Příloha č. 2 výzvy k podání nabídek – TECHNICKÉ PODMÍNKY

Popis výchozího stavu

Jihomoravský kraj pro naplnění některých požadavků plynoucích ze zákona o kybernetické bezpečnosti a související vyhlášky o kybernetické bezpečnosti provozuje bezpečnostní dohledové centrum. Od roku 2017 byly vybrané příspěvkové organizace postupně připojeny do bezpečnostního dohledového centra, které provozuje oddělení Kybernetické operační centrum odboru kancelář ředitele Krajského úřadu Jihomoravského kraje (dále jen „KOC“). KOC zajišťuje pro připojené příspěvkové organizace Jihomoravského kraje služby bezpečnostního dohledového centra. V síti každé připojené příspěvkové organizace (dále jen „PO“) je integrován server pro sběr a odesílání logů z infrastruktury. Logy jsou přes VPN tunel zasílány do KOC k vyhodnocení.

V tabulce 1 je uveden seznam PO, pro které Zadavatel požaduje plnění

KÓD	**Název**	**Adresa**
JMK	Krajský úřad Jihomoravského kraje	Žerotínovo náměstí 449/3, 602 00 Brno
KOC	Kybernetické operační centrum	Žerotínovo náměstí 449/3, 602 00 Brno
ISSA	Integrovaná střední škola automobilní Brno, příspěvková organizace	Křížíkova 106/15, 612 00 Brno
NEMBV	Nemocnice Břeclav, příspěvková organizace	U Nemocnice 3066/1, 690 74 Břeclav
NEMHO	Nemocnice TGM Hodonín, příspěvková organizace	Purkyňova 11, 695 26 Hodonín
NEMHU	Nemocnice Hustopeče, příspěvková organizace	Brněnská 716/41, 693 01 Hustopeče
NEMIV	Nemocnice Ivančice, příspěvková organizace	Široká 401/16, 664 91 Ivančice
NEMKY	Nemocnice Kyjov, příspěvková organizace	Strážovská 1247/22, 697 01 Kyjov
NEMLE	Nemocnice Letovice, příspěvková organizace	Pod Klášterem 55/17, 679 61 Letovice
NEMTI	Nemocnice Tišnov, příspěvková organizace	Purkyňova 279, 666 01 Tišnov
NEMVY	Nemocnice Vyškov, příspěvková organizace	Purkyňova 235/36, 682 01 Vyškov
NEMZN	Nemocnice Znojmo, příspěvková organizace	MUDr. Jana Janského 2675/11, 669 02 Znojmo
SSIPF	Střední škola informatiky, poštovnictví a finančnictví Brno, příspěvková organizace	Čichnova 982/23, 624 00 Brno
SSTE	Střední škola technická a ekonomická Brno, Olomoucká, příspěvková organizace	Olomoucká 1140/61, 627 00 Brno
SUS	Správa a údržba silnic JMK, příspěvková organizace	Ořechovská 541/35, 619 00 Brno
VIDA	Moravian Science Centre Brno, příspěvková organizace	Křížkovského 554/12, 603 00 Brno
ZZS	Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace	Kamenice 798/1d, 625 00 Brno

Tabulka 1 – Seznam organizací

Specifikace poptávaných služeb

Pro režim aktivního dohledu (pracovní dny 8:00 – 17:00) zajistit minimálně jednoho pracovníka na úrovni L1. Ten nebo ti budou přihlášeni do TRIAGE v SIEM a budou provádět aktivní vyhodnocování přicházejících alertů z prostředí. Při monitoringu postupují dle níže uvedeného schématu, kdy může využívat pro svoji práci komunikace v rámci KOC L1, L2, případně komunikovat s IT provozem zákazníků pro doplnění informací.

Při zpracovávání alertů v triage pracovníci postupují systematicky od nejvyšší priority. Pozice L1 postupují dle runbooků, pokud nejsou schopni bezpečnostní událost jednoznačně vyhodnotit a uzavřít nebo pokud jim chybí na daný výskyt runbook, předají tuto událost k řešení vyšší vrstvě L2.

Triage je na konci každého pracovního dne „vyčištěna“. Pokud do poloviny pracovního dne nejsou v polovině, žádají o podporu L2.

Pracovníci L2 se věnují vyšetřování bezpečnostních událostí, které obdrželi od vrstvy L1. Pokud od L1 vyvstane požadavek na úpravu runbooku nebo definování nového, zpracují jej. Sledují trendy v kyberbezpečnosti a aktuální hrozby, které by mohly zákazníky ohrožovat o těchto nálezech informují pravidelně v rámci statusů, v případě kritických nálezů notifikace probíhá bezodkladně pomocí vhodného komunikačního kanálu (tiketing, email, tel. hovor). Obsahem hlášení (ticketů) je návrh mitigačních nebo procesních opatření s ohledem na odstranění nebo minimalizaci dopadů nálezu na požadovanou hladinu bezpečnosti v prostředí. Součástí jejich práce je také definice nových podnětů na pravidla v SIEM a bezpečnostní monitoring, tedy definování slepých detekčních míst.

Specifické činnosti pro L1

Provádí pravidelný dohled v rámci specifikovaného rozsahu. Je prvním pracovníkem, který zpracovává detekované bezpečnostní události v rámci služby triage v technologii SIEM, zakládá z nich v případě potřeby tikety, případně tyto detekce předává k řešení vrstvě L2 nebo zákazníkovi. Provádí zejména tyto konkrétní činnosti:

- sleduje triage v nástroji SIEM,
- sleduje online bezpečnostně relevantní zdroje, aby identifikovali neobvyklou činnost a potenciální hrozby v prostředí,
- provádí základní analýzu detekovaných událostí a incidentů, aby určili jejich vážnost a potenciální dopad na bezpečnostní postavení organizace,
- pokud je incident komplexnější nebo vyžaduje rozsáhlejší analýzu, vývoj postupu nového řešení nebo reakci, L1 takovou události eskaluje na vyšší úrovně v rámci KOC
- součástí práce L1 je dokumentace všech detekovaných true positive nálezů (zakládat tikety) a opatření přijatých k jejich řešení,
- zodpovídá za sledování celkového bezpečnostního stavu organizace a bezpečnostních nástrojů (CENTREON) závažné bezpečnostní události eskaluje výš,
- spolupracuje s dalšími členy týmu KOC, a dodavatele.

Specifické činnosti pro L2

Zpracovává podněty předané z vrstvy L1, provádí hunting v rámci dat zákazníka, navrhuje nový kontent do SIEM, předává podněty na rozvoj. Provádí zejména tyto konkrétní činnosti:

- provádí podrobnější analýzy detekcí, hrozeb a incidentů, které byly eskalovány z úrovně L1. To zahrnuje detailní zkoumání vzorů chování, detekce pokročilých hrozeb a zjišťování potenciálního dopadu na organizaci,
- má za úkol komunikovat s úrovní L1 a vedením KOC

- identifikuje nové nebo existující zranitelnosti a provádějí jejich analýzu se zaměřením na to, jak ohrožují nebo mohou ohrožovat bezpečnost prostředí, aby určil, jak jsou tyto zranitelnosti pro organizaci kritické.
- je zapojen do řízení a koordinace komplexnějších bezpečnostních incidentů, což zahrnuje spolupráci s dodavatelem technické podpory a s pracovníky IT provozu připojených PO,
- je zapojen do vytváření a aktualizace bezpečnostních pravidel a politik, které pomáhají chránit organizaci před hrozbami,
- pracuje s různými bezpečnostními nástroji, včetně SIEM systémů, forenzních nástrojů a dalších technologií, které pomáhají v detekci a analýze hrozeb,
- odpovídá za zlepšování procesů a postupů KOC, aby byla reakce na incidenty efektivnější a rychlejší, dává podněty pro zákazníky na případné zlepšení procesů interních, pokud je to vhodné,
- provádí forenzní analýzu v případě komplexních incidentů, která zahrnuje sběr a analýzu digitálních důkazů a rekonstrukci událostí.