Funkčné a nefunkčné požiadavky na nástroj bezpečnostného monitoringu určený na detekciu a reakciu na koncových bodoch

Zoznam definícií a skratiek

EDR/XDR	Nástroj na detekciu a reakciu na koncových bodoch (Endpoint Detection and Response) alebo aj nástroj pre rozšírenú detekciu a reakciu (Extended Detection and Response)
DNS	Uvedené ako protokol pri sieťovej komunikácii
SIEM	Security Incident and Event Management
SOAR	Security Orchestration, Automation and Response
API	Rozhranie pre programovanie aplikácií (Application Programming Interface)
AI	Umelá inteligencia
IoC	Indikátor kompromitácie
SDK	Software Development Kit
VPN	Virtual Private Network
MS	Microsoft
Microsoft SCCM	Microsoft System Center Configuration Manager
Koncový bod	Počítač, fyzický server, virtuálny server
SOC	Bezpečnostné dohľadové centrum (Security Operation Center)
OVM	Orgán verejnej moci
RBAC	Riadenie prístupu na základe rolí (Role Based Access Control)
WMI	Windows Management Instrumentation
GPO	Skupinová politika/y (Group Policy Object)
DHCP	Dynamic Host Configuration Protocol
PAC	Proxy automatická konfigurácia (Proxy auto-config)
WPAD	Automatické vyhľadanie/zistenie umiestenia proxy servera (Web proxy audo-discovery)
URL	Uniform Resource Locator

Všeobecné požiadavky na riešenie

1. Riešenie musí:
    a. Zabezpečiť pokrytie koncových bodov v prostredí rôznych orgánov verejnej moci (OVM) s centrálnym vyústením do bezpečnostného dohľadového centra (SOC).
    b. pozostávať z jednotného používateľského prostredia, v ktorom:
        i. jednotlivé OVM majú prístup iba ku svojím vlastným dátam, aktívam a alertom, ktoré zbiera, generuje alebo sprístupňuje toto riešenie;
        ii. analytici SOC majú prostredníctvom prihlásenia sa do jednej centrálnej manažment konzoly prístup ku všetkým dátam, aktívam, alertom a zraniteľnostiam, ktoré sú zbierané, generované alebo sprístupňované zo všetkých monitorovaných OVM, a to pre každé OVM jednotlivo a zároveň pre všetky spoločne;

iii. analytici SOC majú možnosť vo všetkých moduloch dodaného riešenia prispôsobiť/nastaviť politiky, pravidlá a procesy dodaného riešenia pomocou jednej centrálnej manažment konzoly alebo API rozhrania, a to pre každé OVM jednotlivo a zároveň pre všetky spoločne.

c. Umožňovať oddelenie dát jednotlivých OVM minimálne na logickej úrovni (RBAC). Oddelenie dát jednotlivých OVM na fyzickej úrovni sa nevyžaduje.
d. Umožňovať identifikáciu zariadenia pre možnosť rozlíšenia zákazníka, napr. formou tagov.
e. Poskytovať retenciu údajov z agentov nasadených na koncových bodoch, ktoré sú uložené v centrálnom úložisku, po dobu minimálne 30 dní. Údajmi sa rozumejú všetky telemetrické dáta alebo nespracované (tzv. raw) udalosti (spustenie procesu, príkazu alebo inej aktivity na koncovom bode), ktoré riešenie z koncového bodu kontinuálne získava.
f. Poskytovať možnosť dodatočne rozšíriť retenciu údajov (samotné rozšírenie retencie nie je predmetom verejného obstarávania, čiže uvedená aktivita nebude realizovaná úspešným uchádzačom v rámci tohto verejného obstarávania a nevstupuje do ceny).
g. Zabezpečiť, aby všetky požadované funkcionality pre nástroj definované v tomto dokumente boli zabezpečené na koncovom bode jedným agentom a boli dostupné na všetkých podporovaných operačných systémoch koncových bodov, ak sú relevantné pre daný operačný systém.
h. Prevádzka centrálnej manažment konzoly musí byť prevádzkovaná v cloudovom prostredí výrobcu.

Funkčné požiadavky na riešenie

1. Integrácia s inými bezpečnostnými nástrojmi a požiadavky na kompatibilitu

1.1. Podpora integrácie s existujúcimi bezpečnostnými nástrojmi (napr. pomocou API):
- SIEM (minimálne s riešením IBM);
- SOAR (minimálne s riešením Fortinet značky FortiSOAR).

1.2. Systém podporuje konektivitu pre izolované prostredia pomocou nastroja proxy a to minimálne v aspoň jednej z nasledujúcich možností:
- Ručné zadanie globálnej proxy URL za pomoci GPO alebo ako manuálna konfigurácia;
- Ručné zadanie súboru PAC prostredníctvom GPO alebo ako manuálna konfigurácia;
- WPAD nakonfigurovaný na automatickú detekciu súboru PAC cez DHCP alebo DNS;
- Lokálnej alebo cloudovej proxy.

1.3. Agent musí podporovať možnosť inštalácie bez požiadavky na reštart koncového bodu alebo nutnosť reštartu je minimalizovaná.

1.4. Agent vyžaduje použitie protokolu TLS 1.2 a vyššiu.

1.5. Agent je schopný využívať interný DNS pre zistenie URL cloud management konzoly.

1.6. Agent nesmie vyžadovať žiadne firewall pravidlá pre komunikáciu smerom z internetu. Komunikácia je vždy naviazaná smerom od agenta do cloudu.
1.7. Všetky dáta v komunikácii medzi agentom a centrálnou manažment konzolousú šifrované.
1.8. Dáta sú uložené na šifrovaných úložiskách.
1.9. Podpora štandardných dátových formátov a protokolov pre výmenu informácií o hrozbách a údajov o udalostiach z koncových bodov, minimálne s formátmi STIX, TAXII alebo API.
1.10. Otvorené, štandardizované a zdokumentované API a SDK na umožnenie vlastných integrácií, integrácií s nástrojmi tretích strán a automatizácie bezpečnostných pracovných postupov. API musí podporovať minimálne Python verziu 3 alebo vyššiu.
1.11. Natívna podpora integrácie s MS Windows Active Directory, ktorá umožňuje synchronizáciu užívateľských účtov, účtov zariadení a bezpečnostných skupín (Pozn.: riešenie musí umožňovať integráciu viacerých MS Windows Active Directory vzhľadom na monitoring viacerých organizácií).
1.12. Natívna podpora integrácie s Kubernetes cluster.
1.13. Natívna podpora integrácie s ďalšími zdrojmi logov a technológiami:
- Nástroj podporuje integrovanie MISP platformy za účelom obohacovania obsahu o ďalšie informácie o hrozbách (Threat Intelligence tretích strán) a ich pravidelnú aktualizáciu.
- Nástroj overuje hodnotu hash vstavanou integráciou na službu VirusTotal, alebo ekvivalent (vstavaná súčasť funkcionality bezpečnostného nástroja).

2. Schopnosti antivírovej ochrany a detekcie na úrovni koncového bodu

2.1. Súčasťou poskytovaného produktu sú aj aktívne funkcie antivírovej ochrany koncového bodu, resp. Next-Generation Antivirus (NGAV).
2.2. Systém musí používať framework MITRE ATT&CK pre pomenúvanie detekčných pravidiel.
2.3. Systém musí podporovať klasifikáciu detekčných pravidiel a alertov podľa kritikalít (stredné, vysoké, kritické, resp. ekvivalent) a zároveň je možné zvoliť kritikalitu pri vlastných pravidlách.
2.4. Systém musí umožňovať tvorbu vlastných detekčných pravidiel.
2.5. Vlastné detekčné pravidlá musí byť možné kategorizovať podľa frameworku MITRE ATT&CK.
2.6. Vlastné detekčné pravidlá musia mať možnosť využívať vstavané automatizované reakcie na incidenty a musia mať možnosť využiť minimálne funkcie tzv. Device Isolation, Process blocking.
2.7. Zaznamenávanie telemetrie prichádzajúcej a odchádzajúcej sieťovej komunikácie v rámci každej koncovej stanice, kde je nainštalovaný agent.
2.8. Systém musí podporovať kontrolu a analýzu rôznych sieťových protokolov, v minimálnom rozsahu HTTP/HTTPS alebo DNS.
2.9. Identifikácia škodlivého kódu na základe známych signatúr, behaviorálnej analýzy správania a strojového učenia, resp. AI. (musí spĺňať všetky uvedené možnosti).
2.10. Identifikácia zmien v konfigurácii systémových súborov.

2.11. Monitoring procesov spustených na koncovom bode (spustenie, ukončenie, narušenie integrity, prístup do pamäte, reťazenie procesov).
2.12. Identifikácia pohybu škodlivého kódu (tzv. malware spreading) v sieti – zdroj, cieľ v rámci koncových bodov pokrytých agentom.
2.13. Ochrana koncového bodu proti malware, ransomware a fileless útokom.
2.14. Monitorovanie registrov Windows zariadení, Windows Events súborov, súborových operácií, procesov OS a aplikácií.
2.15. Monitorovanie spúšťania skriptov a ochrana pred vkladaním škodlivých kódov na monitorovanom zariadení.
2.16. Monitorovanie pripájaných zariadení cez rozhranie USB, čítačku SD kariet alebo Bluetooth.
2.17. Využívanie dostupných administrátorských nástrojov – cmd, PowerShell alebo BITS.
2.18. Plánovanie spúšťania úloh agenta na koncovom bode – minimálne možnosti nastavenia času spustenia úlohy, druhu úloh a ich opakovania.
2.19. Monitorovanie WMI aktivity a to v minimálnom rozsahu tried WmiEventConsumer.
2.20. Logovanie a monitorovanie manipulácie so súbormi na súborovom systéme a to v minimálnom rozsahu akcií: vytvorenie súboru, otvorenie súboru, zmazanie súboru, modifikácia súboru, premenovanie súboru.
2.21. Monitorovanie a detekcia aktivity plánovaných systémových úloh (v rozsahu minimálne vytvorenie, modifikácia a zmazanie plánovanej úlohy).
2.22. Zaznamenáva logy o hash hodnotách v minimálnom rozsahu aspoň jeden štandardný algoritmus (napr. MD5, SHA256, SHA1) pre súbory a procesy spustené na systéme.
2.23. Riešenie monitoruje pipe aktivitu/udalosti na koncovom bode a to v rozsahu pripojenia k pipe a vytvorenia pipe.
2.24. Monitorovanie PowerShell aktivity na koncovom bode v plnom rozsahu spusteného príkazu.
2.25. Monitorovanie aktivity ovládačov, inštalácia ovládačov, zmena ovládačov, načítanie alebo odoberanie ovládačov aj z jadra systému.

3. Kapability pre Threat Hunting

3.1. Možnosť prehľadávať údaje z monitorovaných koncových bodov v celom rozsahu logovaných údajov (tzv. Threat Hunting).
3.2. Možnosť prehľadávať a filtrovať historické/zalogované dáta (zbierané dáta) pomocou vyhľadávacieho jazyka nástroja v celom rozsahu v súlade s požadovanou minimálnou retenciou.
3.3. Možnosť spúšťať vyhľadávanie podľa vlastného dopytu (tzv. Threat Hunting search/request) vrátane možnosti plánovania týchto dopytov pomocou vlastných pravidiel.
3.4. Možnosť na všetkých koncových bodoch definovať vlastné prehľadávanie IoC, ktoré sú importované manuálne alebo cez TAXII, STIX, CSV alebo MISP.

4. Reakcia na kybernetické bezpečnostné incidenty

4.1. Automatizovaný containment kompromitovaného koncového bodu na základe nastaviteľných pravidiel a to ako pre defaultné, tak aj pre vlastné pravidlá.
4.2. Funkcia vzdialeného prístupu ku koncovému bodu v reálnom čase podľa rozdelenia užívateľov a zariadení do rôznych užívateľských skupín alebo tzv. device tags, ktorá podporuje možnosť:
   a) vypnutia koncového bodu;
   b) používať kapability selektívne, minimálne izolovať alebo ukončiť vybrané programy/procesy, ktoré sú spustené na koncovom bode (napr. pomocou vzdialenej konzoly (remote shell);
   c) zobraziť na obrazovke koncového bodu tzv. disclaimer informácie v rámci reakcií na kybernetické bezpečnostné incidenty (tzv. incident response akcie);
   d) spúšťanie vlastných skriptov (minimálne podpísaný powershell skript na vylistovanie procesov, vzdialené spúšťanie powershell skriptov);
   e) vymazať škodlivý kód;
   f) ukončenie a spustenie vybraného procesu;
   g) úplná sieťová izolácia pracovnej stanice pri zachovaní komunikácie systému s agentom na koncovom bode;
   h) úplná sieťová izolácia pracovnej stanice so zachovaním možnosti komunikácie s používateľom koncového bodu, minimálne MS Outlook alebo MS Teams alebo prostredníctvom obstaraváneho riešenia;
   i) vzdialenú správu, kontrolu zastavenia služby a jej odinštalovanie;
   j) ukončenie užívateľských sessions na koncovom bode;
   k) zapnutie a vypnutie firewallu na koncovom bode;
   l) modifikácia a odstraňovanie obsahu registrov;
   m) inštalovanie a odinštalovanie aplikácií a záplat;
   n) reštartovanie, vypnutie a uspatie (hybernácia) koncového bodu.
4.3. Whitelisting defaultných pravidiel spôsobom, že je možné použiť minimálne dva parametre pre whitelisting (napríklad zdrojový hostname a cesta k procesu).
4.4. Možnosť hromadného blokovania pomocou hash.
4.5. Podpora strojového učenia (ML/AI).
4.6. Automatizovaná analýza hlavných príčin akéhokoľvek upozornenia, vrátane sieťových upozornení, ak sú dostupné údaje o koncovom bode.
4.7. Vizualizácia reťazcov vykonaných operácií/zmien (execution) vedúcich k varovaniu.
4.8. Možnosť zobrazenia všetkých akcií a upozornení na časovej osi.
4.9. Vygenerovaný alert obsahuje opis potenciálneho dopadu atertu/incidentu (napr. ransomware, data exfiltration, lateral movement).
4.10. Prednastavené (defaultne) generovanie jedného sumárneho reportu z celého priebehu incidentu.

5. Forenzná a malware analýza

5.1. Možnosť zberu forenzných dôkazov z koncových bodov, a to v minimálnom rozsahu: História prehliadača, AmCache a ShimCache, Netstat, Zoznam objektov po spustení, Zoznam naplánovaných úloh. Stiahnutie musí byť možné vykonať vzdialene. Forenzný team má možnosť exekúcie scriptov.
5.2. Zaznamenávanie a zber forenzných údajov počas celého priebehu incidentu.

5.3. Riešenie poskytuje Sandbox prostredie s možnosťou manuálneho alebo automatizovaného nahrávania vzoriek a ich následnú analýzu.

6. Jednoduchosť nasadenia a správy, integrácie, agent:

6.1. Riešenie musí podporovať rýchly a jednoduchý proces nasadenia pomocou nástroja Microsoft SCCM alebo ekvivalentu, vrátane inštalácie agenta na koncovom bode a jeho úvodnej konfigurácie.

6.2. Riešenie musí podporovať vzdialené odobranie agenta z koncového bodu (odinštalovanie).

6.3. Centralizovaná management konzola, ktorá poskytuje prehľad o celom prostredí koncových bodov. Prostredníctvom tejto konzoly je možná efektívna správa politík pre všetky pripojené koncové body spoločne a zároveň podľa rozdelenia užívateľov a zariadení do užívateľských skupín alebo za pomoci tzv. tagu zariadenia či užívateľa. Centralizovaná management konzola umožňuje správu celého prostredia daných tenantov jednotlivo aj spoločne.

6.4. Priamočiare a intuitívne rozhranie, ktoré bezpečnostným tímom umožňuje:

a) rýchlo rozumieť a reagovať na upozornenia a incidenty;
b) prehľad o práve prebiehajúcich incidentoch;
c) namapovanie alertov do kategórií podľa frameworku MITRE ATT&CK.

6.5. Automatické aktualizácie a inovácie agenta zabezpečujúce, že koncové body a riadiaca infraštruktúra zostanú aktuálne a bezpečné, vrátane manažmentu aktualizácií koncových bodov.

6.6. Škálovateľnosť produktu v zmysle rozširovania počtu koncových bodov, ale aj rozširovanie monitorovaných subjektov ako samostatných tentantov prostredníctvom podpory architektúry popísanej v časti 1 písmeno b. a písmeno c. (tzv. multitenantná architekúra).

6.7. Podpora pre skriptovanie a automatizáciu rutinných úloh ako je nasadenie alebo odobranie agenta, konfigurácia politík a sledovanie stavu koncových bodov.

6.8. Odolnosť agenta voči tzv. tamperingu:

a) bežný užívateľ nebude môcť vypnúť, odinštalovať alebo poškodiť integritu agenta;
b) konfiguračný súbor agenta musí byť neprístupný bežnému užívateľovi.

6.9. Riešenie podporuje možnosť zabrániť zmenám konfigurácie agentov bez autorizácie administrátora, resp. bez administrátorského oprávnenia.

6.10. Agent musí byť schopný zaznamenávať metadáta o správaní koncových bodov, alerty a výsledky úloh aj pre také koncové body, ktoré sú dočasne bez prístupu do siete internet, ich uchovaním na koncovom bode až do ich odoslania do systému aspoň počas 14 dní alebo do naplnenia tzv. pamäte cache s kapacitou minimálne 50 MB.

6.11. Riešenie umožňuje automatické detegovanie a reportovanie aktuálneho stavu agenta koncového bodu – minimálne možnosť aktívne upozorňovať na: koncový bod bez inštalovaného agenta, neaktualizovaný alebo vypnutý agent.

6.12. Pravidelná aktualizácia definícií lokálneho agenta koncového bodu - vzorky vírusov, vektorov útoku, podozrivých IP adries a podobne.

6.13. Po aktivácii agenta je možné presúvanie licencie agenta medzi koncovými bodmi rovnakého typu (napr. pracovná stanica – pracovná stanica, windows server - windows server).

7. Vulnerability management:

7.1. Inštalovaný agent vykonáva sken koncového bodu v reálnom čase.

7.2. Riešenie poskytuje hodnotenie identifikovaných zraniteľností podľa:

a) Klasifikácie podľa štandardu CVE;

b) Klasifikácie podľa výrobcu a jeho threat intelligence.

7.3. Riešenie odporúča patchovanie zraniteľností, ktoré podľa CVE hodnotenia majú hodnotu „High“ a „Critical“.

7.4. Riešenie umožňuje zobraziť históriu možného zneužitia danej zraniteľnosti v rámci koncového bodu v jednej centrálnej manažment konzole.

7.5. Riešenie umožňuje automaticky detegovať, ktoré servery, domény a služby sú vystavené do internetu.

7.6. Riešenie umožňuje vytvárať vlastné dashboardy a reporty o zraniteľnostiach.

7.7. Riešenie umožňuje import dát zo skenerov zraniteľností tretích strán, minimálne Tenable Security Center (pôvodne Tenable.sc) a Tenable Nessus, ktorými už verejný obstarávateľ disponuje).

7.8. Riešenie umožňuje analytikom pracovať s korelovanými výsledkami zo skenov zraniteľností vykonaných agentom bezpečnostného nástroja a z importovaných výsledkov skenov zraniteľností tretích strán (minimálne v rozsahu definovanom v bode 7.7) v jednej centrálnej manažment konzole bezpečnostného nástroja alebo prostredníctvom dodatočného produktu toho istého výrobcu dodávaného ako súčasť predmetu zákazky, okrem prípadu, keď už takýmto produktom Nadobúdateľ disponuje, t. j. FortiSOAR.

8. Reporting:

8.1. Vytváranie podrobných bezpečnostných reportov s jasným vysvetlením stavu koncových bodov a vykonávaných akcií po úroveň štatistických údajov jednotlivých koncových bodov. Možnosť vytvárania vlastných reportov.

8.2. Integrácia (napr. pomocou API rozhrania) s analytickými nástrojmi a nástrojmi pre business intelligence umožňujúca hlbšiu analýzu a vizualizáciu údajov (napríklad PowerBI, Qlik Sense alebo ekvivalent).

8.3. Možnosť exportovania údajov o reportingu aspoň v jednom formáte z CSV, PDF alebo XML.

8.4. Auditovanie všetkých vykonaných akcií prihláseného užívateľa, vrátane live response akcií a možnosť exportovania auditných záznamov.

8.5. Podpora automatických oznámení v reálnom čase o vykonaných reakciách na kybernetické bezpečnostné incidenty.

Nefunkčné požiadavky na riešenie

9. Podporované operačné systémy alebo platformy, na ktorých je plánované nasadenie agenta:

9.1. Operačný systém MS Windows 7 a vyššie.
9.2. Operačný systém MS Windows Server 2008 R2 a vyššie.
9.3. Operačný systém MacOS od verzie MacOS 11.0.
9.4. Operačný systém Linux CentOS od verzie 7 (alebo Centos Stream), Debian od verzie 10, Ubuntu od verzie 14.04.
9.5. Operačný systém RedHat Enterprise Linux 6.4 a vyššie.
9.6. Platforma Kubernetes, Docker.
9.7. Architektúra minimálne x86 (32-bitová verzia) a x64 (64-bitová verzia).

10. Data

10.1. Údaje musia byť spracované, vyhodnocované a uložené v krajinách EÚ v zmysle všeobecného nariadenia na ochranu osobných údajov (GDPR).

11. Podpora a služby

11.1. Produkt, t. j. detekčné pravidlá a obsah (nie samotný softvér) je pravidelne aktualizovaný počas celej doby trvania licencie.
11.2. Nepretržitá 24/7 zákaznícka podpora v slovenskom, českom alebo anglickom jazyku prostredníctvom minimálne dvoch kanálov ako sú telefón, e-mail, chat alebo ticketovací systém.
11.3. Priamy prístup k databáze znalostí výrobcu, vrátane dokumentácie a osvedčených postupov a návodov na riešenie problémov.
11.4. Dostupnosť priebežných školení a certifikačných programov výrobcu dodávaného produktu podľa aktuálnej verzie produktu na zabezpečenie toho, aby mal bezpečnostný tím aktuálne informácie o produkte s najnovšími funkciami produktu a osvedčenými postupmi v rozsahu:
a) minimálne v dvoch termínoch ročne;
b) v minimálnom trvaní 3 dni (1 deň = 8 hodín, počítané po hodinách);
c) on-site v priestoroch objednávateľa;
d) maximálne pre 6 účastníkov školenia na jeden termín.
(nie je súčasťou obstarávaných služieb – nezapočítava sa do ceny zákazky).