatás-térkép,
- szerverek és szolgáltatások objektum leképezései,
- Datafeed-ek, perspective-ek, filter-ek konfigurációi,
- HANGOLÁS: a keletkező nagy számú – többségében false-positive – riasztás Vevővel történő közös áttekintése és minimalizálása legfeljebb napi 50 db riasztási eseményre.
- automatikus riasztások alert-ek kialakítása,
- igény szerinti automatikus riportok definiálása.

Gyártói támogatás

A rendszer valamennyi hardver és szoftver elemére a gyártói terméktámogatást (jótállást) 3 évre (36 hónapra) kér a Vevő. A gyártói support típusának olyan szintűnek kell lennie, hogy hardveres eszközhiba esetén legkésőbb a következő munkanapra cserealkatrészt kell, hogy biztosítson.

Ezenfelül a gyártónak biztosítani kell:

- az 5x8 gyártói telefonos vagy e-mailes támogatást, távoli SSH bejelentkezéssel,
- a gyártói hibajavítások elérését,
- AI- és fő szoftver verziók rendszeres frissítését és azokhoz való hozzáférhetőséget.

Valamennyi gyártói jótállásnak és előfizetésnek ugyanarra a kezdő és lejárati dátumra kell esnie.