PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené
ako otvorená cloudová služba s prvkami strojového učenia

Koncept SOC centra

Previazané s balíkom KPB2 – Návrh SOCaaS služby

Previazané s výstupom
V6 – Popis dashbordov, monitorovacieho a reportovacieho systému

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Úvod do problematiky SOC....4
Koncept operačného centra kybernetickej bezpečnosti....4
Zlepšená spolupráca (angl. improved colaboration)....5
Ľudia pracujúci v SOC centre....5
Tier 1 Bezpečnostný analytik – analytik výstrah (angl. alert analyst)....5
Tier 2 Bezpečnostný analytik – respondent na incidenty (angl. incident responder)....6
Tier 3 Bezpečnostný expert – lovec hrozieb (angl. threat hunter)....6
Bezpečnostný inžinier....6
SOC manažér – prevádzka a manažment (angl. operations and management)....6
CISO - šéf informačnej bezpečnosti (angl. chief information security officer) 6
Certifikácie....7
Základné procesy SOC centra....7
Klasifikácia udalostí a triedenie....7
Tiketový proces (angl. ticketing)....7
Prioritizácia a analýza....8
Náprava a obnova....8
Hodnotenie a audit....8
Nástroje....9
Prevencia vs. detekcia....9
Monitorovanie bezpečnosti siete (angl. Network Security Monitoring - NSM). .9
Prieskum aktív....9
Posudzovanie zraniteľností (angl. Vulnerability Assessment)....10
Monitorovanie správania (angl. Behavioral monitoring)....10
IDS....10
Endpoint Detection and Response EDR....11
Network Detection & Response NDR....11
eXtended Detection & Response XDR....12
SIEM....12
SOAR....12
Ostatné centrá a jednotky riešiace operatívu alebo bezpečnosť....13
SOC....13
NOC....13
CSIRT....13
Údaje o bezpečnosti siete....14
Typy bezpečnostných údajov....14
Výstražné údaje (angl. Alert data)....14
Logy koncových zariadení (angl. Host logs)....14
Relačné dáta (angl. Session data)....15

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Transakčné dáta (angl. Transaction data)....15
Úplné zachytávanie paketov (angl. Full packet capture)....15
Štatistické údaje (angl. Statistical data)....16
Logy koncových zariadení....16
Syslog....16
Server logs....16
Logovanie z medziľahlých sieťových zariadení....17
Proxy logs....17
SIEM....17
Firewally novej generácie (Next-Generation Firewalls, NGFW)....18
Informácie o sieťových tokoch a aplikáciách....19
NetFlow....19
Viditeľnosť a riadenie aplikácií (Application Visibility and Control)....20
Logy ako výstup z filtrovania špecifického obsahu (Content filter logs)....21
Vyhodnocovanie upozornení....21
Zdroje upozornení....21
Generovanie bezpečnostných výstrah....22
Prehľad vyhodnotenia bezpečnostných výstrah....22
Potreba vyhodnotenia výstrahy....22
Vyhodnocovanie bezpečnostných výstrah....23
Deterministická analýza a pravdepodobnostná analýza....24
Digitálna forenzná analýza....25
Digitálny forenzný proces....26
Typy dôkazov....27
Odporúčanie na zber dôkazov....27
Spracovateľský reťazec....28
Integrita a ochrana údajov....28
Priradenie útoku....29
The MITRE ATT&CK Framework....30
The Cyber Kill Chain....30
Diamantový model analýzy narušenia bezpečnosti....31
Prechod cez diamantový model....32
Diamantový Model a Cyber Kill Chain....32
Reakcia na incidenty....33
Politika, plán a postup reakcie na incidenty....34
Prvky politiky reakcie na incidenty....34
Prvky plánu reakcie na incidenty....34
Prvky postupu reakcie na incidenty....34
Zainteresované strany v procese reakcie na incidenty....34
Certifikácia modelu kybernetickej bezpečnosti....34

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

NIST Životný cyklus reakcie na incident.....35
Hardening na základe lekcií.....36
Zhromažďovanie a uchovávanie údajov o incidentoch.....36
Požiadavky na podávanie správ a zdieľanie informácií.....37
Zoznam použitej literatúry.....37
Príloha: Zoznam nástrojov.....39

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Úvod do problematiky SOC

Koncept operačného centra kybernetickej bezpečnosti

Security Operations Centre (SOC) je centralizovaná jednotka, ktorá sa zaoberá bezpečnosťou a zahŕňa ľudí, procesy a technológie, ktorých hlavnou úlohou je nepretržité monitorovanie, prevencia, detekcia, vyšetrovanie (angl. investigation) a reagovanie na kybernetické hrozby. SOC tímy sú zodpovedné za monitorovanie a ochranu aktív (angl. assets) organizácie a implementujú celkovú stratégiu kybernetickej bezpečnosti organizácie.

Prevencia a detekcia poskytujú výhodu, pretože predchádzanie útokom je vždy efektívnejšie, ako reakcia na útoky. Pomocou monitorovania dokážu SOC tímy detegovať podozrivé aktivity a eliminovať ich ešte pred tým, než dokážu spôsobiť škody. Pri tomto kroku sa tiež získava čo najviac informácií potrebných na ďalšie vyšetrovanie. Počas vyšetrovania sa zisťuje povaha hrozby a rozsah v akom sa jej podarilo preniknúť do infraštruktúry. Takisto sa hľadajú indikátory a ohrozené oblasti skôr ako budú zneužité. Posledným krokom je odpoveď, respektíve reakcia na incident. Hneď ako bol incident potvrdený, SOC tím vykonáva všetky potrebné akcie ako sú napríklad izolácia koncových zariadení, ukončenie škodlivých procesov, zmazanie súborov a podobne. Po skončení incidentu sa SOC tím snaží obnoviť systémy a dáta, ktoré boli stratené alebo ohrozené. Ak bol tento krok úspešný, sieť by sa mala nachádzať v stave, v akom bola pred incidentom. Pri obnove systémov je potrebné prihliadať na hlavné komponenty obnovy systémov po krízovej udalosti (angl. disaster recovery) a plánovania kontinuity podnikania (angl. business continuity planning). Jedným z nich je cieľ doby zotavenia (angl. recovery time objective - RTO), ktorý predstavuje maximálny tolerovaný interval výpadku daného zariadenia, systému, siete, alebo aplikácie, ktorý môže nastať po chybe, alebo kritickej udalosti.

SOC prináša množstvo benefitov pre organizácie a ich bezpečnosť. Tu spomenieme niekoľko z nich.

Centralizované znalosti (anglicky centralized knowledge)

Pri veľkom množstve útokov je veľká šanca, že budú niektoré z nich prehliadnuté. SOC prináša lepšie vybavenie pre kybernetických odborníkov, ktoré im zabezpečí kompletný prehľad o celej sieti a potenciálnych zraniteľnostiach. Takisto poskytuje centrálne

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

uchovávanie a zdieľanie informácií, vďaka ktorému disponuje celý tím rovnakými informáciami, čo pomáha efektívnejšej identifikácii hrozieb a ich zneškodneniu.

Kontrola nákladov(angl. cost control)

Vo všeobecnosti sú SOC efektívnejšie vzhľadom na náklady pre organizácie. Či už ide o umiestenie tímu na jednom mieste, v jednej budove alebo efektívnejšie predchádzanie útokom a škodám, všetko z toho dokáže šetriť financie organizácie.

Zlepšená spolupráca (angl. improved colaboration)

Zo združenia SOC tímu na jednom mieste profituje aj spolupráca medzi členmi tímu, tým že sa vedia lepšie dohodnúť a deliť si prácu medzi sebou, čím sa zamedzuje duplicitným činnostiam. Tým, že je SOC centralizovaný na jednom mieste, sa zrýchľuje aj doba odozvy na hrozby, čím sa útočníkom naopak skracuje čas na prevedenie úspešného útoku.

Kvalifikovaná odbornosť(angl. skilled expertise)

SOC so sebou prináša odborníkov na kybernetickú bezpečnosť s rôznymi zručnosťami v tejto oblasti, ktoré môžu spolu kombinovať a používať pri vývoji riešení kybernetickej bezpečnosti. Poslednou z výhod, ktorú spomenieme je sofistikované monitorovanie siete, na ktoré SOC využíva najnovšie monitorovacie a detekčné nástroje, ktoré pomáhajú lepšie detegovať potenciálne slabé miesta v sieti a riešiť ich skôr ako sa stanú problémom.

Ľudia pracujúci v SOC centre

Pozície v SOC centre majú hierarchickú štruktúru, ktorá zodpovedá úrovni odbornosti pracovníkov. Túto štruktúru zobrazuje obrázok 1.1. Ľudia pracujúci v SOC centre sú rozdelení do troch stupňov - Tier 1 až Tier 3, ktoré dopĺňajú bezpečnostný inžinier, manažér SOC centra a CISO, ako líder celého centra.

Tier 1 Bezpečnostný analytik – analytik výstrah (angl. alert analyst)

Spravuje a konfiguruje monitorovacie nástroje, spúšťa skenovania zraniteľností a kontroluje reporty o zraniteľnostiach, kontroluje tiež najnovšie výstrahy a určuje ich

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

relevantnosť a naliehavosť, vytvára tikety pre výstrahy, ktoré signalizujú incident a vyžadujú kontrolu od analytikov úrovne Tier 2. Viac o tiketoch uvádzame v časti Tiketový proces (angl. ticketing) v kapitole 1.1.3 Základné procesy SOC centra.

Tier 2 Bezpečnostný analytik – respondent na incidenty (angl. incident responder)

Kontroluje tikety prijaté od Tier 1, využíva spravodajstvo o hrozbách (angl. threat intelligence) na identifikáciu ovplyvnených systémov a rozsahu útoku, kontroluje a zbiera dáta o aktívach systému pre ďalšie vyšetrovanie. Určuje a riadi nápravu a obnovu systémov.

Tier 3 Bezpečnostný expert – lovec hrozieb (angl. threat hunter)

Hodnotí údaje o aktívach a zraniteľnostiach, skúma spôsoby identifikácie skrytých hrozieb, ktoré sa mohli dostať do siete bez toho, aby ich niektorý detekčný systém zachytil, pomocou najnovších informácií o hrozbách, vykonáva penetračné testy s cieľom overiť odolnosť a identifikovať slabé miesta, ktoré treba opraviť, odporúča ako optimalizovať monitorovacie nástroje.

Bezpečnostný inžinier

Označovaný aj ako Bezpečnostný architekt uzatvára sekciu operatívnych pracovníkov SOC centra. Spravuje a navrhuje nástroje na monitorovanie a analýzu. Buduje bezpečnostnú architektúru a spolupracuje s vývojármi na zabezpečení tejto architektúry. Môže ísť o softvérového alebo hardvérového špecialistu, ktorý pri produkcii informačných systémov venuje náležitú pozornosť bezpečnostným aspektom. Zabezpečuje nástroje a riešenia, ktoré organizácii umožňujú efektívne reagovať na útoky. [3]

SOC manažér – prevádzka a manažment (angl. operations and management)

Dohliada na činnosť SOC tímu, prijíma, najíma a školí zamestnancov, riadi procesy, a kontroluje správy o incidentoch, meria metriky výkonu SOC a oznamuje hodnotu bezpečnostných operácií vedúcim spoločností.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

CISO - šéf informačnej bezpečnosti (angl. chief information security officer)

Definuje bezpečnostné operácie organizácie. Interaguje s vedením o otázkach zabezpečenia a úlohách súvisiacich s dodržiavaním predpisov. CISO poskytuje konečný pohľad na politiky, stratégie a postupy týkajúce sa kybernetickej bezpečnosti organizácie. Má tiež primárnu úlohu pri dodržiavaní predpisov, riadení rizík a implementácii politík na splnenie konkrétnych požiadaviek na bezpečnosť. [3]

Certifikácie

Stať sa relevantným pracovníkom SOC centra nám môžu pomôcť certifikácie, ktoré sú dostupné od rôznych organizácií. Tu uvádzame zopár príkladov:

- Cisco Certified CyberOps Associate
- CompTIA Cybersecurity Analyst Certification
- Information Security Certifications $(ISC)^2$
- Global Information Assurance Certification (GIAC)

Ďalšími odporúčanými zručnosťami sú napríklad programovanie v jazyku Python, či znalosť Linuxu.

Základné procesy SOC centra

V tejto časti stručne popíšeme základné kategórie procesov vykonávané analytikmi vyššie popísaných úrovní v SOC centre.

Klasifikácia udalostí a triedenie

Pre vyjadrenie skutočnej hodnoty zberu logov a dát sa v literatúre často objavuje výrok, že efektívny zber dáva analytikom možnosť nájsť "signál v šume". Kľúčové indikátory podozrivej udalosti sa môžu nachádzať napríklad v aktivite používateľa, či systémových udalostiach. Špecifické sekvencie a kombinácie týchto udalostí v špecifických vzoroch môžu signalizovať udalosť, ktorá si vyžaduje pozornosť. Bližšie jednotlivé monitorované udalosti popíšeme v časti 1.2.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Za kľúč k úspechu v tejto fáze sa považuje mať spôsob, ako rýchlo klasifikovať každú udalosť, aby sme mohli uprednostniť a eskalovať kritické udalosti, ktoré si vyžadujú dodatočné vyšetrovanie.

Tiketový proces (angl. ticketing)

Tikety sa používajú na sledovanie problémov súvisiacich s aktívami či (bezpečnostnými) udalosťami. Tiket je pracovná požiadavka vytvorená ako reakcia na situáciu, ktorá si vyžaduje ďalšie skúmanie. Keď z analyzovaných údajov o aktivitách a udalostiach, zväčša bezpečnostného charakteru, vznikne podozrenie na možný problém, je vytvorený takýto tiket, ktorý sa následne pridelí inému pracovníkovi, ktorý problém vyšetrí a vyrieši. [4]

Prioritizácia a analýza

Stanovenie priorít je kľúčom k úspechu v akejkoľvek oblasti, obzvlášť v oblasti kybernetickej bezpečnosti. Je potrebné sa zamerať na tie udalosti, ktoré by mohli mať najväčší vplyv na biznis operácie. Tu je potrebné vedieť, ktoré aktíva sú najkritickejšie a označiť ich ako kľúčové pre poskytovanie biznis procesov v organizácii (angl. bussiness-critical assets). Udržiavanie kontinuity podnikania organizácie (angl. business continuity) je najdôležitejšou zodpovednosťou SOC tímu.

Náprava a obnova

Čím rýchlejšie dokáže SOC tím odhaliť a reagovať na incident, tým je pravdepodobnejšie, že bude schopný obmedziť poškodenie a zabrániť podobnému útoku v budúcnosti. Pri tomto bode je potrebné vedieť robiť správne rozhodnutia, a zvážiť, či je väčší záujem o obnovu po incidente alebo o dôkladné vyšetrovanie kybernetického zločinu. A preto je veľmi dôležitá spolupráca a komunikácia s manažérskym tímom a dokumentácia potrebných informácií.

V niektorých prípadoch SOC tím prenecháva proces nápravy a obnovy iným IT oddeleniam. V takom prípade SOC analytik vytvorí tiket a/alebo žiadosť na riadenie zmeny (angl. change control request) a deleguje ju na zodpovedné osoby.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Hodnotenie a audit

Vždy je optimálne nájsť a opraviť slabé miesta skôr, ako ich zneužije útočník na získanie prístupu do danej siete.

Najlepším spôsobom, ako to urobiť, je vykonávať pravidelné hodnotenia zraniteľností (angl. vulnerability assessment) a podrobne preskúmať ich výsledky. Tieto hodnotenia identifikujú skôr technické nedostatky ako procedurálne, takže sa treba uistiť, že tím rieši aj medzery v procesoch SOC, ktoré by tím tiež mohli vystaviť riziku.

V procese riadenia informačnej bezpečnosti (angl. information risk management), ktorú manažuje osoba v roli CISO. Táto osoba nutnou súčasťou aj zavedený proces manažmentu rizík, kde už ide tak o informačné ako aj o operačné riziká identifikovaných aktív danej organizácie. Pokiaľ sa niektoré identifikované riziká týkajú aj ľudí, procesov alebo technológií SOC centra, môže byť osoba v roli manažéra SOC centra označená ako vlastník daných rizík a ďalej bude jej povinnosťou riešenie daných rizík podľa dohodnutých pravidiel a postupov v organizácii.

Nástroje

V tejto kapitole uvádzame základné delenie nástrojov využívaných analytikmi v SOC centre podľa účelu využitia. V každej kategórii existuje viacero dostupných riešení od rôznych výrobcov. Jednotlivé nástroje môžu byť komerčné, iné sú dostupné ako open-source riešenia. Pri každej kategórii bude ako príklad spomenutý konkrétny nástroj, poprípade aj open-source variant. Ich alternatívy a ďalšie možnosti budú uvedené v časti Príloha A Zoznam nástrojov.

Prevencia vs. detekcia

Pre obranu v kybernetickom priestore existuje viacero odlišných prístupov, pri hrubom delení sa však tieto prístupy delia do dvoch základných kategórií, a to prevenčné a detekčné. Pri prevenčnej stratégií kladie organizácia dôraz na takzvané opevnenie (angl. hardening). Pri detekčnej stratégii sa bezpečnostný tím venuje proaktívnej identifikácii a náprave hrozieb, ktoré narušili bezpečnosť organizácie. Prevenčný prístup je najčastejší, avšak v dnešnej dobe už nie je tak efektívny ako v minulosti, resp. nie je vhodné sa spoliehať

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

iba naň. Preto pridávanie detekčného prístupu do bezpečnostnej stratégie organizácie sa stáva čoraz viac potrebným k ochrane proti moderným kybernetickým hrozbám.

Monitorovanie bezpečnosti siete (angl. Network Security Monitoring - NSM)

Ide o automatizovaný proces, ktorý monitoruje zariadenia (koncové, sieťové) a prevádzku, či neobsahujú bezpečnostné zraniteľnosti (angl. vulnerabilities), hrozby alebo podozrivé aktivity. Organizácie ho môžu použiť na rýchle odhalenie a reakciu na porušenia kybernetickej bezpečnosti. Primárnym cieľom je poskytovať nepretržitú službu, ktorá kontroluje prostredie na prítomnosť podozrivých aktivít a hrozieb. Pracovníci potom môžu preskúmať nahlásené aktivity a prijať vhodné nápravné opatrenia. [5]

Prieskum aktív

Prvým krokom pri ochrane siete je poznať samotnú sieť a čo sa v nej nachádza. Je potrebné vedieť, aké systémy (laptopy, servery) v nej existujú a čo je na nich nainštalované (aplikácie, služby, aktívne porty, a iné). Spoľahlivý inventár aktív spolu s automatizovanou schopnosťou objavovať nové, je základom pre budovanie SOC. Na katedre KIS sa v minulosti testovali nástroje pre inventarizáciu aktív ako Lansweeper, SpiceWorks, a nástroje, ktoré poskytujú aj vykresľovanie topologických máp celej sieťovej infraštruktúry, ako sú Auvik a LibreNMS [6]–[8] .

Posudzovanie zraniteľností (angl. Vulnerability Assessment)

Zraniteľnosti predstavujú malé "praskliny", ktoré útočníci využívajú na infiltráciu do siete, zariadení, systémov, či aplikácií. Toto je často označované ako útočná plocha (angl. attack surface). Je preto nevyhnutné neustále kontrolovať a vyhodnocovať zraniteľnosti celej siete. Navyše to môžu vyžadovať rôzne regulácie, zákony a smernice. Ide napríklad o americké smernice ako PCI-DSS, či SOX. Na Slovensku sú to najmä Zákon 69/2018 Z. z. [9] , či Vyhláška NBÚ 362/2018 Z. z. [10] V tejto kategórii je možné použiť nástroje ako Nessus, Nexpose, OpenVAS (Greenbone), Owas-zap, nmap, a iné.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Monitorovanie správania (angl. Behavioral monitoring)

Efektívne monitorovanie kybernetickej bezpečnosti spočíva v správe výnimiek (angl. exception management) a sledovaní správania samotnej siete. Pod pojmom výnimky sa myslia napríklad porušovanie stanovených pravidiel, chybové hlásenia, veľké zmeny v aktivite siete, neočakávané reštarty a podobne. K tomuto je potrebné vytvoriť tzv. normu (angl. base line), ktorá predstavuje správanie siete v bežnej prevádzke. Vytvorenie takejto základnej línie správania systému a siete poskytuje potrebný podklad na zistenie anomálií, ktoré často signalizujú prítomnosť podozrivej aktivity v sieti. Pri jej tvorbe je dôležité skombinovať viaceré dostupné technológie monitorovania správania, aby sa poskytla úplná perspektíva. Aplikovanie korelačných pravidiel na tieto údaje navyše pomôže identifikovať a klasifikovať najnovšie riziká, ako aj zachytávať údaje na podporu hĺbkového forenzného vyšetrovania.

IDS

Detekcia narušenia v mieste vstupu do siete môže mať najväčší vplyv na zníženie rizika narušenia systémov, ktoré sa v organizácii nachádzajú a úniku dát. To je dôvod, prečo je Intrusion Detection Systems (IDS) považovaný za jeden z nevyhnutných nástrojov SOC na identifikáciu známych útokov a známej aktivity útočníka. IDS, na rozdiel od nástrojov na monitorovanie správania, ktoré sme popísali vyššie, funguje na základe znakov (angl. signatures) alebo pravidiel, ktoré hľadajú známe vzorce podozrivej sieťovej prevádzky a aktivity systému, ktoré by mohli signalizovať narušenie. Keď sa zistí v sieti táto aktivita alebo prevádzka, je potrebné o tom okamžite vedieť, aby sa mohlo začať vyšetrovanie s cieľom obmedziť akékoľvek škody. Ide o typ bezpečnostného softvéru, ktorý automaticky upozorní správcov, keď sa niekto alebo niečo pokúša ohroziť informačný systém škodlivými aktivitami, ako sú napríklad útoky DDOS alebo porušenie bezpečnostných zásad. IDS funguje tak, že monitoruje aktivitu systému prostredníctvom skúmania zraniteľností v systéme, integrity súborov a analýzy vzorov založených na už známych útokoch. Automaticky tiež monitoruje internet, aby vyhľadal najnovšie hrozby, ktoré by mohli viesť k budúcemu útoku. Nástroje sa ešte delia na HIDS a NIDS. Pri HIDS nájdu využitie nástroje ako Tripwire a OSSEC, za nástroje kategórie NIDS sa považujú Snort a Suricata.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Spoločným menovateľom ďalších troch skupín nástrojov je detekcia a reakcia (angl. detection and response). V texte nižšie uvedieme delenie a definície týchto nástrojov podľa zdroja [11] .

Endpoint Detection and Response EDR

Každé zariadenie pripojené k sieti predstavuje potenciálny vektor útoku pre hrozby z internetu a každé z týchto pripojení je potenciálnou bránou k údajom uloženým na danom zariadení. Vo všeobecnosti riešenia EDR zhromažďujú údaje z koncových bodov, používajú ich na identifikáciu potenciálnych hrozieb a poskytujú užitočné spôsoby, ako tieto potenciálne hrozby skúmať a reagovať na ne – moderné riešenia tento proces automatizujú s následným vytvorením reportu (angl. reporting). Príkladom EDR nástroja je SymantecEDR, SentinelOne, či Enterprise Inspector od spoločnosti Eseta OpenEDR, ktoré predstavuje open-source variantu.

Network Detection & Response NDR

Táto skupina nástrojov sa vyvinula z konvenčnej sieťovej bezpečnosti a je podoblasťou Network Traffic Analysis (NTA). Zabezpečuje plnú viditeľnosť známych a neznámych hrozieb prechádzajúcich sieťou. Riešenia zvyčajne poskytujú centralizovanú, strojovo založenú analýzu sieťovej prevádzky a riešenia odozvy, vrátane efektívnych pracovných tokov a automatizácie. Umiestnenie (angl. positioning) v sieti a pomoc strojového učenia poskytuje úplný prehľad a analýzu siete s cieľom identifikovať a eliminovať najmä neoprávneným pohybom útočníkov v sieti (angl. lateral movements). Nástrojmi tejto kategórie sú Stellar Cyber, Vectra NDR, Reveal(x) či Flowmon.

eXtended Detection & Response XDR

Táto skupina nástrojov rozširuje potenciál EDR systémov pomocou silnejšej umelej inteligencie, ako aj automatizačného prístupu. XDR nielenže integruje koncové body, ale poskytuje aj prehľad o podnikovej sieti tým, že ide nad rámec jedno vektorového bodového riešenia a zahŕňa sieťovú prevádzku medzi rôznymi zariadeniami, ako aj aplikácie na analýzu a hodnotenie.

Spolu s použitím SIEM môže byť táto korelácia a viditeľnosť ďalej posilnená. Výstražné údaje a udalosti môžu byť doplnené o ďalšie (meta) údaje, ktoré uľahčujú

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

zmiernenie - prevencia útokov(angl. mitigation) a nápravu - obnovenie systémov) po útokoch napr. malvérom (angl. remediation). Do tejto kategórie spadajú Cynet Auto XDR, Trend Micro, InsightIDR, či Cortex XDR.

SIEM

Zhromažďovanie a analýza systémových udalostí z celej siete poskytuje množstvo zdrojového materiálu, ktorý môže byť použitý na získanie informácií o podozrivých aktivitách. SIEM nástroje boli vyvinuté na základe predpokladu, že hľadaním určitých vzorcov činností a sekvencií udalostí môže SOC tím odhaliť kybernetický útok. Nástroje SIEM poskytujú základ pre budovanie SOC vďaka svojej schopnosti aplikovať pravidlá dynamickej korelácie proti množstvu rôznorodých údajov z logov, s cieľom nájsť najnovšie hrozby. SIEM popíšeme bližšie v podkapitole 1.2.2. Medzi zástupcov SIEM nástrojov patria napríklad Splunk, IBM Qradar alebo open-source SIEMonster a ELK stack riešenie.

SOAR

Platformy SOAR sú podobné SIEM v tom, že agregujú, korelujú a analyzujú výstrahy. Technológia SOAR navyše integruje spravodajstvo o hrozbách (angl. threat intelligence) a automatizuje pracovné postupy vyšetrovania incidentov a reakcie na ne, na základe príručiek vyvinutých bezpečnostným tímom. SOAR kladie dôraz na integračné nástroje a automatizáciu pracovných postupov SOC. Organizuje mnoho manuálnych procesov, ako je vyšetrovanie bezpečnostných výstrah, ktoré si vyžadujú zásah človeka len v prípade potreby. To umožňuje bezpečnostným pracovníkom riešiť naliehavejšie záležitosti a precízne vyšetrovanie a nápravu hrozieb.

Všetky vyššie uvedené nástroje neskôr v časti 1.3.1 zosumarizujeme z pohľadu možných zdrojov upozornení, a uvedieme v prehľadnej schéme nástrojov.

Ostatné centrá a jednotky riešiace operatívu alebo bezpečnosť

V oblasti, do ktorej táto práca spadá, sa často vyskytuje otázka rozdielnosti Security Operations Center (SOC), Network Operations Center (NOC), či Computer Security Incident Response Team (CSIRT). Hoci sa nájdu ciele, ktoré majú tieto centrá spoločné, ich rozdiely sú zrejmé. Rozdielnosti najlepšie zachytávajú nasledovné zdroje [12], [13] .

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

SOC

Operačné centrum kybernetickej bezpečnosti sa zameriava na všetky veci týkajúce sa bezpečnosti, t.j. detekciu hrozieb, monitorovanie, analýzu, reakciu na incidenty a forenznú analýzu. SOC zaisťuje dostupnosť a chráni sieť vytváraním a neustálym zlepšovaním bezpečnostnej architektúry a infraštruktúry chrániacej IT zdroje danej organizácie. SOC centrum chráni sieť pred hrozbami vytvorenými ľuďmi, ako sú malvér, vírusy a iné kybernetické útoky. SOC je centralizované miesto, kde tím pracuje 24/7/365 na ochrane IT zdrojov bezpečnosti.

NOC

Network Operations Center (NOC) sa zameriava na inštaláciu, údržbu, výkon a dostupnosť siete. Jeho úlohou je zabezpečiť, aby prístup k sieti, serverom, aplikáciám a údajom bol vždy dostupný, a aby spĺňali potreby organizácie a zmluvy o úrovni služieb (angl. Service Level Agreements - SLA). NOC sa primárne zameriava na poskytovanie služieb a aplikácií, prevádzku, údržbu a prevenciu/obnovu po prevádzkových katastrofách a iných neočakávaných udalostiach. Podobne ako SOC, aj NOC je centralizované miesto, ktoré poskytuje hore uvedené služby.

CSIRT

Tím reakcie na bezpečnostné incidenty počítača (angl. Computer Security Incident Response Team - CSIRT) je centralizovaná jednotka, ktorej cieľom je spravovať bezpečnostné incidenty v organizácii a reagovať na ne. Môže spadať pod SOC alebo môže pôsobiť ako hlavná bezpečnostná organizácia samostatne. CSIRT sa líši od SOC v tom, že je to zvyčajne konglomerát rolí v rámci podniku, ktoré sú zapojené do všetkých typov funkcií reakcie na incidenty. Vrátane vzťahov s verejnosťou (PR), marketingu, zákazníckej podpory a manažmentu. Konečným cieľom CSIRT je minimalizovať a kontrolovať škody vyplývajúce z incidentu. CSIRT musí riešiť nie len samotnú hrozbu, ale aj komunikovať so zákazníkmi, predstavenstvom a verejnosťou o incidente. A napríklad v prípade, ak udalosť spôsobil interný aktér, bude potrebné prijať disciplinárne a možno aj právne kroky voči príslušným zamestnancom.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Vo všeobecnosti platí, že začlenenie vyššie spomenutých centier SOC, NOC a CSIRT do bezpečnostného portfólia firmy alebo organizácie veľmi závisí od jej samotnej veľkosti, štruktúry a potrieb. Ako uviedli vyššie spomenuté zdroje, môže dochádzať aj ku kombinácii, respektíve zlučovaniu daných centier.

Údaje o bezpečnosti siete

V tejto kapitole sa venujeme údajom, s ktorými pracujú analytici v SOC centre, a ktoré je možné zo sieťových zariadení zbierať, analyzovať, vyhodnocovať, riešiť a reagovať na ne. Popíšeme základné typy údajov a zdroje, z ktorých pochádzajú. Takisto bude na tomto mieste spomenutý SIEM, ktorý predstavuje zoskupenie nástrojov pracujúcich s týmito dátami. Pokiaľ nie je uvedené inak, zdrojom nasledujúcich častí je kurz Cisco CyberOps Associate [2] .

Typy bezpečnostných údajov

Základné typy dát možno rozdeliť do šiestich kategórií, a to výstražné údaje, údaje z koncových zariadení, relačné a transakčné dáta, dáta z úplného zachytávania paketov a štatistické dáta. V tejto časti práce spomenuté kategórie stručne popíšeme.

Výstražné údaje (angl. Alert data)

Výstražné údaje pozostávajú zo správ generovaných systémami prevencie narušenia (IPS) alebo systémami detekcie narušenia (IDS) v reakcii na prevádzku, ktorá porušuje pravidlo alebo sa zhoduje s popisom známeho zneužitia, tzv. signatúrou. Ďalej budeme používať už len pojem signatúra. Sieťové IDS (NIDS)sa dodávajú nakonfigurované s pravidlami pre známe zneužitia (angl. expoloits).

Logy koncových zariadení (angl. Host logs)

Host-based intrusion detection systems (HIDS), tieto systémy na detekciu narušenia bezpečnosti bežia na jednotlivých používateľských zariadeniach. Ďalej budeme používať len pojem host-based IDS, alebo HIDS. HIDS nielen deteguje narušenia, ale vo forme tzv. host-based firewallov (bezpečnostných brán na používateľských zariadeniach) môže tiež zabrániť narušeniu. Tento softvér vytvára logy a ukladá ich na koncovom zariadení. V podnikoch je komplikované mať prehľad o dianí na jednotlivých koncových zariadeniach, preto mnohé riešenia obsahujú funkciu, ako logy odosielať na servery centralizovanej správy logov (angl.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

centralized log management servers). Týmto spôsobom je možné logy vyhľadávať z centrálneho miesta pomocou nástrojov NSM. Systémy HIDS môžu používať agentov na odosielanie logov na centralizované servery.

Relačné dáta (angl. Session data)

Údaje o relácii sú záznamom konverzácie medzi dvoma koncovými bodmi siete (najčastejšie klient a server). Údaje o relácii nie sú samotné údaje získané a používané klientom. Údaje o relácii zahŕňajú identifikačné informácie, päticu informácií (angl. five tuples), zdrojovú a cieľovú IP adresu, čísla zdrojového a cieľového portu a typ (IP kód) používaného protokolu. Údaje o relácii zvyčajne zahŕňajú aj ID relácie, množstvo údajov prenesených podľa zdroja a cieľa a informácie súvisiace s trvaním relácie.

Transakčné dáta (angl. Transaction data)

Údaje o transakciách pozostávajú zo správ, ktoré sa vymieňajú počas sieťových relácií. Tieto transakcie je možné zobraziť v prepisoch zachytávania paketov. Logy zariadení uchovávané servermi obsahujú aj informácie o transakciách, ktoré sa vyskytujú medzi klientmi a servermi. Relácia môže napríklad zahŕňať sťahovanie obsahu z webového servera. Transakcie, ktoré predstavujú požiadavky a odpovede, budú zaznamenané v logoch prístupu na serveri alebo prostredníctvom NIDS. Relácia je všetka prevádzka zapojená do vytvárania požiadavky, transakcia je samotná požiadavka.

Úplné zachytávanie paketov (angl. Full packet capture)

Úplné zachytenia paketov sú najpodrobnejšie sieťové údaje, ktoré sa vo všeobecnosti zhromažďujú. Kvôli množstvu detailov sú tiež najnáročnejšími typmi údajov na ukladanie a vyhľadávanie. Úplné zachytenia paketov obsahujú aj skutočný obsah konverzácií. Úplné zachytenia paketov obsahujú text e-mailových správ, HTML na webových stránkach a súbory, ktoré vstupujú do siete alebo ju opúšťajú. Extrahovaný obsah možno obnoviť zo zachytenia úplných paketov a analyzovať na prítomnosť škodlivého softvéru alebo správania používateľov, ktoré porušuje obchodné a bezpečnostné zásady.

Štatistické údaje (angl. Statistical data)

Podobne ako údaje o reláciách, aj štatistické údaje sa týkajú sieťovej prevádzky. Štatistické údaje sa vytvárajú prostredníctvom analýzy iných foriem sieťových údajov. Z

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

týchto analýz možno urobiť závery, ktoré popisujú alebo predpovedajú správanie siete. Štatistické charakteristiky normálneho správania siete je možné porovnať so súčasnou sieťovou prevádzkou v snahe odhaliť anomálie. Štatisticky významné rozdiely by mali vyvolať poplach (alarm) a urýchlené vyšetrovanie.

Network Behavior Analysis (NBA) a Network Behavior Anomaly Detection (NBAD) sú prístupy k monitorovaniu sieťovej bezpečnosti, ktoré využívajú pokročilé analytické techniky na analýzu dát sieťovej telemetrie protokolom NetFlow alebo Internet Protocol Flow Export (IPFIX). Techniky, ako sú prediktívna analytika a umelá inteligencia, vykonávajú pokročilé analýzy podrobných údajov o reláciách, aby odhalili potenciálne bezpečnostné incidenty.

Logy koncových zariadení

Významnými údajmi, ktoré sme oddelili do samostatnej podkapitoly sú logy koncových zariadení, ktoré nás informujú o stave koncových zariadení, a poskytujú nám ďalší uhol pohľadu na sieť.

Syslog

Syslog obsahuje špecifikácie pre formáty správ, štruktúru aplikácie klient-server a sieťový protokol. Tento štandard sa používa na zaznamenávanie udalostí na centralizované syslog servery. Jedná sa o klient/server protokol podporovaný širokou škálou zariadení.

Odosielateľ odosiela malú textovú správu (<1kB) do syslog prijímača. Správy sa odosielajú cez port 514 (UDP) a 5000 (TCP). Tieto údaje sú, s výnimkou napr. SSL, zvyčajne odosielané vo forme obyčajného textu.

Server logs

Logy zo serverov sú základným zdrojom údajov pre monitorovanie bezpečnosti siete. Obzvlášť dôležité sú logy DNS (proxy) serverov, ktoré dokumentujú všetky dotazy a odpovede DNS, ktoré sa vyskytujú v sieti. Sú taktiež užitočné na identifikáciu koncových zariadení, ktorí mohli navštíviť nebezpečné webové stránky, a na identifikáciu exfiltrácie údajov DNS a pripojení k malvérovým command-and-control serverom. Obsah log súborov udalostí závisí od typu servera.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Logovanie z medziľahlých sieťových zariadení

Bezpečnostné zariadenia, ako aj iné medziľahlé sieťové zariadenia je možné nakonfigurovať tak, aby odosielali udalosti a výstrahy na platformy správy zabezpečenia pomocou protokolu SNMP alebo syslogu.

Proxy logs

Proxy servery, ako sú tie, ktoré sa používajú na webové a DNS požiadavky, obsahujú cenné logy, ktoré sú primárnym zdrojom údajov na monitorovanie bezpečnosti siete. Proxy server generuje logy všetkých požiadaviek a odpovedí. Tieto logy možno potom analyzovať, aby sa zistilo, ktoré koncové zariadenia odosielajú požiadavky, či sú ciele bezpečné alebo potenciálne škodlivé, a tiež získať prehľad o druhu zdrojov, ktoré boli stiahnuté.

Webové servery proxy poskytujú údaje, ktoré pomáhajú určiť, či boli odpovede z web stránky generované ako odpoveď na legitímne požiadavky, alebo boli zmanipulované tak, aby vyzerali ako odpovede, ale v skutočnosti ide o zneužitie. Je tiež možné použiť webové proxy na kontrolu odchádzajúcej prevádzky ako prostriedok ochrany pred stratou údajov (angl. data loss prevention, DLP). DLP zahŕňa skenovanie odchádzajúcej prevádzky, aby sa zistilo, či údaje, ktoré opúšťajú web, obsahujú citlivé, dôverné alebo tajné informácie.

SIEM

Používa sa v mnohých organizáciách na poskytovanie správ v reálnom čase a dlhodobej analýzy bezpečnostných udalostí, ako je znázornené na obrázku 1.3. Fialové šípky nám znázorňujú vstupy, ktoré zahŕňajú informácie zbierané z jednotlivých zariadení. Oranžové šípky predstavujú výstupy, ktoré SIEM po spracovaní informácií ponúka (napr. dashboardy a reporty)

Cieľom SIEM nástrojov je poskytnúť komplexný pohľad na podnikovú sieť pomocou nasledujúcich funkcií:

- **Zhromažďovanie údajov (angl. Log collection)** – Záznamy o udalostiach zo zdrojov (aktív) v celej organizácii poskytujú dôležité forenzné informácie a pomáhajú pri riešení požiadaviek na podávanie správ o zhode.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

- **Normalizácia (angl. Normalization**) – Mapuje správy logov z rôznych systémov do spoločného dátového modelu, čo umožňuje organizácii pripojiť sa a analyzovať súvisiace udalosti, aj keď sú pôvodne zaznamenané v rôznych zdrojových formátoch.
- **Korelácia (angl. Corelation**) – Spája logy a udalosti z rôznych systémov alebo aplikácií, čím urýchľuje detekciu a reakciu na bezpečnostné hrozby.
- **Agregácia (angl. Aggregation**) – Znižuje objem údajov o udalostiach konsolidáciou duplicitných záznamov udalostí.
- **Hlásenie (angl. Reporting)** – Predstavuje korelované a agregované údaje o udalostiach monitorovaných v reálnom čase a dlhodobých súhrnoch vrátane grafických interaktívnych panelov (angl. dashboards).
- **Súlad (angl. Compliance)** – Toto je nahlasovanie na splnenie požiadaviek rôznych nariadení o dodržiavaní regulácií.

Firewally novej generácie (Next-Generation Firewalls, NGFW)

Next-Generation Firewalls rozširujú sieťovú bezpečnosť za IP adresy a čísla portov transportnej vrstvy na aplikačnú vrstvu, resp. ešte aj hlbšie za túto úroveň analýzy. NextGen firewally sú pokročilé zariadenia, ktoré poskytujú oveľa viac funkcií ako predchádzajúce generácie zariadení na zabezpečenie siete. Jednou z týchto funkcií sú informačné panely (angl. dashboards) s interaktívnymi funkciami, ktoré umožňujú rýchle správy o špecifických informáciách bez potreby SIEM alebo iných nástrojov pre koreláciu udalostí.

Bežné udalosti NGFW zahŕňajú:

- **Udalosť pripojenia (angl. Connection Event)** – Logy pripojení obsahujú údaje o reláciách, ktoré zisťuje priamo Next-Generation IPS (NGIPS). Udalosti pripojenia zahŕňajú základné vlastnosti pripojenia, ako sú časové pečiatky, zdrojové a cieľové adresy IP a metadáta o tom, prečo bolo pripojenie zalogované, napríklad ktoré pravidlo riadenia prístupu zalogovalo udalosť.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

- **Udalosť narušenia (angl. Intrusion Event)** – systém skúma pakety, ktoré prechádzajú sieťou, na škodlivú aktivitu, ktorá by mohla ovplyvniť dostupnosť, integritu a dôvernosť koncového zariadenia a jeho údajov. Keď systém identifikuje možné narušenie, vygeneruje udalosť narušenia, ktorá je záznamom dátumu, času, typu zneužitia a kontextových informácií o zdroji útoku a jeho cieli.
- **Udalosť koncového zariadenia (angl. Host or Endpoint Event)** - Keď sa v sieti objaví koncové zariadenie, môže ho systém zistiť a zaznamenať podrobnosti o hardvéri zariadenia, IP adresách a poslednej známej prítomnosti v sieti.
- **Udalosť zisťovania siete (angl. Network Discovery Event)** - Udalosti zisťovania siete predstavujú zmeny, ktoré boli zistené v monitorovanej sieti. Tieto zmeny sa zaznamenávajú v reakcii na politiky zisťovania siete, ktoré špecifikujú druhy údajov, ktoré sa majú zhromažďovať, segmenty siete, ktoré sa majú monitorovať, a hardvérové rozhrania zariadenia, ktoré by sa malo použiť na zhromažďovanie udalostí.
- **Udalosť Netflow (angl. Netflow Event)** - zisťovanie siete môže využívať množstvo mechanizmov, jedným z nich je použitie exportovaných záznamov toku NetFlow na generovanie nových udalostí pre koncové zariadenia a servery.

Informácie o sieťových tokoch a aplikáciách

Informácie o sieťových tokoch nám poskytujú detailnejšie dáta a pohľad na sieť, respektíve sieťovú prevádzku. Hoci NetFlow protokol nebol pôvodne koncipovaný ako nástroj na monitorovanie bezpečnosti siete, považuje sa za užitočný nástroj pri analýze bezpečnostných incidentov siete. Môže sa použiť na pochopenie správania jednotlivých používateľov, alebo na sledovanie pohybu útočníka, či zneužitia z používateľa na používateľa (angl. host to host) v rámci siete.

NetFlow

NetFlow je protokol od spoločnosti Cisco, ako nástroj na riešenie problémov so sieťou a účtovanie prenesených dát založené na reláciách. NetFlow efektívne poskytuje

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

dôležitú sadu služieb pre IP aplikácie, vrátane účtovania sieťovej prevádzky (angl. accounting), účtovania siete na základe používania (angl. billing), plánovania siete, bezpečnosti, možností monitorovania odmietnutia služby a monitorovania siete. NetFlow poskytuje informácie o sieťových používateľoch a aplikáciách, časoch špičiek v sieti a smerovaní prevádzky. NetFlow nevykonáva úplné zachytávanie paketov, ani nezachytáva samotný obsah v pakete. NetFlow zaznamenáva informácie o toku paketov vrátane metadát. Cisco umožnilo jeho použitie (vo verzii 9) ako základ pre štandard IETF s názvom IPFIX.

NetFlow je založený na sade 5 až 7 atribútov IP paketov:

- Zdrojová IP adresa
- Cieľová adresa IP
- Zdrojový port
- Cieľový port
- Typ protokolu vrstvy L3
- Trieda služby
- Rozhranie smerovača alebo prepínača

Všetky pakety s rovnakou zdrojovou/cieľovou IP adresou, zdrojovými/cieľovými portami, typom protokolu a triedou služby sú zoskupené do toku a potom sa pakety a bajty spočítajú. Všetky záznamy toku NetFlow budú obsahovať prvých päť položiek v zozname vyššie a časové pečiatky začiatku a konca toku. Dodatočné informácie sú veľmi variabilné a možno ich nakonfigurovať. K dispozícii je veľké množstvo atribútov pre tok. IANA register subjektov IPFIX uvádza niekoľko stoviek, pričom prvých 128 je najčastejšie používaných.

Viditeľnosť a riadenie aplikácií (Application Visibility and Control)

Identifikácia sieťových aplikácií podľa portu poskytuje veľmi malú granularitu a prehľad o správaní používateľov. Viditeľnosť aplikácie prostredníctvom identifikácie signatúr aplikácií však identifikuje, čo používatelia robia. Výrobcovia zvyčajne pri svojich produktoch uvádzajú koľko aplikácií vedia rozoznať, pričom počet sa pohybuje od 1000 smerom nahor.

Application Visibility and Control (AVC) systém od spoločnosti Cisco kombinuje viaceré technológie na rozpoznávanie, analýzu a riadenie viac ako 1000 aplikácií. AVC používa novú generáciu sieťového rozpoznávania aplikácií (angl. network-based application recognition) verzie 2 (NBAR2), tiež známu ako Next-Generation NBAR, na zisťovanie a

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

klasifikáciu aplikácií používaných v sieti. Podobné nástroje poskytujú aj ďalší výrobcovia, no v tejto práci sa im nebudeme ďalej venovať.

Logy ako výstup z filtrovania špecifického obsahu (Content filter logs)

Zariadenia, ktoré poskytujú filtrovanie obsahu, ako napríklad Cisco Email Security Appliance (ESA) a Cisco Web Security Appliance (WSA), poskytujú širokú škálu funkcií na monitorovanie bezpečnosti. Pre mnohé z týchto funkcií je k dispozícii logovanie.

ESA má napríklad viac ako 30 logov, ktoré možno použiť na monitorovanie väčšiny aspektov doručovania e-mailov, fungovania systému, antivírusových, antispamových operácií a zoznamov blokovaných a povolených rozhodnutí. Väčšina logov je uložená v textových súboroch a možno ich zhromažďovať na syslog serveroch alebo ich možno odoslať na servery FTP alebo SCP. Okrem toho môžu byť upozornenia týkajúce sa fungovania samotného zariadenia a jeho podsystémov monitorované e-mailom pre správcov, ktorí sú zodpovední za monitorovanie a prevádzku zariadenia.

Zariadenia WSA ponúkajú podobnú úroveň fungovania. WSA efektívne funguje ako webový proxy server, čo znamená, že zaznamenáva všetky prichádzajúce a odchádzajúce informácie o transakciách pre prenos HTTP. WSA možno nakonfigurovať na odosielanie logov na server rôznymi spôsobmi, vrátane syslog, FTP a SCP. Ďalšie logy, ktoré má WSA k dispozícii, zahŕňajú logy rozhodnutí ACL, logy skenovania škodlivého softvéru a logy filtrovania reputácie webu.

Vyhodnocovanie upozornení

V tejto časti popíšeme prácu s údajmi, ktoré sme spomínali v časti: Údaje o bezpečnosti siete pomocou nástrojov, ktoré sme popísali v časti: Nástroje

Zdroje upozornení

V tejto časti sa venujeme zdrojom upozornení a výstražných dát. Našim cieľom v tejto práci je poskytnúť SOC analytikom všetky tri základné funkcie, t.j. úplné zachytávanie paketov a dátové typy, systémy detekcie narušenia a nástroje na analýzu výstrah (angl. alerts). Tieto funkcie sa nám aj podarilo pokryť, pričom systémy detekcie narušenia sme

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

riešili iba na úrovni siete, a nie na úrovni jednotlivých koncových zariadení a kritických serverov.

Detekčné nástroje na zhromažďovanie bezpečnostných výstrah

Našim cieľom je vytvoriť také integrované prostredie, aby sa čo najviac zjednodušilo nasadenie komplexného riešenia NSM, a využili sa už existujúce systémy, ktoré už boli na katedre nasadené v minulosti, a nemuseli sa výrazne meniť, ani nahrádzať, pokiaľ spĺňajú požadovaný účel.

Generovanie bezpečnostných výstrah

Bezpečnostné výstrahy sú oznamovacie správy, ktoré sú generované nástrojmi, systémami a bezpečnostnými zariadeniami NSM (angl. Alert generation). Možno ich použiť na upozornenie analytikov kybernetickej bezpečnosti na udalosti, ktoré si vyžadujú pozornosť. Analytik kybernetickej bezpečnosti môže pracovať s frontom takýchto výstražných upozornení, ktoré ďalej môže skúmať, klasifikovať, eskalovať alebo zrušiť upozornenia.

Výstrahy budú vo všeobecnosti obsahovať päticu informácií, ak sú k dispozícii, ako aj časové pečiatky a informácie identifikujúce, ktoré zariadenie alebo systém generoval výstrahu.

Ďalšími informáciami môžu byť informácie o tom, či bolo na prevádzku aplikované rozhodnutie o povolení alebo zamietnutí, niektoré zachytené dáta z užitočnej časti paketu (angl. packet payload), hodnota hash pre stiahnutý súbor alebo iný typ údaju.

V závislosti od technológie zabezpečenia môžu byť výstrahy generované na základe pravidiel, signatúr, anomálií alebo správania. Bez ohľadu na to, ako sú generované, podmienky, ktoré spúšťajú výstrahu, musia byť nejakým spôsobom vopred definované.

Informácie nájdené vo výstrahách, ktoré sa zobrazujú v ELK, sa budú líšiť vo formáte správy, pretože pochádzajú z rôznych zdrojov. Pre analytika kybernetickej bezpečnosti je dôležité, aby bol schopný interpretovať, čo spustilo výstrahu, aby bolo možné výstrahu vyšetriť. Z tohto dôvodu by mal analytik kybernetickej bezpečnosti rozumieť komponentom pravidiel IDS Suricata, ktoré sú hlavným zdrojom upozornení v našom nasadenom systéme ELK.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Prehľad vyhodnotenia bezpečnostných výstrah

V tejto časti popíšeme motiváciu vyhodnocovania dát, samotné vyhodnocovanie a možné výsledky tohto procesu. Spomenieme aj dva typy prístupu k analýze. Informácie pri spracovaní tejto časti sme čerpali hlavne zo zdroja [2] .

Potreba vyhodnotenia výstrahy

Hrozby sa neustále menia, pretože sa objavujú nové zraniteľné miesta a vyvíjajú sa nové hrozby. Ako sa menia potreby používateľov a organizácie, mení sa aj útok. Aktéri hrozieb sa naučili, ako rýchlo meniť atribúty útokov, aby sa vyhli odhaleniu. Nie je možné navrhnúť opatrenia na zabránenie všetkým možným hrozbám Aktéri hrozieb budú vždy vyvíjať čo najväčšiu o to, aby sa vyhli ochranným opatreniam, bez ohľadu na to, aké sofistikované môžu byť tieto opatrenia. Preto nastávajú situácie, v ktorých analytik odhalí útok počas toho ako prebieha, alebo až po tom ako sa vyskytol nejaký incident. Odporúča sa, aby pravidlá detekcie boli viac konzervatívne. Inými slovami, je lepšie mať upozornenia, ktoré sú niekedy generované legitímnou prevádzkou, ako mať pravidlá, ktoré vynechávajú škodlivú prevádzku. Z tohto dôvodu je potrebné, aby skúsení analytici kybernetickej bezpečnosti preskúmali výstrahy, aby zistili, či skutočne došlo k zneužitiu.

Vyhodnocovanie bezpečnostných výstrah

Bezpečnostné incidenty sú klasifikované pomocou schémy prevzatej z lekárskej diagnostiky. Ide o to, že buď diagnóza môže byť presná, pravdivá, nepresná alebo nepravdivá. Falošné diagnózy sú buď drahé, alebo nebezpečné. Pri analýze bezpečnosti siete sa analytikovi kybernetickej bezpečnosti zobrazí výstraha. Analytik kybernetickej bezpečnosti sa pýta: „Systém hovorí, že došlo k zneužitiu. Je to pravda?"

Upozornenia možno klasifikovať takto:

- Skutočne pozitívne (angl. true positive)
  - Upozornenie bolo overené ako skutočný bezpečnostný incident.
  - Skutočné pozitíva sú požadovaným typom výstrahy. Znamená to, že pravidlá, ktoré generujú upozornenia, fungovali správne.
- Falošne pozitívne (angl. false positive)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

- Výstraha nenaznačuje skutočný bezpečnostný incident. Ide o legitímnu aktivitu, ktorá vedie k falošne pozitívnemu výsledku.
- Nie sú žiadúce. Hoci nenaznačujú, že došlo k nezistenému zneužitiu, sú nákladné, pretože analytici kybernetickej bezpečnosti musia prešetriť falošné poplachy, a tým sa uberá čas vyšetrovaniu výstrah, ktoré poukazujú na skutočné zneužitie.

Alternatívnou situáciou je, že upozornenie nebolo vygenerované. Neprítomnosť výstrahy možno klasifikovať ako:

- Skutočne negatívne (angl. true negative)
  - Nevyskytol sa žiadny bezpečnostný incident. Aktivita je legitímna.
  - Sú žiaduce. Naznačujú, že legitímna - normálna prevádzka je správne ignorovaná a nevydávajú sa chybné upozornenia.
- Falošne negatívne (angl. false negative)
  - Došlo k nezistenému incidentu.
  - Sú nebezpečné. Naznačujú, že bezpečnostné systémy, ktoré sú na mieste, nezistili zneužitie. Tieto incidenty môžu zostať dlho neodhalené a môže dôjsť k strate a poškodeniu údajov.

Legitímne udalosti sú tie, ktoré by nemali spúšťať upozornenia. Nadmerné legitímne udalosti naznačujú, že niektoré pravidlá alebo iné detektory je potrebné zlepšiť alebo odstrániť. Falošne negatívne správy môžu byť objavené až dlho po zneužití. To sa môže stať prostredníctvom retrospektívnej bezpečnostnej analýzy (angl. retrospective security analysis, RSA). RSA sa môže vyskytnúť, keď sa na archivované údaje o zabezpečení siete použijú novo získané pravidlá alebo iné informácie o hrozbách. Z tohto dôvodu je dôležité monitorovať spravodajstvo o hrozbách (angl. threat intelligence), aby sme sa dozvedeli o nových zraniteľnostiach a zneužitiach a vyhodnotili pravdepodobnosť, či sieť bola voči nim niekedy v minulosti zraniteľná. V niektorých prípadoch môže byť pridanie nových zmierňujúcich techník dostatočné, v iných je potrebné vykonať podrobnejšiu analýzu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Deterministická analýza a pravdepodobnostná analýza

Na vyhodnotenie rizika, či prieniky, zneužitia budú v danej sieti úspešné (angl. exploits), možno použiť štatistické techniky, pričom sa využívajú dva všeobecné prístupy, a to deterministická a pravdepodobnostná analýza (angl. deterministic analysis and probabilistic analysis).

Deterministická analýza vychádza z predpokladu, že na to aby bol prienik úspešný, musia byť úspešné aj všetky predchádzajúce kroky. Analytik kybernetickej bezpečnosti pozná kroky na úspešné zneužitie.

Pravdepodobnostná analýza používa štatistické techniky na určenie pravdepodobnosti, čie dôjde k úspešnému zneužitiu, na základe pravdepodobnosti, s ktorou môže byť každý krok zneužitia úspešný.

Digitálna forenzná analýza

V záujme ochrany organizácie a predchádzania počítačovej kriminalite je potrebné identifikovať aktérov hrozby, nahlásiť ich príslušným orgánom a poskytnúť dôkazy na podporu trestného stíhania. Analytici kybernetickej bezpečnosti prvého stupňa sú často prví, ktorí odhalia pochybenia a preto musia vedieť, ako správne zaobchádzať s dôkazmi a pripisovať ich aktérom hrozieb.

Digitálna forenzná technika je získavanie a vyšetrovanie informácií nájdených na digitálnych zariadeniach, ktoré súvisia s trestnou činnosťou. Týmito informáciami môžu byť údaje o pamäťových zariadeniach, vo volatilnej počítačovej pamäti, alebo stopy počítačovej kriminality, ktoré sa uchovávajú v sieťových údajoch, ako sú napríklad zachytenia plných údajov (pcaps) alebo logy, ktoré sme spomenuli v časti 1.2.1 Typy bezpečnostných údajov. Je nevyhnutné, aby sa všetky indikátory narušenia bezpečnosti zachovali pre budúcu analýzu a priradenie útoku.

Činnosť kyberzločinu možno vo všeobecnosti charakterizovať ako činnosť pochádzajúcu z konkrétnych organizácií alebo aj mimo nich. Vyšetrovanie priestupkov osôb, nezastrešených niektorou organizáciou, sa týka jednotlivcov vo vnútri organizácie. Títo jednotlivci sa môžu správať spôsobom, ktorý porušuje používateľské dohody alebo iné správanie, ktoré ešte nemožno zaradiť ako trestno-právny zločin. Ak sú však jednotlivci

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

podozriví z účasti na trestnej činnosti zahŕňajúcej krádež alebo zničenie duševného vlastníctva, organizácia sa môže rozhodnúť zapojiť orgány činné v trestnom konaní, a v takom prípade sa vyšetrovanie zverejní. Interní používatelia mohli tiež použiť sieť organizácie na vykonávanie iných kriminálnych aktivít, ktoré nesúvisia s poslaním organizácie, ale sú v rozpore s rôznymi právnymi predpismi. V tomto prípade vykonajú vyšetrovanie verejní činitelia.

Keď externý útočník zneužije sieť a ukradne alebo pozmení údaje, je potrebné zhromaždiť dôkazy na zdokumentovanie rozsahu zneužitia. Rôzne regulačné orgány špecifikujú rozsah opatrení, ktoré musí organizácia vykonať, v prípade ak boli ohrozené rôzne typy údajov. Výsledky forenzného vyšetrovania môžu pomôcť identifikovať opatrenia, ktoré je potrebné vykonať.

V niektorých prípadoch môže byť predmetom vyšetrovania samotná organizácia. Analytici kybernetickej bezpečnosti sa môžu ocitnúť v priamom kontakte s digitálnymi forenznými dôkazmi, ktoré podrobne opisujú správanie členov organizácie. Analytici musia poznať požiadavky týkajúce sa uchovávania a zaobchádzania s takýmito dôkazmi. Ak tak neurobia, môže to mať za následok trestné sankcie pre organizáciu a dokonca aj pre analytika kybernetickej bezpečnosti, ak sa preukáže úmysel zničiť dôkazy.

Digitálny forenzný proces

Je dôležité, aby organizácia vyvinula dobre zdokumentované procesy a postupy pre digitálnu forenznú analýzu. Súlad s predpismi si môže vyžadovať túto dokumentáciu a túto dokumentáciu môžu orgány kontrolovať v prípade verejného vyšetrovania.

Špeciálna publikácia, NIST 800-86 Sprievodca integráciou forenzných techník reakcie na incidenty, je cenným zdrojom pre organizácie, ktoré potrebujú poradenstvo pri vývoji digitálnych forenzných plánov. Odporúča sa napríklad, aby sa forenzná analýza vykonávala pomocou štvorfázového procesu.

- Zber (angl. collection) - ide o identifikáciu potenciálnych zdrojov forenzných údajov a získavanie, manipuláciu a uchovávanie týchto údajov. Táto fáza je kritická, pretože je potrebné venovať osobitnú pozornosť tomu, aby nedošlo k poškodeniu, strate alebo vynechaniu dôležitých údajov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

- Vyšetrenie (angl. examination) – t.j. posúdenie a extrahovanie relevantných informácií zo zozbieraných údajov (napr. dekompresia alebo dešifrovanie údajov). Možno bude potrebné odstrániť informácie, ktoré sú pre vyšetrovanie irelevantné. Identifikácia skutočných dôkazov vo veľkých zbierkach údajov môže byť veľmi náročná a to aj časovo.
- Analýza (angl. analysis) - to znamená vyvodenie záverov z údajov. Mali by sa zdokumentovať významné prvky, ako sú ľudia, miesta, časy, udalosti atď. Tento krok môže zahŕňať aj koreláciu údajov z viacerých zdrojov.
- Nahlásenie (angl. reporting) - To zahŕňa prípravu a prezentáciu informácií, ktoré vyplynuli z analýzy. Podávanie správ by malo byť nestranné a v prípade potreby by sa mali poskytnúť alternatívne vysvetlenia. Mali by sa zahrnúť obmedzenia analýzy a problémy, ktoré sa vyskytli. Mali by sa urobiť aj návrhy na ďalšie vyšetrovanie a ďalšie kroky.

Typy dôkazov

V súdnom konaní sa dôkazy vo všeobecnosti klasifikujú ako priame alebo nepriame. Priame dôkazy sú dôkazy, ktoré mal obvinený nepochybne k dispozícii, alebo sú dôkazmi očitých svedkov od niekoho, kto priamo pozoroval kriminálne správanie.

Dôkazy sa ďalej klasifikujú ako:

- Najlepší dôkaz – Toto je dôkaz, ktorý je v pôvodnom stave. Týmito dôkazmi môžu byť úložné zariadenia používané obvineným alebo archívy spisov, pri ktorých sa dá dokázať, že sú nezmenené.
- Potvrdzujúce dôkazy – Toto je dôkaz, ktorý podporuje tvrdenie, ktoré vychádza z najlepších dôkazov.
- Nepriamy dôkaz – Ide o dôkaz, ktorý v kombinácii s inými faktami zakladá hypotézu. (Napríklad dôkaz, že jednotlivec spáchal podobné trestné činy, môže podporiť tvrdenie, že osoba spáchala trestný čin, z ktorého je obvinená)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Odporúčanie na zber dôkazov

IETF RFC 3227 poskytuje usmernenia pre zber digitálnych dôkazov. Opisuje odporúčanie na zber digitálnych dôkazov na základe nestálosti (volatilnosti) údajov. Údaje uložené v pamäti RAM sú najviac nestále a po vypnutí zariadenia sa stratia. Okrem toho môžu byť dôležité údaje v nestálej pamäti prepísané rutinnými strojovými procesmi. Zhromažďovanie digitálnych dôkazov by preto malo začať s najnestabilnejšími dôkazmi a pokračovať k viac stabilným. Príklad poradia zhromažďovania dôkazov od najmenej stabilných, po viac stabilné, je nasledujúci:

1. Pamäťové registre, vyrovnávacie pamäte
2. Smerovacia tabuľka, ARP tabuľka, tabuľka procesov, štatistiky jadra, RAM
3. Systémy dočasných súborov
4. Neprchavé médiá, pevné a vymeniteľné
5. Diaľkové zaznamenávanie a monitorovanie údajov
6. Fyzické prepojenia a topológie
7. Archívne médiá, pásky alebo iné zálohy

Podrobnosti o systémoch, z ktorých boli zhromaždené dôkazy, vrátane toho, kto má k týmto systémom prístup a na akej úrovni oprávnení by sa mali zaznamenávať. Takéto podrobnosti by mali zahŕňať hardvérové a softvérové konfigurácie systémov, z ktorých boli údaje získané.

Spracovateľský reťazec

Hoci dôkazy mohli byť zhromaždené zo zdrojov, ktoré podporujú pripisovanie obvinenému jednotlivcovi, možno tvrdiť, že dôkazy mohli byť po ich zhromaždení pozmenené alebo vymyslené. Aby bolo možné čeliť tomuto argumentu, je potrebné definovať a dodržiavať prísny reťazec kontroly. Spracovateľský reťazec zahŕňa zhromažďovanie, manipuláciu a bezpečné uchovávanie dôkazov. Mali by sa viesť podrobné záznamy, v zmysle odpovedí na nasledujúce otázky:

- Kto objavil a zhromaždil dôkazy?
- Všetky podrobnosti o nakladaní s dôkazmi vrátane časov, miest a zúčastneného personálu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

- Kto má primárnu zodpovednosť za dôkazy, kedy bola zodpovednosť pridelená a kedy sa zmenila väzba?
- Kto má fyzický prístup k dôkazom, kým boli uložené? Prístup by mal byť obmedzený len na najnutnejší personál.

Integrita a ochrana údajov

Pri zbere dát je dôležité, aby boli zachované v pôvodnom stave. Časová pečiatka súborov by mala byť zachovaná. Z tohto dôvodu by sa pôvodné dôkazy mali skopírovať a analýza by sa mala vykonávať iba na kópiách originálu. Je to preto, aby sa predišlo náhodnej strate alebo zmene dôkazov. Keďže časové pečiatky môžu byť súčasťou dôkazov, treba sa vyhnúť otváraniu súborov z pôvodného média.

Proces používaný na vytváranie kópií dôkazov, ktoré sa používajú pri vyšetrovaní, by sa mal zaznamenať. Kedykoľvek je to možné, kópie by mali byť priamymi kópiami pôvodných úložných jednotiek na bitovej úrovni. Malo by byť možné porovnať archivovaný obraz disku a obraz vyšetrovaného disku, aby sa zistilo, či sa s obsahom skúmaného disku nemanipulovalo. Z tohto dôvodu je dôležité pôvodný disk archivovať a chrániť, aby bol zachovaný v pôvodnom, nepoškodenom stave.

Volatilná pamäť môže obsahovať forenzné dôkazy, preto by sa mali použiť špeciálne nástroje na uchovanie týchto dôkazov pred vypnutím zariadenia a stratou dôkazov. Používatelia by nemali odpájať ani vypínať infikované počítače, pokiaľ im to výslovne nepovolí bezpečnostný personál.

Dodržiavanie týchto procesov zabezpečí, že sa zachovajú všetky dôkazy o nesprávnom konaní a bude možné identifikovať akékoľvek náznaky kompromitácie.

Priradenie útoku

Po vyhodnotení rozsahu kybernetického útoku a zhromaždení a uchovaní dôkazov sa môže reakcia na incident presunúť k identifikácii zdroja útoku. Existuje široká škála aktérov hrozieb, od nespokojných jednotlivcov, hackerov, kyberzločincov a zločineckých gangov alebo jednotlivých štátov. Niektorí zločinci konajú zvnútra siete, zatiaľ čo iní môžu byť na druhej strane sveta. Sofistikovanosť počítačovej kriminality sa tiež líši.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Priradenie hrozby sa vzťahuje na akt určenia jednotlivca, organizácie alebo národa zodpovedného za narušenie bezpečnosti. Identifikácia zodpovedných aktérov hrozby by sa mala uskutočniť prostredníctvom systematického vyšetrovania dôkazov.

Pri vyšetrovaní založenom na dôkazoch tím pre reakciu na incidenty koreluje taktiky, techniky a postupy (TTP), ktoré boli použité pri incidente, s inými známymi zneužitiami. Kyberzločinci, podobne ako iní zločinci, majú špecifické črty, ktoré sú spoločné pre väčšinu ich zločinov. Dôkazy o počítačovej kriminalite sú len zriedka priamym dôkazom. Identifikácia spoločných čŕt medzi TTP pre známych a neznámych aktérov hrozby je nepriamy dôkaz.

Niektoré aspekty hrozby, ktoré môžu pomôcť pri pripisovaní, sú umiestnenie pôvodných koncových zariadení alebo domén, vlastnosti kódu používaného v malvéri, používané nástroje a ďalšie techniky. Niekedy na úrovni národnej bezpečnosti nemožno hrozby otvorene pripísať, pretože by to odhalilo metódy a schopnosti, ktoré je potrebné chrániť.

Pri interných hrozbách hrá hlavnú úlohu správa aktív. Odhalenie zariadení, z ktorých bol spustený útok, môže viesť priamo k aktérovi hrozby. IP adresy, MAC adresy a protokoly DHCP môžu pomôcť sledovať adresy použité pri útoku späť na konkrétne zariadenie. AAA Logy zo zariadení s databázou používateľov slúžiace pre autentifikáciu, autorizáciu a účtovanie (angl. Authentication, Authorization, Accounting, AAA) sú v tomto smere veľmi užitočné, pretože sledujú kto v akom čase pristupoval k akým sieťovým zdrojom.

The MITRE ATT&CK Framework

Jedným zo spôsobov, ako pripísať útok konkrétnym aktérom hrozieb, t.j. identifikovať daných aktérov, je modelovať správanie aktérov hrozby. Rámec MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) umožňuje schopnosť odhaliť TTP útočníkov ako súčasť obrany pred hrozbami a priradenia útoku. MITRE ATT&CK Framework je globálna databáza znalostí o správaní sa aktérov hrozieb. Je založený na pozorovaní a analýze skutočných prienikov do siete s cieľom opísať správanie útočníka, nie útok samotný. Je navrhnutý tak, aby umožnil automatizované zdieľanie informácií definovaním dátových štruktúr na výmenu informácií medzi komunitou používateľov a organizáciou MITRE.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

V čase písania tejto práce obsahuje tento rámec 14 taktík, 185 techník a 367 sub-techník [14] .

The Cyber Kill Chain

Cyber Kill Chain vyvinula spoločnosť Lockheed Martin na identifikáciu a prevenciu kybernetických prienikov. Ku Cyber Kill Chain vedie sedem krokov. Zameranie sa na tieto kroky pomáha analytikom pochopiť techniky, nástroje a postupy aktérov hrozieb. Pri reakcii na bezpečnostný incident je cieľom odhaliť a zastaviť útok čo najskôr v procese jeho priebehu (angl. kill chain progression). Čím skôr je útok zastavený, tým menšie poškodenie je spôsobené, a tým menej sa útočník dozvie o cieľovej sieti.

Cyber Kill Chain špecifikuje, čo musí útočník splniť, aby dosiahol svoj cieľ. Ak je útočník zastavený v ktorejkoľvek fáze, reťazec útoku je prerušený. Prelomenie reťazca znamená, že obranca úspešne zmaril vniknutie aktéra hrozby. Aktéri hrozieb sú úspešní vtedy, ak dokončia krok 7:

1. Prieskum (angl. Reconnaissance)
2. Ozbrojenie (angl. Weaponization)
3. Doručenie (angl. Delivery)
4. Využitie (angl. Exploitation)
5. Inštalácia (angl. Installation)
6. Príkaz a ovládanie (angl. Command and control)
7. Akcie na ciele (angl. Actions on objectives)

Viac o tomto rámci, respektíve krokoch Cyber Kill Chain sme popísali v dokumente s názvom KrokyCyberKillChain, ktorý je uložený v Prílohe B.

Diamantový model analýzy narušenia bezpečnosti

Diamantový model je určený pre analýzu narušenia bezpečnosti, bezpečnostného incidentu, alebo udalosti (angl. diamond model of intrusion analysis) a pozostáva zo štyroch častí. V diamantovom modeli je udalosť časovo ohraničená aktivita, ktorá je obmedzená na konkrétny krok, v ktorom útočník využíva schopnosť nad infraštruktúrou zaútočiť na obeť s cieľom dosiahnuť konkrétny výsledok.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Štyri základné vlastnosti udalosti narušenia sú útočník, schopnosť, infraštruktúra a obeť:

- Útočník (angl. Adversary) – Toto sú strany zodpovedné za vniknutie.
- Schopnosť (angl. Capability) – Ide o nástroj alebo techniku, ktorú útočník používa na útok na obeť.
- Infraštruktúra (angl. Infrastructure) - Toto je sieťová cesta alebo cesty, ktoré útočníci používajú na vytvorenie a udržiavanie systému pre riadenie a ovládanie cieľových zariadení, ktoré na tento účel zneužijú pre generovanie útoku.
- Obeť (angl. Victim) – Toto je cieľ útoku. Obeť však môže byť spočiatku cieľom a potom môže byť použitá ako súčasť infraštruktúry na spustenie iných útokov.

Meta-funkcie mierne rozširujú model tak, aby zahŕňal nasledujúce dôležité prvky:

- Časová pečiatka – označuje čas začiatku a konca udalosti a je neoddeliteľnou súčasťou zoskupovania škodlivých aktivít.
- Fáza – toto je analogické s krokmi v Cyber Kill Chain, škodlivá aktivita zahŕňa dva alebo viac krokov vykonaných za sebou na dosiahnutie požadovaného výsledku.
- Výsledok – určuje, čo útočník z udalosti získal. Výsledky možno zdokumentovať ako jeden alebo viacero z nasledujúcich údajov: ohrozenie dôvernosti, ohrozenie integrity a ohrozenie dostupnosti.
- Smer – označuje smer udalosti naprieč diamantovým modelom. Patria medzi ne smery: nepriateľ k infraštruktúre, infraštruktúra k obeti, obeť k infraštruktúre a infraštruktúra k útočníkovi.
- Metodológia – používa sa na klasifikáciu všeobecného typu udalosti, ako je skenovanie portov, phishing, útok na doručenie obsahu, záplava TCP segmentami so žiadosťou o synchronizáciu a iné.
- Zdroje – ide o jeden alebo viac externých zdrojov, ktoré útočník používa na napadnutie, ako je softvér, znalosti útočníka, informácie (napr. používateľské mená a heslá) a aktíva na vykonanie útoku (hardvér, finančné prostriedky, zariadenia, prístup k sieti).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Prechod cez diamantový model

Analytik kybernetickej bezpečnosti môže byť vyzvaný, aby použil diamantový model analýzy narušenia na vytvorenie diagramu série udalostí narušenia. Diamantový model je ideálny na ilustráciu toho, ako útočník prechádza z jednej udalosti do druhej (angl. pivoting).

Napríklad na obrázku 1.8 na nasledovnej strane zamestnanec hlási, že jeho počítač sa správa abnormálne. Kontrola koncového zariadenia vykonaná bezpečnostným technikom naznačuje, že počítač je infikovaný škodlivým softvérom. Analýza malvéru ukazuje, že malvér obsahuje zoznam názvov domén Command and control (CnC). Tieto názvy domén sa rozlišujú na zoznam adries IP. Tieto adresy IP sa potom používajú na identifikáciu útočníka, ako aj na skúmanie protokolov, aby sa zistilo, či iné obete v organizácii používajú daný kanál CnC.

Diamantový Model a Cyber Kill Chain

Protivníci nepôsobia len v jednej udalosti. Namiesto toho sa udalosti spájajú do reťazca, v ktorom musí byť každá udalosť úspešne dokončená pred ďalšou udalosťou. Toto vlákno udalostí možno namapovať na reťazec Cyber Kill Chain.

Nasledujúci príklad, zobrazený na obrázku 1.9 na nasledujúcej strane, ilustruje celý proces útočníka, keď vertikálne prechádzajú Cyber Kill Chain, používajú kompromitované zariadenie používateľa na horizontálny prechod k inej obeti a potom začínajú ďalšie vlákno aktivity.

1. Útočník vykoná na webe vyhľadávanie obete spoločnosti Gadgets, Inc., ktorá ako súčasť výsledkov získa názov domény gadgets.com.

2. Útočník používa novoobjavenú doménu gadets.com na nové vyhľadávanie „správca siete gadget.com“ a objavuje príspevky na fórach od používateľov, ktorí tvrdia, že sú správcami siete gadget.com. Používateľské profily odhaľujú ich e-mailové adresy.

3. Útočník posiela phishingové e-maily s pripojeným trójskym koňom administrátorom siete gadget.com.

4. Jeden správca siete (NA1) gadget.com otvorí škodlivú prílohu. Tým sa spustí priložený exploit, ktorý umožní ďalšie spustenie kódu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

5. Kompromitovaný používateľ NA1 odošle správu HTTP post na IP adresu a zaregistruje ju v CnC riadiacej jednotke (riadiaci server). Kompromitovaný používateľ NA1 dostane odpoveď HTTP.

6. Reverzným inžinierstvom sa zistilo, že malvér má nakonfigurované ďalšie IP adresy, ktoré fungujú ako záloha, ak prvý CnC server neodpovedá.

7. Prostredníctvom správy s odpoveďou CnC HTTP odoslanej koncovému zariadeniu NA1 začne malvér fungovať ako webový proxy pre nové pripojenia TCP.

8. Prostredníctvom informácií zo servera proxy, ktorý beží na používateľovi NA1, útočník na webe vyhľadá „najdôležitejší výskum všetkých čias“ a nájde obeť 2, „Zaujímavý výskum Inc“.

9. Útočník skontroluje zoznam e-mailových kontaktov NA1, či neobsahuje nejaké kontakty od spoločnosti „Zaujímavý výskum Inc.“ a objaví kontakt na vedúceho výskumného pracovníka danej spoločnosti.

10. Vedúci výskumu danej spoločnosti dostane e-mail typu spear-phish z e-mailovej adresy NA1 spoločnosti Gadget Inc. odoslanej od používateľa spoločnosti NA1 s rovnakým neželaným obsahom, ako bolo zaznamenané v udalosti 3 (Trójsky kôň).

Útočník má teraz dve obete pod svojou kontrolou, z ktorých možno spustiť ďalšie útoky. Útočník by napríklad mohol vydolovať e-mailové kontakty vedúceho výskumu pre ďalšie potenciálne obete. Útočník môže tiež nastaviť ďalší proxy na exfiltráciu všetkých súborov vedúceho výskumu.

Reakcia na incidenty

Reakcia na incidenty (angl. Incident Response) zahŕňa metódy, zásady a postupy, ktoré organizácia používa pri reakcii na kybernetický útok. Cieľom reakcie na incidenty je obmedziť dopad útoku, posúdiť spôsobenú škodu a implementovať postupy obnovy. Je nevyhnutné, aby organizácie vytvorili a udržiavali podrobné plány reakcie na incidenty a určili zamestnancov, ktorí budú zodpovední za realizáciu všetkých aspektov tohto plánu.

Odporúčania amerického Národného inštitútu pre štandardy a technológie (National Institute of Standards and Technology, NIST) pre reakciu na incidenty sú podrobne uvedené

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

v ich špeciálnej publikácii 800-61, revízia 2 s názvom „Computer Security Incident Handling Guide“ [15] .

Politika, plán a postup reakcie na incidenty

V tejto časti stručne popíšeme prvky politiky, plány a postupu reakcie na kybernetické bezpečnostné incidenty.

Prvky politiky reakcie na incidenty

Politika reakcie na incidenty podrobne uvádza, ako by sa malo s incidentmi zaobchádzať na základe poslania, veľkosti a funkcie organizácie. Politika by sa mala pravidelne prehodnocovať, aby sa prispôsobila tak, aby spĺňala ciele stanoveného plánu.

Prvky plánu reakcie na incidenty

Dobrý plán reakcie na incident pomáha minimalizovať škody spôsobené incidentom. Pomáha tiež zlepšiť celkový program reakcie na incidenty tým, že ho upraví podľa získaných skúseností. Zabezpečí to, že každá strana zapojená do reakcie na incident jasne rozumie nielen tomu, čo bude robiť, ale aj tomu, čo budú robiť ostatní.

Prvky postupu reakcie na incidenty

Postupy, ktoré sa dodržiavajú počas reakcie na incident, by sa mali riadiť plánom reakcie na incident.

Zainteresované strany v procese reakcie na incidenty

Do riešenia incidentov sa môžu zapojiť aj iné skupiny a jednotlivci v rámci organizácie (angl. Incident Response Stakeholders). Niektoré centrá a jednotky sme spomenuli v časti 1.1.5 Ostatné centrá a jednotky riešiace operatívu alebo bezpečnosť. Je dôležité zabezpečiť, aby spolupracovali skôr, ako dôjde k incidentu. Ich odborné znalosti a schopnosti môžu pomôcť tímu reakcie na incidenty počítačovej bezpečnosti (Computer Security Incident Response Team - CSIRT) zvládnuť incident rýchlo a správne.

Certifikácia modelu kybernetickej bezpečnosti

Rámec Cybersecurity Maturity Model Certification (CMMC) bol vytvorený s cieľom posúdiť schopnosť organizácií, ktoré vykonávajú funkcie pre Ministerstvo obrany USA

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

(Department of Defense - DoD), chrániť vojenský dodávateľský reťazec pred narušeniami alebo stratami v dôsledku incidentov kybernetickej bezpečnosti. Porušenia bezpečnosti súvisiace s informáciami DoD naznačili, že normy NIST neboli dostatočné na zmiernenie rastúceho a vyvíjajúceho sa prostredia hrozieb, najmä zo strany aktérov hrozieb národných štátov. Aby spoločnosti dostali zmluvy od ministerstva obrany, musia byť tieto spoločnosti certifikované. Certifikácia pozostáva z piatich úrovní s rôznymi požadovanými úrovňami v závislosti od stupňa bezpečnosti požadovaného projektom.

CMMC certifikuje organizácie podľa úrovne. Pre väčšinu domén existuje päť úrovní, avšak pre reakciu na incident sú len štyri. Čím vyššia je úroveň certifikácie, tým spôsobilejšia je schopnosť organizácie v oblasti kybernetickej bezpečnosti.

- Úroveň 2 – Vytvorte plán reakcie na incident, ktorý nasleduje po procese NIST. Detegujte, nahlasujte a priorizuje udalosti. Reagujte na udalosti podľa vopred definovaných postupov. Analyzujte príčinu incidentov s cieľom zmierniť budúce problémy.
- Úroveň 3 – Dokumentujte a oznamujte incidenty zainteresovaným stranám, ktoré boli identifikované v pláne reakcie na incidenty. Otestujte schopnosť organizácie reagovať na incidenty.
- Úroveň 4 – Využite znalosti o taktike, technikách a postupoch útočníka (TTP) na zdokonalenie plánovania a vykonávania reakcie na incidenty. Vytvorte operačné centrum kybernetickej bezpečnosti (SOC), ktoré umožňuje schopnosť reakcie 24/7.
- Úroveň 5 - Využívajte akceptované a systematické techniky počítačového forenzného zhromažďovania údajov vrátane bezpečnej manipulácie a uchovávania forenzných údajov. Vyvíjajte a používajte manuálne a automatizované reakcie v reálnom čase na potenciálne incidenty, ktoré sa riadia známymi vzormi.

NIST Životný cyklus reakcie na incident

NIST definuje štyri kroky v životnom cykle procesu reakcie na incident, ako je znázornené na obrázku nižšie.

- Príprava – Členovia CSIRT sú vyškolení v tom, ako reagovať na incident. Členovia CSIRT by si mali neustále rozvíjať znalosti o vznikajúcich hrozbách.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

- Detekcia a analýza – prostredníctvom nepretržitého monitorovania jednotka CSIRT rýchlo identifikuje, analyzuje a overuje incident.
    - Prekurzor – Toto je znak toho, že v budúcnosti môže dôjsť k incidentu.
    - Indikátor – Toto je znamenie, že k incidentu už mohlo dôjsť alebo v súčasnosti prebieha.
- Potlačenie (angl. Containment), odstránenie (angl. eradication), a obnova (angl. recovery) – CSIRT implementuje postupy na potlačenie hrozby, odstránenie vplyvu na organizačné aktíva a použitie záloh na obnovu údajov a softvéru. Táto fáza sa môže vrátiť k detekcii a analýze s cieľom získať viac informácií alebo rozšíriť rozsah vyšetrovania.
- Činnosti po incidente – CSIRT potom dokumentuje, ako sa incident riešil, odporúča zmeny pre budúcu reakciu a špecifikuje, ako sa vyhnúť aby sa podobný incident opakoval v budúcnosti.

Hardening na základe lekcií

Po vyriešení závažného incidentu by mala organizácia usporiadať stretnutie zainteresovaných strán s cieľom preskúmať efektívnosť procesu riešenia incidentov a identifikovať potrebné sprísnenie existujúcich bezpečnostných kontrol a postupov.

Zhromažďovanie a uchovávanie údajov o incidentoch

Vďaka stretnutiam zainteresovaných strán možno zozbierané údaje použiť na určenie nákladov na incident z rozpočtových dôvodov, ako aj na určenie efektívnosti CSIRT a na identifikáciu možných bezpečnostných slabín v celom systéme. Zbierať je potrebné tie údaje, ktoré možno použiť na definovanie a spresnenie procesu riešenia incidentov.

V každej organizácii by mala byť zavedená politika, ktorá uvádza, ako dlho sa uchovávajú dôkazy o incidente. Dôkazy sa často uchovávajú mnoho mesiacov alebo rokov po incidente. V niektorých prípadoch môžu predpisy a smernice nariadiť obdobie uchovávania. Toto sú niektoré z rozhodujúcich faktorov pre uchovávanie dôkazov:

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

- Trestné stíhanie – ak bude útočník stíhaný z dôvodu bezpečnostného incidentu, dôkazy by sa mali uchovávať až do ukončenia všetkých právnych krokov. Pri právnych úkonoch by sa žiadny dôkaz nemal prehliadať ani považovať za bezvýznamný. Zásady organizácie môžu uvádzať, že žiadne dôkazy týkajúce sa incidentu, ktoré boli spojené s právnymi krokmi, nesmú byť nikdy vymazané ani zničené.
- Typ údajov – organizácia môže uviesť, že určité typy údajov by sa mali uchovávať počas určitého obdobia. Položky, ako je e-mail alebo text, môže byť potrebné uchovávať iba 90 dní. Je možné, že dôležitejšie údaje, ako sú údaje použité pri reakcii na incident (ktoré neboli právne stíhané), bude potrebné uchovávať tri roky alebo dlhšie.
- Náklady – Ak je potrebné skladovať veľa hardvéru a pamäťových médií na dlhú dobu, ich skladovanie sa môže predražiť. Pamätať je potrebné aj na to, že ako sa technológie menia, musia byť uložené aj funkčné zariadenia, ktoré budú schopné používať zastaraný hardvér a pamäťové médiá.

Požiadavky na podávanie správ a zdieľanie informácií

Právny tím by mal konzultovať vládne nariadenia, aby presne určil zodpovednosť organizácie za nahlásenie incidentu. Okrem právnych požiadaviek a úvah zainteresovaných strán NIST odporúča, aby organizácia koordinovala s organizáciami podrobnosti o incidente. Organizácia by napríklad mohla zaznamenať incident do databázy komunity VERIS.

Zoznam použitej literatúry

[1] Damoglu Burak, ‘Introduction to Security Operations Center | by Burak Damoglu | Medium’, Sep. 25, 2020. https://medium.com/@BurakDamoglu/introduction-to-security-operations-center-73e2e50f3ba7 (accessed Mar. 13, 2023).
[2] ‘Course: 2022_CyberOps’, 2020. https://lms.netacad.com/course/view.php?id=1418088 (accessed Mar. 29, 2023).
[3] Tyagi Aakanksha, ‘Role And Responsibilities of a SOC Analyst - InfosecTrain’, May 17, 2021. https://www.infosectrain.com/blog/role-and-responsibilities-of-a-soc-analyst/ (accessed Mar. 15, 2023).
[4] ‘Ticketing process - IBM Documentation’, Mar. 03, 2021. https://www.ibm.com/docs/en/sss/3.1.1?topic=siteprotector-ticketing-process (accessed Mar. 15, 2023).
[5] Carklin Nicolette, ‘Network Security Monitoring: A Complete Guide’, Feb. 07, 2022. https://www.parallels.com/blogs/ras/network-security-monitoring/ (accessed Mar. 15, 2023).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

[6] Ploštica Marek, ‘Simulátory počítačových sietí – analýza II’, Bakalárska práca, Žilinská univerzita v Žiline , 2021.
[7] Čulík Štefan, ‘Prehľadová analýza dostupných nástrojov pre mapovanie prepojení a vizualizáciu zariadení v sieti’, Bakalárska práca, Žilinská univerzita v Žiline , 2022.
[8] Husová Simona, ‘Implementácia bezpečnostných opatrení pre zmiernenie rizík pri poskytovaní IaaS služieb v akademickom prostredí’, Diplomová práca, Žilinská univerzita v Žiline , 2022.
[9] ‘69/2018 Z.z. - Zákon o kybernetickej bezpečnosti a... - SLOV-LEX’. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/ (accessed Jan. 19, 2021).
[10] ‘362/2018 Z.z. - Vyhláška Národného bezpečnostného úradu’. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/362/ (accessed May 10, 2020).
[11] ‘EDR, NDR, XDR, MDR - Different concepts of Detection &… | Nomios Group’, Sep. 26, 2021. https://www.nomios.com/news-blog/edr-ndr-xdr-mdr/ (accessed Mar. 15, 2023).
[12] ‘NOC vs SOC: Comparing Network & Security Operations Centers | Splunk’, Jan. 30, 2023. https://www.splunk.com/en_us/blog/learn/noc-vs-soc.html (accessed Mar. 18, 2023).
[13] ‘What is the Difference Between a SOC and a CSIRT? | Rapid7 Blog’, Apr. 19, 2017. https://www.rapid7.com/blog/post/2017/04/19/difference-between-a-soc-and-a-csirt/ (accessed Mar. 18, 2023).
[14] ‘What is MITRE ATT&CK: An Explainer’. https://www.exabeam.com/explainers/mitre-attck/what-is-mitre-attck-an-explainer/ (accessed Apr. 13, 2023).
[15] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, ‘Computer Security Incident Handling Guide’, Aug. 2012, doi: 10.6028/NIST.SP.800-61R2.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Príloha: Zoznam nástrojov

Vulnerability Assessment			
Názov	**Spoločnosť**	**Licencia**	**Poznámka**
Intruder	Intruder Ltd.	Proprietary	free trial 14 dní
Acunetix	Invicti Security	Proprietary	Contact for Quote
Nessus	Tenable Inc	Proprietary	free trial 7 dní
Invicti (Netsparker)	Invicti Security	Proprietary	Contact for Quote, free trial cloud only
Nexpose	Rapid7	Proprietary	free trial 30 dní
Burp Suite	PortSwigger Ltd.	Proprietary	free trial
Tripwire IP360	Tripwire	Proprietary	Contact for Quote
OpenVAS	Greenbone Networks	Open-source	
Nikto2	-	Open-source	
W3AF	-	Open-source	

HIDS			
Názov	**Spoločnosť**	**Licencia**	**Poznámka**
Security Event Manager	Solarwinds	Proprietary	
Samhain	Samhain	Open-source	
OSSEC	-	Open-source	
Wazuh	Wazuh	Open-source	Postavené nad OSSEC
Tripwire	Tripwire	Open-source	Momentálne neudržiavané
Tripwire Enterprise	Tripwire	Proprietary	Nahradilo Tripwire a je spoplatnené
NIDS			
Názov	**Spoločnosť**	**Licencia**	**Poznámka**
Snort	Cisco	Open-source	

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Zeek/Bro	-	Open-source	
Suricata	-	Open-source	
Open WIPS-NG	-	Open-source	
Sagan	-	Open-source	

EDR			
Názov	**Spoločnosť**	**Licencia**	**Poznámka**
EDR Security Service	Cynet	Proprietary	aj XDR riešenie, free trial 14 dní
Endpoint Central (Desktop Central)	ManageEngine	Proprietary	Contact for Quote, free trial 30 dní
CrowdStrike - Falcon Insight	CrowdStrike	Proprietary	free trial, EDR and XDR in a single platform
Carbon Black	VMware	Proprietary	
SentinelOne	SentinelOne	Proprietary	EDR and XDR
Symantec EDR	Broadcom	Proprietary	
Cybereason	Cybereason	Proprietary	
Cisco Secure Endpoint (AMP for Endpoints)	Cisco	Proprietary	free trial 30 dní
OpenEDR	-	Open-source	

NDR			
Názov	**Spoločnosť**	**Licencia**	**Poznámka**
Stellar Cyber	Stellar Cyber	Proprietary	NDR within XDR
ExtraHop Reveal(x)	ExtraHop networks	Proprietary	
Vectra NDR	Vectra.ai	Proprietary	
Hillstone Networks	Hillstone Networks	Proprietary	NDR, ponúka aj XDR

IronNet	IronNet	Proprietary	
Darktrace	Darktrace	Proprietary	
Lastline	Lastline	Proprietary	
Flowmon	Flowmon networks	Proprietary	Get a Quote, free trial 30 dní

XDR			
Názov	**Spoločnosť**	**Licencia**	**Poznámka**
Cynet Auto XDR	Cynet	Proprietary	aj EDR riešenie, free trial 14 dní
Cortex XDR	Palo Alto Networks	Proprietary	
Sophos	Sophos	Proprietary	Contact for quote
Symantec	Broadcom	Proprietary	
InsightIDR	Rapid7	Proprietary	free trial, „It was XDR before XDR was even a thing“ (označované aj ako SIEM)
Fidelis Elevate	Fidelis Cybersecurity	Proprietary	free trial 15 dní
Trend Micro	Trend Micro	Proprietary	free trial 60 dní
SecureX	Cisco	Proprietary	
SIEM			
Názov	**Spoločnosť**	**Licencia**	**Poznámka**
Splunk	Splunk	Proprietary	Free trial 60 dní, potom free verzia (<500MB/deň)
Exabeam Fusion	Exabeam	Proprietary	Potreba licencie
Log360	ManageEngine	Proprietary	Free trial 30 dní, potom free verzia

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

			(25 workstation, 5 log sources...)
Logpoint	LogPoint	Proprietary	Cena výpočet pomocou kalkulačky
USM	AlienVault / AT&T Cybersecurity	Proprietary	
LogRhythm SIEM	LogRythm	Proprietary	Subscription, Contact for Quote
Qradar SIEM	IBM	Proprietary	Cena na základe počtu workstations / serverov, licencie na základe memoranda s FRI
Elastic Stack	Elastic	Open-source	Bežná funkcionalita free, možnosť komerčných doplnkov
SIEMonster	SIEMonster	Open-source	Single server do 100 endpointov, plus ďalšie platené edície
OSSIM	AlienVault / AT&T Cybersecurity	Open-source	

PACKET ANALYZERS			
Názov	**Spoločnosť**	**Licencia**	**Poznámka**
Deep Packet Inspection and Analysis Tool	SolarWinds	Proprietary	Free trial 30 dní
PRTG	Passler	Proprietary	Do 100 senzorov free
Omnipeek	LiveAction	Proprietary	Free trial

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

tcpdump	-	Open-source	CLI
WinDump	-	Open-source	Klon tcpdump pre Windows
Wireshark	-	Open-source	GUI
tshark	-	Open-source	CLI verzia Wiresharku
NetworkMiner	Netresec	Open-source	
Fiddler	Telerik	Proprietary	Free trial 10 dní
Capsa	Colasoft	Proprietary	Dostupná free verzia s obmedzeniami

FLOW ANALYZERS			
Názov	**Spoločnosť**	**Licencia**	**Poznámka**
SolarWinds NetFlow Traffic Analyzer	SolarWinds	Proprietary	Free trial 30 dní
ManageEngine NetFlow Analyzer	ManageEngine	Proprietary	Dostupná free verzia
nProbe	ntop	Proprietary	Požaduje licenciu per systém
Ntopng	Ntop	Proprietary	Potreba licencie
Scrutinizer	Plixer	Nezistené	
Noction Flow Analyzer	Noction	Proprietary	Potreba licencie
Kentik	Kentik technologies	Proprietary	Free trial 30 dní
PRTG	Passler	Proprietary	Do 100 senzorov free
Nagios	Nagios	Proprietary	Free trial 30 dní

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Financované
Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY