VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

SCÉNÁŘ DO ŠKOLÍCÍ PLATFORMY BUTCA PRO PROBLEMATIKU SOC

SCENARIO FOR THE BUTCA TRAINING PLATFORM FOR SOC

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Valentýna Sadecká

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. Zdeněk Martinásek, Ph.D.

SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Valentýna Sadecká ***ID:*** 231275

Ročník: 3 ***Akademický rok:*** 2023/24

NÁZEV TÉMATU:

Scénář do školící platformy BUTCA pro problematiku SOC

POKYNY PRO VYPRACOVÁNÍ:

Hlavním cílem práce je návrh a implementace nového herního scénáře do platformy BUTCA, který bude zaměřen na výuku problematiky SOC (Security Operation Center). Analyzujte současný stav problematiky a navrhněte scénář obsahující běžné vybavení SOCu (Log managment a detekci incidentu). Implementujte architekturu SOC do platformy BUTCA a vytvořte nejméně dva scénáře různé obtížnosti (Blue team).

DOPORUČENÁ LITERATURA:

[1] SCHINAGL, Stef; SCHOON, Keith; PAANS, Ronald. A framework for designing a security operations centre (SOC). In: 2015 48th Hawaii International Conference on System Sciences. IEEE, 2015. p. 2253-2262.

[2] VIELBERTH, Manfred, et al. A digital twin-based cyber range for SOC analysts. In: IFIP Annual Conference on Data and Applications Security and Privacy. Cham: Springer International Publishing, 2021. p. 293-311.

Termín zadání: 5.2.2024 ***Termín odevzdání:*** 28.5.2024

Vedoucí práce: doc. Ing. Zdeněk Martinásek, Ph.D.

Konzultant: Michal Trtil

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Bakalářská práce se zaměřuje na problematiku Security Operation Center (Bezpečnostních operačních středisek) a návrhu herních scénářů pro jejich výuku. Obsahuje analýzu problematiky, jejich nástrojů a běžného vybavení. V praktické části jsou navrhnuty scénáře a jejich implementace do výukové platformy. Následně jsou zhodnoceny výsledky z testování výukových scénářů.

KLÍČOVÁ SLOVA

Security Operation Center, SOC, SIEM, Log managment, BUTCA, bezpečnostní analýza,

ABSTRACT

The thesis focuses on the issue of Security Operation Centers and the design of game scenarios for their teaching. It contains an analysis of the issue, their tools and common equipment. In the practical part, scenarios are proposed and implemented into the learning platform. In the end, the results from the testing of teaching scenarios are evaluated.

KEYWORDS

Security Operation Center, SOC, SIEM, Log managment, BUTCA, security analysis,

SADECKÁ, Valentýna. *Scénář do školící platformy BUTCA pro problematiku SOC*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2024, 63 s. Bakalářská práce. Vedoucí práce: doc. Ing. Zdeněk Martinásek, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Valentýna Sadecká
VUT ID autora:	231275
Typ práce:	Bakalářská práce
Akademický rok:	2023/24
Téma závěrečné práce:	Scénář do školící platformy BUTCA pro problematiku SOC

Prohlašuji, že svou závěrečnou práci jsem vypracovala samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autorky*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Ráda bych poděkovala vedoucímu bakalářské práce panu doc. Ing. Zdeněkovi Martináskovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů

Úvod

Kybernetické útoky a hrozby jsou nedílnou součástí dnešní doby a informačních technologií. Protože informační technologie jsou dnes již neodlučitelnou součástí a kritickými body pro fungování naší společnosti zasahující do všech oblastí našeho každodenního života, je nezbytné zabývat se jejich obranou a ochranou.

Kybernetická bezpečnost se nemusí vždy rovnat penetračnímu testování, nebo snaze proniknout do systému skrz zranitelnosti nebo lidskou chybu. SOC (Security Operation Center) jsou bezpečnostní centra dohlížející na bezpečnost technologií. Analytici vyšetřující probíhající události a slabá místa v zabezpečení jsou klíčovými aspekty pro rychlou reakci na incidenty, obranu proti útokům a zmírnění jejich dopadu.

Odborníci na informační bezpečnost v oblastech monitoringu jsou nedocenitelnou součástí, protože stojí v první linii, kdy mohou identifikovat právě probíhající útok nebo předejít fatálním důsledkům jako je zničení systémů, krádeži dat nebo citlivých informací.

Příkladem může být phishingový útok, jehož podstatou je získání citlivých informací tím, že se vydávají za důvěryhodnou entitu třeba skrz email. Nástroje SOC detekují podezřelou událost a analytici provedou vyšetření, zda email obsahuje neobvyklé odkazy, přílohy či domény, zkomolenou emailovou adresu, podezřelé požadavky a další znaky phishingových útoků. Mohou provést hlubší analýzu odkazů, varují uživatele či zákaznické firmy, spolupracují s jinými IT týmy, aby blokovaly podezřelé emailové adresy a domény. Pokud byl útok úspěšný, analyzují rozsah způsobených škod.

První část práce se věnuje principů SOC a jejich nástrojům. Druhá část se zabývá návrhem scénářů, jejich implementaci a testování, aby se mohly stát praktickým nástrojem pro výuku. Cílem práce je navrhnout dva výukové scénáře, které pomohou pochopit principy SOC, jejich implementace a fungování, na kterých lze dále stavět znalostní a kompetenční dovednosti.

Cíle práce

- Analýza současného stavu SOC.
- Návrh architektury scénářů pro výuku.
- Návrh a implementace dvou scénářů do výukové platformy.
- Otestování scénářů reálnými hráči.
- Vyhodnocení výsledků.

1 Security Operation Center (SOC)

Security Operation Center, také známá jako SOC, je centralizovaný způsob kybernetické ochrany, jež kombinací postupů, technologií a lidských zdrojů monitoruje, vyšetřuje a reaguje na potencionální rizika, bezpečnostní incidenty a události. Komplexní struktura zajišťuje, aby se dosáhlo uspokojivého výsledku, kterého by pouze s jednotlivými a oddělenými entitami nebylo možné dosáhnout. [4]

Důležitou pozici mají bezpečnostní analytici a experti na kybernetickou bezpečnost, jež pomocí nástrojů sbírají informace, vyhodnocují riziko a reagují na něj odpovídajícím způsobem. Odbornost analytiků, jejich znalosti a případný trénink je tak klíčovým prvkem. [1]

Centrálním nástrojem pro shromažďování informací je nejčasněji užíván SIEM (Security Information and Event Manager), jež sbírá data nejčastěji ve formátů logů a analyzuje je podle definovaných pravidel navržených tak, aby co nejlépe detekoval možná rizika a incidenty. Jeden z účelů je vytvořit automatizovaný systém, který varuje SOC tým, pokud nastane definovaný scénář.[7]

Jedním z možných nástrojů je také log manager. Ten však nesbírá informace jen o bezpečnosti, resp. není jeho primární funkcí shromažďovat bezpečnostní data a vyhodnocovat je, ale zabývá se shromažďováním a jejich uchováváním, případně efektivním vyhledáváním v logách. [8]

V kybernetické bezpečnosti rozlišujeme rozdíl mezi bezpečnostními incidenty a bezpečnostními událostmi. V České Republice je upřesňuje definici §7, Zákona o kybernetické bezpečnosti. [9]

Bezpečnostní událost definuje zákon jako: *"kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací."* Ve své podstatě se tak jedná o pokusy o narušení bezpečnosti, zatím však nedošlo k jejímu porušení, pouze hrozí tato možnost.

Bezpečnostní incident je pak definován jako: *"Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.* Lze tedy říct, že událost, která úspěšně porušila bezpečnost se stává bezpečnostním incidentem.

Je žádoucí aby SOC odhalil možný útok, nebo porušení zabezpečení už na úrovni události, aniž by došlo k k bezpečnostnímu incidentu. Nutno však podotknout, že se událost a incident občas zaměňují nebo nejsou jasně definované v používaných nástrojích jako např. v Azure Sentinelu. [17] Přesto je ale potřeba tyto dva pojmy rozlišovat, například při důkazním zajišťování.

Dalším důležitým a často užívaným pojmem nejen v rámci SOC, ale v celé řadě IT služeb poskytujíc zákazníkovi dohled, opravu nebo správu systémů a zařízení, je **eskalace**, čímž se rozumí předání řešeného problému od jednoho pracovníka k druhému pracovníkovi, v případě že první pracovník jej nemůže vyřešit. [1]

1.1 Implementace SOC

Celkem by mělo být pět základních funkcí, tak aby SOC poskytovalo efektivní kybernetické zabezpečení organizacím. Implementace SOC se může lišit dle přístupu nebo potřeby. Například velmi často bývá implementován spolu s NOC (network operation center)[2], které na rozdíl od SOC monitoruje dostupnost služeb. Jejich implementace je však velmi podobná a často se v některých místech protíná. Mezi základní důležité funkce SOC podle zdroje [1], na kterých SOC stojí a měl by je pokrýt jsou:

- Inteligenční rámec
- Rámce základního zabezpečení
- Monitoring
- Penetrační testování
- Forenzní zajištění

Inteligenční rámec

Je rámec v jádru velmi podobný CERT (Computer Emergency Responce Team). Tato část obsahuje kompetentní a zkušení odborníci, jež komunikují ve vnitřním prostředí mezi sebou a jinými týmy, ale i s vnějšími subjekty - odborníky, organizacemi, vnějšími týmy a další. Analyzují vzorce hrozeb a výsledky monitorování, definují pravidla pro filtrování událostí a dávají pokyny operačnímu a bezpečnostnímu personálu. [1]

Základního zabezpečení

Analytici SOC pro základní zabezpečení dohlížejí na provozní procesy pro zabezpečující servery, operační systémy a síťové komponenty a provádějí skenování zranitelnosti a dodržování předpisů, aby ověřili dodržování pokynů pro zabezpečení. Kromě toho vyhledávají známé zranitelnosti a ověřují udržovanou úroveň zabezpečeni na základě aktuálních pokynů k aktualizacím s vysokou prioritou a zabezpečením. Tato funkce také dohlíží na nastavení a provozní efektivitu ochrany koncových bodů (např. antivirus), firewallů, Intrusion Detection and Protection System (IDS/IPS), Public Key Infrastructure (PKI) atd. [1]

Monitoring

Monitorovací funkce v SOC má za úkol dohlížet data proudící v síti a pokouší se detekovat anomálie v síťové komunikaci. Větší objem logovacích dat a signálů jsou uchovávaný, filtrovány a tříděny skrz sady dynamických pravidel k nalezeních případných hrozeb.[1] Jeden z hlavních úkolů je nastavit SIEM tak, aby detekoval a upozornil pouze na relevantní události a incidenty. [7]

Penetrační testování

Penetrační testy se používají jak jako nedílná součást vývoje zabezpečovací služby, tak v rámci provozního prostředí. Penetrační test může určit, jak je systém připravený na útok - zda je možné prolomit obranu systému, která obrana byla prolomena a jaké informace lze ze systému získat; [1]

Forenzní zajištění

Analytici SOC jsou zkušení v hledání podrobností v datovém provozu a v infrastruktuře dat sesbíraných z logů. Pokud je vyžadována forenzní vyšetřování od povolaných úřadů, tito analytici pomáhají při shromažďování elektronických důkazů a jejich úschovy tak, aby se neporušil řetězec důkazů. [1]

Existuje i mnoho dalších rámců, které se používají v SOC a záleží na organizaci, jak je implementuje. Mnohé z nich nejsou pevně rozdělené, například analytici L1 na monitoringu mohou provádět prvotní odpověď na incident - tedy základní a první kroky při řešení incidentu a události, některé z nich mohou hned vyřešit oni, nebo je eskalují k analytikům L2 a L3. [3]

1.2 Úrovně v SOC týmu

Kromě předchozího rozdělení podle rámců, lze dělit úrovně SOC podle úrovně potřebného vzdělání, stupně zaučení, zkušenosti, specializace[3], a ceny takového člena týmu, které můžeme vidět i v již zmíněných rámcích. [1] Například pro osobu v prvním, inteligenčním rámci, je potřeba větší odbornosti a vzdělání než v monitorovací části, bude pro firmu tedy i dražší.

Podle tohoto lze SOC analytiky dělit na tři úrovně. Mnohé certifikační kurzy a školení se řídí podle těchto úrovní od úrovně 1 až po úroveň 3. Vělká část školení probíhá pro juniorní pozice jako je L1 v rámci monitoringu, identifikaci a řešení incidentů, analýzy a mnoho dalších. Pro seniorní pozice jako L2 a L3 probíhá spíše specializovaný trénink zaměřený na konkrétní oblasti[4]

úroveň 1.

Pracovníci, označována taky jako L1 (Layer 1) analytici, jsou odpovědní za třídění bezpečnostních incidentů a určování jejich závažnosti. To zahrnuje identifikaci zdroje incidentu, jeho rozsahu a posouzení dopadu. Poskytují počáteční reakci k incidentu jako je prvotní opatření a následnou eskalaci do vyšších úrovních. Pokud analytik první úrovně usoudí, že je potřeba podrobnějšího vyšetření, shromáždí co nejvíc možných informací a eskaluje je dál na analytiky druhé úrovně.[4]

úroveň 2.

Analytici 2. úrovně resp. L2 jsou zodpovědní za vyšetřování bezpečnostních incidentů a určení jejich hlavní příčiny. Může se jednat o analýzu protokolů, síťového provozu a dalších zdrojů dat. Poskytují také podrobné zprávy o incidentech a doporučení jejich řešení či nápravě. [4]

úroveň 3.

L3 Analytici proaktivně vyhledávají hrozby a zranitelnosti v systémech, což též vyžaduje analýzu protokolů, síťového provozu a dalších zdrojů dat za účelem identifikace hrozeb. Tak též podávají podrobné zprávy a doporučení k nápravě. Jejich reakce na incidenty bývají komplexnější. Kromě toho prohledávají forenzní a telemetrická data, zda neodhalí hrozby jež softwarová kontrola a sběr dat nemusel identifikovat, označována jako threat hunting. [4]

úroveň 4.

Některé zdroje [4] mluví i o čtvrté úrovni v SOC týmu a to o managementu. O osobě nebo skupině osob, které se starají o fungování předchozích úrovní, komunikaci napříč týmy, organizací a vedení. Tyto osoby by měli, kromě managerských kvalit, mít i odborné znalosti a zkušenosti z předchozích úrovních.

2 Log Managent

Log jsou záznamy, respektive soubory, ve kterých se shromažďují informace o systému a aplikacích. V IT jsou často používány při zjišťování problémů, testování, vývoji aplikací, zabezpečování systémů a dalších. [8] Zaznamenávají chyby, zprávy z aplikací, události jako je přístupy do aplikací, transakce v aplikaci (např. databázích), aktivity na serveru. Existují [13]:

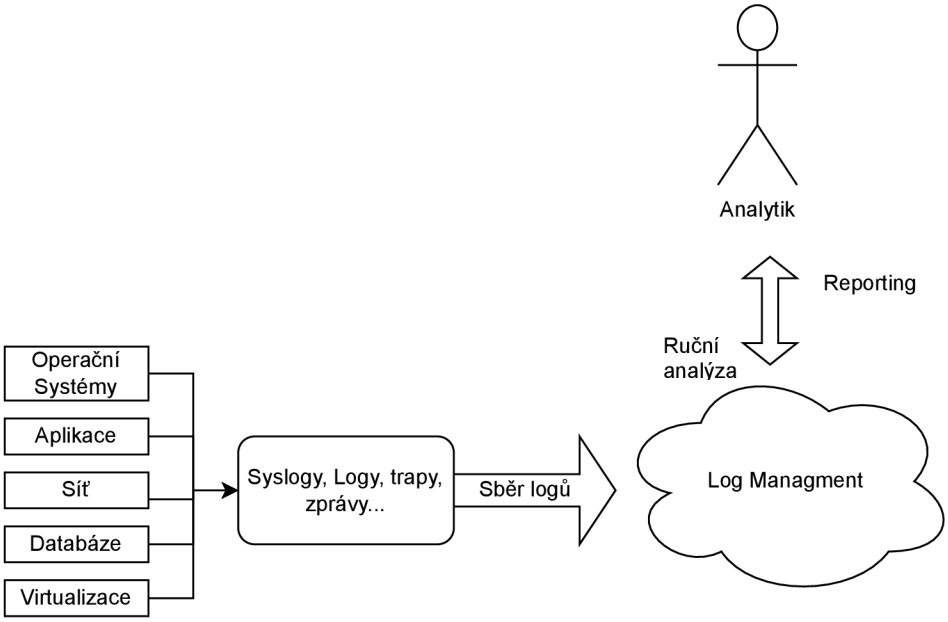
- **Eventové logy** - vysokoúrovnostní logy, jež zaznamenávají síťový provoz a využití jako jsou nesprávné pokusy o zadání hesla, přihlašovaní a události v aplikacích.
- **Serverové logy** - jedná se o soubory, do kterých se zapisují akce na určitém serveru, po určitou dobu.
- **Systémové logy** - Také známé jako Syslogy, jsou záznamy událostí, ke kterým dochází v operačním systému, jako jsou spouštění, úpravy, neočekávané vypnutí, selhání, varování, a kritické události. Generují je Windows, Linux i macOS.
- **Autorizační logy a logy přístupu (Acess)**- obsahují seznam osob nebo botů, kteří přistoupili do konkrétního programu nebo souborů.
- **Logy změn** - Záznam změn všech úprav provedených v aplikacích nebo souborů v průběhu času
- **Dostupnostní (Avaliability) logy** - ukládá výkon systému, dobu provozu a dostupnosti.
- **Zdrojové logy** - Potíže s připojením a omezením kapacity
- **Bezpečnostní logy** - obsahují informace o provozu systému, souborů nebo aplikací, které odpovídají bezpečnostním profilům např. ve firewallu.

Správa logů, nebo taky log management, je neustálý proces shromažďovaní, ukládání, zpracování, syntézy dat a analýzy ze systémů, aplikací a zařízení za účelem optimalizace výkonu systému, identifikace technických problémů, lepší správy zdrojů a posílení zabezpečení. [8]

Cílem log managementu je vytvořit nástroj pro jednoduší analýzu logů, efektivní sledování událostí a správu logů za účelem jednoduší interpretace záznamů primárně pro sledování bezpečnosti, diagnostiku a optimalizaci.[12]

2.1 Sběr logů

Logy se dají sbírat ze systémů, zařízení nebo programů. V rámci bezpečnosti to bývají často firewally, operační systémy, síťové prvky, aplikace, z antivirových a bezpečnostních nástrojů a mnoho dalších.[8] Logy jsou tak uloženy v místní paměti.



Obr. 2.1: Struktura sběru logů.

Některé aplikace nebo zařízení mohou logy posílat přímo na určený server pro zpracování logů, bez dodatečné instalace logovacího agenta.

Pokud zařízení takovou možnost nemá, používají se **agenti**. To je mechanismus resp. program, který je uložený v zařízení, a vygenerované logy poté pošle do centrálního serveru. Výhoda tohoto užití je možnost filtrace a načasování jejich sběru a odesílání, aby neúměrně nezatěžovali síť. [5]

Operační systémy od Windows mají možnost užití WMI (Windows Managment Instrumentation) [10], která poskytuje standardizovaný způsob pro sběr a správu logů ve svém systému. Není ovšem uzpůsoben pro jejich odesílání na server a je při jeho užití s tímto počítat

SNMP je příkladem jak sbírat data o stavu zařízení za pomoci protokolů. [8] Jedná se o protokol Simple Network Management Protocol a je tedy užívaný pro správu a monitorování sítě v reálném čase. Povolený SNMP agent na zařízení je upozorněn vždy, když dojde k nějaké události a pošle je SNMP trapem do kolektoru. Dalšími protokoly je Syslog, nebo posílání logů přes zabezpečený HTTPS protokol.

2.2 Ukládání logů

Významnou problematikou log managementu je bezpečné a efektivní uchovávání dat z logů. Musí se zajistit, aby data byla přístupná, organizovaná a chráněna po dlouhou

dobu. Úložiště by mělo být škálovatelné, aby se dalo v případě potřeby rozšiřovat a poskytovalo vysoký výkon při ukládání a přístupu k logům, zejména během analýzy při kritických incidentech. Organizace může udržovat vlastní fyzické servery, které si spravuje, nebo mohou využít služby cloudových úložišť. [8]

Je nutné určit politiku uchovávání, která bude určovat délku uchovávání logů, než budou archivovány nebo vymazány, tak aby se dosáhlo rovnováhy mezi právními předpisy a smluvními podmínkami, a náklady za úložiště.[8]

Organizace jsou často povinny uchovávat logy po určitou data, než mohou být smazána, aby mohla posloužit právě při forenzní analýze. Tento čas uchovávání, však mnohdy dlouze přesahuje čas jejich využití v rámci odhalování problémů a rychlý přístup k nim není prioritou. Jedním z možných prostředků pro úsporu místa v tomto případě je třeba komprimace dat, která zato snižuje rychlost přístupu k datům při jejich dekomprimaci. [12]

Logy můžou obsahovat citlivá data a informace - například IP adresy, hostname, informace o stavech zařízení... - z tohoto důvodu je zabezpečení úložiště velmi důležité. Je potřeba silná kontrola přístupu, šifrování a uchovávat auditní záznamy o změnách na úložišti, aby se zamezilo nechtěnému úniku a manipulaci.[12]

Často je vyžadována integrace s nástroji pro analýzu a monitorování, která umožní data efektivně zpracovávat a vizualizovat. Výhoda této integrace je také možnost výstrah, detekci anomálií a prediktivní analýzu v reálném čase. [8]

2.3 Formátování logů

Logy bývají shromažďovány v různých formátech, jako je třeba JSON, XML nebo CEF (Commont Event Format) [8], existuje však mnoho dalších formátů. Windows jako jeden z nejrozšířenější operační systém pro desktopové a laptopové zařízení má svůj vlastní formát logů - Windows Event Log (EVT). MacOS používá rozdílné formáty podle toho o jaké veze MacOS se jedná. Různé aplikace mohou mít vlastní formát logů. Pro efektivní analýzu je však potřeba aby byl formát jednotný.

Logy mohou být strukturované nebo nestrukturované. Mezi strukturované logy patří právě již zmiňované JSON, XML, CEF. Jedná se o logy, jež mají předem definovanou strukturu a formát. Nejčastěji fungují na bázi klíč-hodnota. Jejich začlenění do jednotné struktury je tak nejjednodušší. [14]

Výpis 2.1: Příklad strukturovaného JSON logu.

```
{
"timestamp": "2022-12-23T12:34:56Z",
"level": "error",
"message": "There was an error processing the request",
"request_id": "1234567890",
"user_id": "John_doe"
}
```

Nestrukturované logy jsou nejčastěji ve formě plaintextu. Nemají přesně danou strukturu a musí projít tzv. parsováním - tedy tříděním textu podle definovaných pravidel nebo syntaxe za účelem extrakce strukturovaných dat. Parsováním ovšem můžou procházet i již strukturované logy, pokud mají nekompatibilní strukturu. [14]

Logy často prochází agregací. Tedy sjednocováním nebo seskupováním logů podle dat nebo záznamů do jedné skupiny za účelem redukce množství dat. K agregaci může docházet podle klíčových atributů jako jsou typy událostí, IP adresy (zdrojové nebo cílové), výchozí entity, apod.; podle času a časových intervalů, podobnosti událostí, statistiky, síťových spojení, statistické korelace a mnoho dalších příznaků, které umožní dávat logy do analyticky významných a logických skupin.[12]

2.4 Analýza

Analýza logů obsahuje systematické zkoumání dat z logů s cílem získat informace o systému nebo službě, identifikovat vzorce a detekovat anomálie, a získat cenné znalosti pro budoucí analýzy. [8] Díky tomu se lze rozhodovat o dalších postupech, optimalizovat výkon a zabezpečení, zajistit plynulý provoz ve spravované sítě, případně pomáhat při odstraňování závad. Součástí analýzy může být i jejich formátování do jednotné formy a jejich agregace, ačkoliv jsou v této práci probrány odděleně.

Filtrování je užitečný nástroj použitý pro možnosti vyhledávání, ve formě dotazů, které umožňují třídit velké množství logů podle klíčových atributů - klíčová slova, časová období, IP adresy,...- k určení relevantních dat.

Používá se korelace a rozpoznávání vzorců, která pomáhá rozpoznávat vztahy mezi logy a odhaluje případná skrytá spojení a poskytuje hlubší náhled do systému. [15]Nastavují se výstrahy pro předem definované podmínky s monitoringem v reálném čase, což umožňuje včas varovat bezpečnostní a operační týmy.

Některé systémy do své analytické praxe zahrnují i algoritmy strojového učení, které pomáhají automatizovat odhalování neobvyklých aktivit a bezpečnostních hrozeb. Cílem je zkrátit dobu řešení a reakce na incident. [12] Je však nutné podotknout,

že analýza logů v Log Managementu není primární součástí, ale nadstavbou, která je již ovšem ve spoustě nástrojů zahrnuta.

2.5 Rozdíl mezi Log Managmentem a SIEM

Log Management se primárně zabývá sběrem logů, ukládání a uchování, případně přístupem k nim, tříděním a obecně správou logovacích dat z určených zdrojů v systému. Účelem je uchovat logy pro účely auditu, monitoringu, analýzu, ať bezpečnostní nebo technickou, a dodržení zákonných podmínek v centralizovaném úložišti.

V praxi spousta Log Managementových nástrojů poskytuje minimálně základní analýzu, filtrace a nástroje pro korelaci, jejich rozsah však je daleko menší než je požadováno u SIEM a zaměřený na vyhledávání a seskupování informací. Hlubší analýza bude v rámci Log Managementu probíhat spíše za účasti analytika. Některé nástroje mohou poskytovat i varování při bezpečnostní události a tak se přibližovat blízko SIEM.

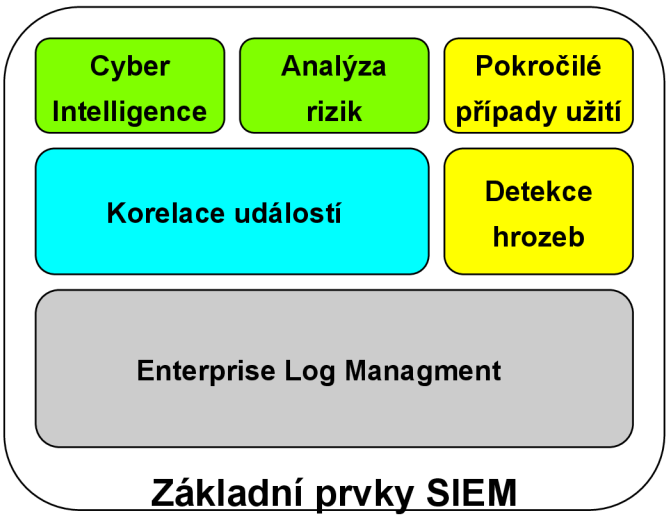
SIEM je nástroj zaměřený přímo na vyhledávání bezpečnostních událostí, na rozdíl od Log managementu jehož primární funkce je jiná. SIEM přistupuje k Log Managementovému nástroji nebo jej v sobě má přímo integrovaný a provádí nad ním složitější a hlubší bezpečnostní analýzu dat, korelace, detekce anomálií a generuje z nich bezpečnostní alerty. Mimo to je SIEM většinou plně automatizovaný systém a to včetně automatizované reakce na incidenty nebo možnosti definování pravidel pro generování alertů, aby mohlo k reakci dojít v reálném čase.

Log Management lze použít pro hledání hrozeb, analýzu a generování alertů, takové řešení však vyžaduje daleko více práce, zdrojů a času. Pokud pracujeme v rámci rozsáhlých sítí a systémů, je SIEM, který v sobě už Log Management obsahuje, daleko lepším řešením a to i za cenu vyšších financí.

3 Security Information and Event Manager

Jedná se o nástroj, respektive řešení zabezpečení organizace, který shromažďuje velké množství dat, nejčastěji formou logů, které svými nástroji analyzuje a vyhodnocuje reakce. Tento nástroj je často referován krátce jako SIEM. [16]

Pokud data vykazují znaky známé bezpečnostní hrozby, útoku, nebo porušení zabezpečení může poskytnout automatizovanou reakci pro zabezpečení, případně první kroky v analýze. Tyto data jsou stahována z koncových zařízení, aplikací, cloudu, serverů nebo síťových prvků a posílána do SIEM. Poskytuje tak přehled o aktivitách a událostech v síti, včetně koncových zařízení, a umožňuje rychlou reakci na kybernetické útoky a hrozby. Podobným, ne však stejným je SEM (Security Event Manager) nebo SIM (Security Information Manager). [7]



Obr. 3.1: Základní prvky SIEM. [7]

SEM je správa událostí zabezpečení, čili monitorování a analýzy událostí a zabezpečení v reálném čase, který řeší hrozby, identifikuje vzorce případně zajišťuje reakci na incidenty. Sleduje konkrétní události a varovné signály naznačující slabé zabezpečení. [16]

SIM je správa informací, tedy proces shromažďování, ukládání a monitorování dat z událostí a aktivit pro účely analýzy. Jedná se o dlouhodobější a širší proces. SIEM je tak spojení obou principů.[16]

Na obr. 3 můžeme vidět základní stavební prvky SIEM, které by měl obsahovat. Některé, jako Log Management už byly zmíněné a vysvětlené. Na jiné, jako analýza nebo korelace se podíváme samostatně blíže.

Cyber Intelligence - Je shromažďování informací o kyberkriminalitě z celé řady veřejných, soukromých a otevřených zdrojů a následné zpracování a analýzu těchto informací. Tedy se jedná o znalost, která umožňuje předejít nebo zmírnit následkům kybernetického útoku.[7]

Korelace událostí - Určování vztahů mezi událostmi, jestli spolu souvisí, jak na sebe případně navazují. Je důležité, aby byl vytvořený silný korelační systém, protože se do něj promítají Detekce Hrozeb, Pokročilých případů užití atd.[7]

Detekce hrozeb - Jsou shromážděná pravidla, resp. základní případy použití nebo taky "use-case". Jsou založeny na pravidlech, které se poté promítají do korelací a detekuji hrozby, které přicházejí ze systému. Jsou to IDS Alerty korelované s logy webových serverů, Malwarové alerty s Firewallovými logy, apod.[7]

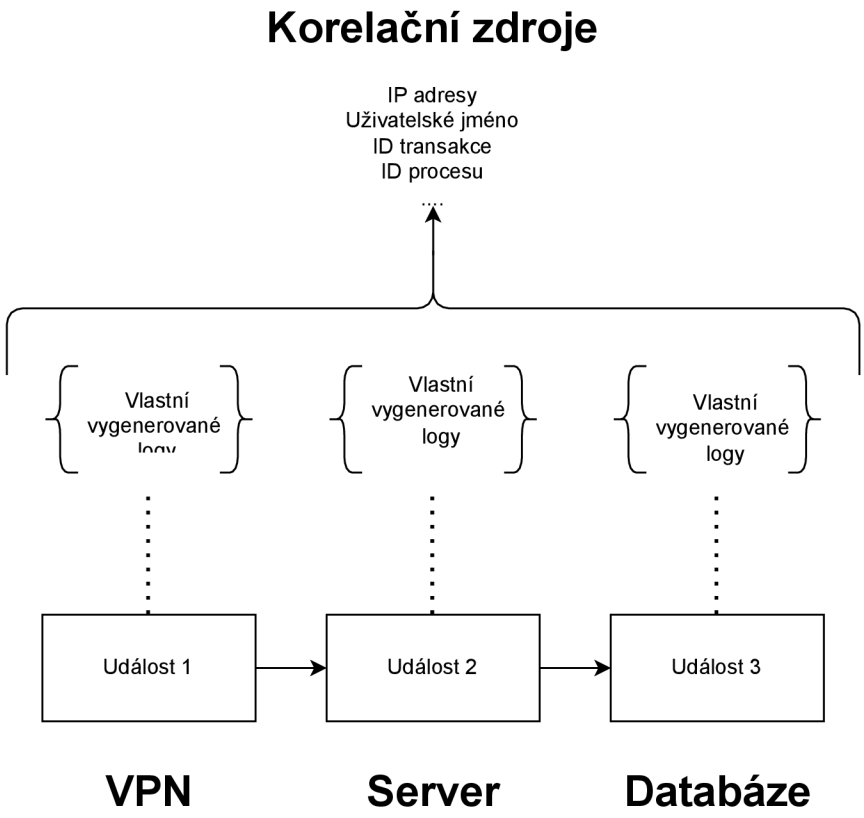
3.1 Analýza a Korelace

SIEM ve většině případů již obsahuje Log Management a některé částí jako sběr, ukládání dat nebo formátování logů tedy sdílejí. Analýza bude v rámci SIEM zaměřená více na bezpečnostní anomálie a události, navíc bývá rozvrstvena do více částí. Při analýze se hledají smysluplné vzorce v bezpečnostních datech resp. v logách. Importování výsledků do grafů a grafických zpracování, možnost sestavování dotazů nad daty. [12]

Sestavování modelů chování uživatelů s nimiž se pak srovnávají jejich případné aktivity a možné povolené přístupy s cílem určit potenciální zneužití práv a přístupu. Důležitá je zde i retrospekce - vrácení se v pomyslném čase, zkoumání dat minulých, pro stanovení běžných rizikových vzorců za delší časové období.

Korelace se definuje jako vzájemný vztah mezi dvěma procesy nebo veličinami.[6] V Log Managementu a SIEM má své významné místo v analýze. Díky ní můžeme identifikovat vzájemné vztahy mezi logy z různých zdrojů, aby se sloučil do jednoho komplexního pohledu na systém, jeho události a aktivity v něm. Zejména pak v rozsáhlém a složitém IT prostředí, kde jsou data generovány z desítek ne-li stovek zařízení a je tedy obtížné pochopit, sledovat a vyhodnocovat vzájemné souvislosti a příčiny problémů.

Součástí určování korelací je přidávání časových značek, jakmile se log dostane do systému. To ve výsledku znamená, že se všechny logy dají sledovat pro časovou korelaci, nebo určit jejich časová osa, která pak slouží při rekonstrukci událostí. Dalším krokem ve tvorbě korelace je propojování událostí. Běžným přístup pro jejich propojování je identifikace společných atributů mezi rozdílnými logy z různých zdrojů. Tyto atributy můžou být IP adresy, uživatelská jména, ID transakcí nebo názvy procesů, které mohou být použity pro určení vztahů mezi logy generované stejným problémem. [12]



Obr. 3.2: Korelace událostí [15]

Korelace nám umožňuje sestavovat řetězec událostí, sledovat tok činností, souslednost událostí a možný přerod v bezpečnostní incident nebo událost. Poskytují komplexní pohled na událostí související se zabezpečením a pomáhá odhalit složité kybernetické hrozby a útoky.[7]

Priorita výstrahy se mimo jiné určuje podle toho, zda je součástí delšího řetězce událostí. Tím se omezí pravděpodobnost, že analytik bude unaven z neustálého přísunu malých, nesouvislých bezpečnostních událostí, kde by se mohlo stát, že poté nějakou zanedbá, a místo toho mu umožní soustředit se na kritické problém v menším počtu. [15]

Kromě toho, korelace pomáhá při zjišťování hlavní příčiny a zdroje, tím že určí primární událost, která se stala spouštěčem dalších událostí, které systém zaregistroval. Korelace logů tak ve výsledku umožňuje rychlejší a přesnější odezvu na událost, pomáhá spojovat data z logů a posuzuje rozsah a dopad události nebo incidentu. Existuje několik druhů korelace používaných pro hledání bezpečnostních událostí.

[7]

Korelace podobnosti

Spočívá v porovnávání jednoho alertu resp. vyšetřované sady dat, s jinými alerty [6], nebo skupinou alertů, které již proběhly nebo byly importovány. Algoritmus se snaží je během času seskupovat a používat je pro vyvolání varování. Výhoda je, že tato metoda nevyžaduje přesnou definici typů útoků. [7]

Znalostní korelace

Jedná se o korelaci s nadefinovanými pravidly. Vyžaduje tedy předchozí znalost a vytvoření pravidel. Korelace nastane za splnění přesných podmínek. Proto je potřeba pravidelná aktualizace báze znalostí o útoku.[7]

Zástupcem tvorby těchto korelací, je vytváření pravidel, u kterých je potřeba znalost a porozumění útoku. Jedná se také o nejčastější formu nastavení korelací se kterou se v SIEM lze setkat. Můžeme se podívat na příklad Výpis 3.1, kde je příklad formy korelačního pravidla pro bruteforce attack, kde se srovná počet pokusů o přihlášení v daném čase a pokud splní podmínky, vyvolá alert. [15]

Výpis 3.1: Příklad korelačního pravidla; pseudokód

```
1 If system.detection = Event1
2 where Event1=(failed logons count > N)
3 then alert=(bruteforce attack)
```

Dalšími příklady, může být pravidlo, kdy se uživatel přihlašuje ke svému účtu v nezvyklý čas ve tři ráno a pokouší se opakovaně dostat do administrátorsky spravovaných částí systému. Nebo přijde email s nezabezpečeným odkazem, který se po otevření snaží v systému spustit skript. Fakt, že takové událost spustí alert, ale ještě neznamená, že se skutečně jedná o bezpečnostní událost. Od toho je potřeba vyšetření bezpečnostním analytikem.

statistická korelace

Nevyžaduje předchozí znalost útoku ani definování pravidel. Místo toho se používá znalost a statistika běžných aktivit. [7]

3.2 Wazuh

Wazuh je opersource SIEM, který sleduje zařízení v reálném čase. Vzhledem k tomu, že se jedná o opensource, může na něm tak pracovat komunita a jedná se o volně dostupný nástroj, který využívá jiné opensourcové nástroje. Tento fakt, je jak výhodou

tak nevýhodou. [18]

Wazuh má vše co by se od SIEM dalo v základu požadovat. Log managment, kdy sbírá a archivuje logy. Nad logy pak funguje detekce incidentů, ale obsahuje i detekci zranitelnosti zařízení, sleduje zda se zabezpečení zařízení shoduje s regulatorními požadavky nebo shromažďuje informace o zařízení jak hardwarové tak softwarové, čímž umožňuje udržovat přehled o monitorované síti.

Díky otevřenému kódu lze vše upravovat pro vlastní potřeby, které ovšem vyžaduje komplexní znalost systému a jazyků nebo kódu, které využívá.

Na rozdíl od placených řešení neobsahuje tolik nadstavbových nástrojů. Tyto nástroje nejsou pro SIEM nutné, ale zjednodušují samotné vyšetřování událostí, mohou zjednodušit správu SIEM, definování pravidel, procházení logů a dalších funkcí.

Například porovnáme-li ukládání logů s Azure Sentinelem (placený SIEM od Microsoft) [17], zjistíme, že Sentinel ukládá logy v tabulkových databázích, zatímco Wazuh ukládá logy v logový souborech, což může vést k horšímu výkonu při vyhledávání. Lze také poznamenat, že Wazuh zobrazí ve svém uživatelském rozhraní pouze logy, které se mu podařilo parsovat a odpovídají detekčním pravidlům - tedy zobrazí alerty. Pokud bychom se chtěli podívat na logy, které Wazuh nepozná, nebo nejsou alertové, musíme se podívat do souboru, ve kterém ukládá všechny logy, zatímco Sentinel má přístupnou databázi všech logů a nad nimi implementované vyhledávání. I přesto je Wazuh intuitivní a příjemný nástroj pro SIEM řešení.

3.2.1 Wazuh agent

Podle technické dokumentace [22] se jedná o multiplatformní software, který jede na endpointovém zařízení, které chceme monitorovat. Podstatné je, aby agent neovlivnil významným způsobem výkon na zařízení, kde je instalován. Je podporován na nejčastějších operačních systémech jako je Linux, Windows nebo MacOS. V průměru je potřeba 35MB RAM.

Agent jede na zařízení, které monitorujeme, a komunikuje se serverem, kam posílá data ve skoro reálném čase. Pro komunikaci se serverem se používá autentizovaný šifrovaný kanál.

Tento agent provádí několik důležitých funkcí [22]:

- **Sběr logů** - z log souborů sbírá zapsané logy a posílá je na server, kde se k nim přidají informace jako je časový otisk, kdy se log poslal, jaký agent jej poslal a další...
- **FIM (File Integrity Monitoring)** - agent monitoruje určené soubory, které se nastaví v konfiguračním souboru a v případě, že se změní jejich sumcheck, pošle upozornění.

- **System monitory** - agent sbírá data o systému. Hardwarové i softwarové nastavení.
- **Active response** - přes agenta lze vyvolat automatizovanou reakci na události jako je například restart, zablokování uživatele, blokování IP adresy...
- **Cloud security a Container Security** - kromě samotných endpointů může Wazuh monitorovat bezpečnost i u Cloudových služeb a konteinerů
- **Security Configuration Assessment** - proces ověřování, zda všechny systémy vyhovují sadě předem definovaných pravidel týkajících se nastavení konfigurace a schváleného použití aplikací.
- **Comand execution** - Skrz konfigurační soubor může pravidelně Wazuh spouštět skripty a příkazy a podávat o jejich provedení správu do serveru.
- **Malware Detection** - jedná se o soubor detekční pravidel a technik, které rozpoznají různé druhy malwaru a podají o nich správu na serveru. Mimo jiné, lze nastavit i automatickou reakci na jejich odstranění.

Ne vždy je možné na zařízení posílat logy skrz agenta,tato situace může mít dvě řešení. Použít zařízení s agentem jako prostředníka, kdy stahujeme logy do monitorovaného zařízení a posíláme jej skrz agenta do serveru. Tento způsob lze uplatnit, pokud nechceme nebo nemůžeme použít server jako sběrný uzel.

Druhý způsob je bez instalování dalších softwarů nebo agentů. Server vytvoří SSH spojení se zařízením, na kterém nelze agenta nainstalovat, stahuje z něj logy, monitoruje složky a soubory nebo spouští příkazy.

3.2.2 Wazuh server

Server analyzuje události, které přichází od Wazuh agentů a posílá alerty, pokud zaznamená anomálie nebo nebezpečné události. Lze skrz něj nastavovat konfiguraci agentů a monitoruje jejich stav.

Server lze nainstalovat na jednom hostovacím zařízení, nebo na několika zařízeních, které fungují jako cluster server. Cluster server je vytvářen několika servery propojených mezi sebou a tvářící se jako jedno zařízení. Toto seskupení se používá pro zvýšení rychlosti a efektivnosti. Další výhodou je spolehlivost - pokud jeden cluster vypadne, ostatní mohou zastat jeho činnost. [21]

Podle dokumentace je doporučeno, aby operašční systém, na kterém server funguje byl Linux. Doporučené distribuce a jejich verze můžete vidět v tabulce Tab.3.1

Co se týče Hardwareových doporučení, záleží na počtu agentů, které do serveru posílají data. Minimální požadavky a doporučené požadavky můžeme vidět v tabulce Tab 3.2

Dalšími parametry je velikost úložiště pro logy, ale vzhledem k tomu, že vytvořené stoje se načítají v rámci scénářů ze snapshotu a nefungují stále, nejedná se o

Tab. 3.1: Přehled doporučených distribucí Linux pro Wazuh Server [21]

Distribuce	Verze
Amazon Linux	2
CentOS	7, 8
Red Hat Enterprise Linux	7, 8, 9
Ubuntu	16.04, 18.04, 20.04, 22.04

podstatný problém. Pro demonstraci jeden agent na pracovním počítači generuje v průměru 0.04GB dat za 90 dní.

Tab. 3.2: Přehled Hardwarových požadavků pro server [21]

	RAM(GB)	CPU(cores)
Minimální požadavky	2	2
Doporučené parametry pro 1-25 agentů	8	4
Doporučené parametry pro 25-50 agentů	8	8
Doporučené parametry pro 50-100 agentů	8	8

3.2.3 Wazuh indexer

Jedná se o vysoce škálovatelný nástroj pro fulltextové vyhledávání a analýzu. Tento komponent indexuje a ukládá alerty generované serverem a umožňuje vyhledávání a analýzu dat v téměř reálném čase. [20]

Indexer, stejně jako server, lze nainstalovat na jedno zařízení a nebo ve více uzlech jako cluster, pro poskytnutí lepší škálovatelnosti, dostupnosti a výkonu. Je podporován na Linuxových distribucích stejných jako v tabulce Tab 3.1. Jeho hardwarové parametry jsou ovšem vyšší než u serveru. Doporučené požadavky pro každý jeden uzel najdeme v tabulce Tab 3.3[20]

Požadavky uložiště jsou u indexeru větší, ale ani tak se nejedná o záležitost, které by měla velký dopad při implementaci ve scénářích. Zůstaneme.li u stejného příkladu jako u serveru, tak indexer generuje pro jednu pracovní stanici okolo 1.5 GB dat za 90 dní.

3.2.4 Wazuh dashboard

Tento komponent je flexibilní webové rozhraní pro zobrazování logů událostí, analýzu a grafickou vizualizaci bezpečnostních dat. Poskytuje předem připravené řídící

Tab. 3.3: Přehled Hardwarových požadavků pro každý uzel indexeru [20]

	RAM(GB)	CPU(cores)
`Minimální požadavky`	4	2
`Doporučené parametry`	16	5

panely, které umožňují intuitivní orientaci uživatelským rozhraním.[19]

Pomocí Dashboardu můžeme procházet a vizualizovat bezpečnostní události a incidenty, zjištěné zranitelnosti, data FIM, posouzení konfiguraci, události z cloudové infrastruktury a dodržování předpisů.[19]

Dashboad je možné mít na jednom uzlu spolu s indexerem nebo samostatně na jednom uzlu. I zde je podporován jenom Linux s distribucemi v tabulce Tab. 3.1

Hardwarové požadavky můžeme vidět v tabulce Tab 3.4

Tab. 3.4: Přehled Hardwarových požadavků pro Dashboard [19]

	RAM(GB)	CPU(cores)
`Minimální požadavky`	4	2
`Doporučené parametry`	8	4

Uživatelské rozhraní jede na IP adrese uzlu a lze zobrazit v internetovém prohlížeči, standardně na portu 443. Dojde zde k výměně certifikátu se zařízením, které se připojuje. Protože se jedná o certifikát vytvořený Wazuh a není známou certifikační autoritou, bude prohlížeč hlásit nebezpečnou stránku. Tento certifikát lze vyměnit za ten od certifikační autority. Podporované webové prohlížeče jsou[19]:

- Google Chrom 95 nebo novější
- Firefox 95 nebo novější
- Safari 13.7 nebo novější

Autoři výslovně specifikují, že Explorer 11 není podporovaným prohlížečem. Webové prohlížeče, které staví na Chromiu, mohou fungovat pro zobrazování Dashboardu. Chromium je opensource prohlížeč od společnosti Google, který sdílí velkou část kódu s Google Chrom.

4 Návrh vlastních scénářů do BUTCA

Při tvorbě scénářů je potřeba brát v potaz nejen tématiku SOC, ale také jak musí být konstruovány v rámci vybrané platformy, do které je následně implementujeme.

Problematika SOC je velmi komplexní téma, které přesahuje do různých odvětví a nemá striktně nastavené hranice. Ačkoliv jsou důležitou součásti kyberbezpečnostní analytici, podstatnou část hraje také architektura.

Umět správně implementovat a nakonfigurovat nástroje a pochopit jakým způsobem tyto nástroje fungují je stejně důležité, jako pochopit podstatu analýzy, kterou analytici provádí. Optimálně nastavené nástroje dokáží ušetřit čas analytikům a snížit pravděpodobnost chyby.

4.1 Výuková platforma BUTCA

BUTCA (Brno University of Technology Cyber Arena) je technická platforma VUT určená pro výuku a trénink v oblasti bezpečnosti. [23] Před vytvoření samotných scénářů je potřeba se seznámit s platformou, ve které budou implementovány.

Scénáře na ni jsou ve formátu "Capture the flag". Hráč hledá vlajku, která je někde ukrytá nebo ji skládá z informací, které má dostupné. Když vlajku odhalí, posune se do dalšího úkolu. Uživatelské rozhraní BUTCA si lze prohlédnout na obrázku Obr. 4.1

Každý scénář se skládá z:

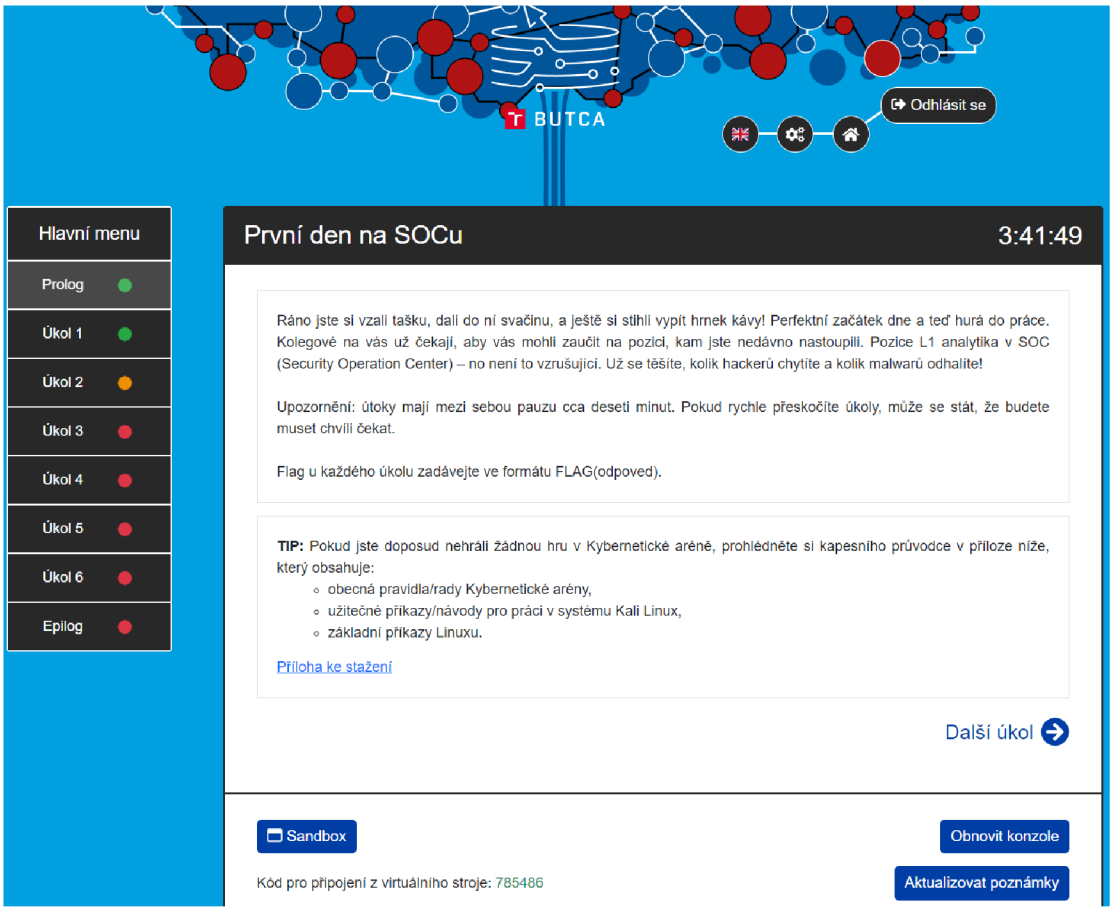
- Prolog - slouží jako úvod do hry.
- Úkoly - bodované podle náročnosti.
- Vlajky - cíl úkolu, kterého se snaží hráč dosáhnout.
- Nápověd - každý úkol má nápovědy s bodovou penalizací.
- Epilog - slouží jako zakončení scénáře.
- Závěrečný test.

Další součástí je sandbox, který obsahuje virtuální stroje, kde může uživatel plnit zadání úkolů. Tyto virtuální stroje se spouští ze snapshotu předem vložených a nastavených virtuálních strojů. Každý hráč má vlastní sandboxové prostředí.

4.2 Obecný návrh scénářů

V této části se zabýváme obecným návrhem scénářů a jejich nástrojů, na kterých potom budou stát scénáře již implementované do BUTCA.

Důležitými součásti, které scénáře musí obsahovat jsou Log Management a detekce incidentů. Tyto části můžeme rozdělit, tedy zvolit vhodný Log Manager a nad



Obr. 4.1: Scénář druhý v rozhraní BUTCA z pohledu hráče

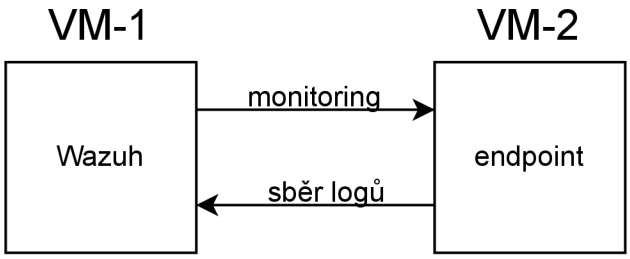
to postavit nástroj pro detekci incidentů. Druhou možností je zvolit nástroj, který obsahuje oba prvky a tím je SIEM.

SIEM je pro implementaci SOC velmi často používán a proto se nabízí jako ideálním řešení, zvlášť je-li vysoce pravděpodobné, že s ním SOC analytici přijdou do kontaktu. Pro účely práce je použit opensourcový SIEM nástroj Wazuh, který byl představen v teorii.

Pro problematiku SOC je podstatné znát jak pracují SOC analytici, ale seznámit se také s architekturou a principy se kterými fungují jejich nástroje. Z tohoto důvodů by měl být jeden scénář zaměřen na architekturu a jeden na analytickou činnost.

Na obrázku Obr 4.2 si můžeme prohlédnout návrh pro vytvoření virtuálních strojů. VM-1 zde představuje server, na kterém je nainstalovaný Wazuh, zde probíhá detekce incidentů a zpracování logů. VM-2 funguje jako endpointové zařízení, které Wazuh monitoruje a sbírá z něj logy.

Aby stroje mohly společně komunikovat v rámci sandboxu, je nejvýhodnějším řešením nastavit pro ně statické IP adresy v jedné síti. Toto nastavení umožní také



Obr. 4.2: Základní topologie virtuálních strojů pro BUTCA

jednotnou nápovědu nebo instrukce pro hráče, aniž by se musely brát rozdílné IP v potaz.

Druhý problém, kterému se předejde, je, že Wazuh agent posílá data na předem určenou IP adresu. Změna IP by znamenala, že agent nebude moct posílat data na server a komponenty se po spuštění nepropojí. Minimálně VM-1, tak bude muset mít vždy statickou IP.

4.3 Scénář 1.

Zaměření se na architekturu SOC centra nese problém v tom, že každé SOC středisko bude fungovat na jiných nástrojích i jiným způsobem. Důležité je tak zaměřit se na princip fungování, než na samotný nástroj, ačkoliv se scénář musí nástroji přizpůsobit.

Hráč by měl v tomto scénáři projít důležitými body, které jsou u SOC sdílené, ačkoliv se samotné implementace můžou lišit. Hlavním cílem je, aby hráči nasadili vlastní prostředí, které budou monitorovat.

Topologie zde zůstává stejná jako u obrázku Obr. 4.2. Ze začátku však na endpointu není nainstalovaný agent pro monitoring a tedy neprobíhá žádné posílání dat. V tabulce Tab.4.1 si lze prohlédnout souhrn úkolů a témat, pro které jsou určeny.

Některé části, například úkol 1 a úkol 2 byly přidány z praktického důvodu. První úkol je navádí k připojení se do uživatelského rozhraní. Druhý úkol se snaží předejít komplikacím při instalaci agenta, kdy je potřeba zvolit architekturu a distribuci operačního systému cílového zařízení.

4.3.1 Zadání úkolů

Tato část obsahuje už samotné zadání jednotlivých úkolů a prologu, tedy textu, který vidí už jednotlivý hráči a který je navádí k tomu, co mají dělat.

Tab. 4.1: Přehled témat 1. scénáře, kterými by měl hráč projít a jejich bodové hodnocení

	Téma	Body
`Prolog`	SOC	-
`úkol 1`	SIEM	5
`úkol 2`	Wazuh agent	10
`úkol 3`	Wazuh agent - monitoring	15
`úkol 4`	Sběr logů	15
`úkol 5`	Detekční pravidla	15
`úkol 6`	Analýza incidentu	2
`úkol 7`	Reporting	10
`úkol 8`	Automatic response	15
`-`	závěrečný test	13

Text se v herní platformě může formátově lišit. Obsahově zůstává stejným, může však být doplněním hesly pro stroje, přílohou jako je report, upozorněními ohledně načasování logů, nebo pozměněným formátem vlajky, který je jednotný pro všechny hry v platformě a měl by zůstat zachován.

Prolog

Jako stážista jste se dostali do firmy, která se mimo jiné provozuje SOC (Security Operation Center). SOC je operační středisko zaměřené na bezpečnost, které běží v režimu 24/7 a monitoruje zařízení v síti jak svoje, tak jiným organizacím, a v případě že zaregistruje bezpečnostní riziko, podezřelý event nebo bezpečnostní incident může podniknout určité kroky pro zabezpečení, předat událost na CSIRT team nebo reportuje události dané organizaci, aby sjednala nápravu.

Analytici, kteří patří do SOC, jsou nejčastěji dělení do tří kategorií:

- L1 – je obvykle zodpovědný za sledování a prvotní analýzu bezpečnostních událostí a incidentů. Vyhodnocují upozornění a rozhodují, zda je potřeba další akce nebo se jedná o „false positive“. Pokud je to nutné eskalují závažnější události do vyšších úrovní. Vedou dokumentaci.
- L2 – poskytuje hlubší analýzu v závažnějším incidentu, vyšetřování a reakce v případě pokročilých útoků, koordinují reakci s ostatními týmy nebo analytiky. Může být také zodpovědný za vytváření a udržování bezpečnostních politik, procedur a dokumentace.
- L3 – zabývají se incidenty, které se eskalují z L2. Zabývají hledáním kybernetických hrozeb – podezřelá komunikace, nedostatečné zabezpečení apod. Vy-

tváření a implementace strategií pro zlepšení bezpečnosti organizace. Školení a mentorování méně zkušených členů týmu SOC.

Protože jste ve firmě noví, dali vám tréninkové pracovní prostředí, kde si zkusíte nasazení svého vlastního monitorovacího systému pro SOC! Hodně štěstí!

úkol 1

Ve firmě používají SIEM (Security Information and Event Management) – tento nástroj jim poskytuje jak Log Management, tak detekci incidentů.

Log Managment je proces sbírání, ukládání a zpracování logů z dohlížených zařízení. Tyto logy prochází systémem pro detekci incidentů, mnohdy upravené pro potřeby firmy, a spustí varování, pokud události korelují s nastavenými pravidly.

SIEM je systém který spojuje obě tyto části právě pro potřeby bezpečnosti.

Váš první úkol je zjistit, jaký SIEM vaše firma používá a připojit se do něj pomocí prohlížeče z Wazuh1. Dashboard běží na adrese: 10.10.2.15

Flag: název používaného SIEM

úkol 2

Dostali jste se na úvodní stránku SIEM. Kromě svého serveru, na kterém funguje, zatím nesbírá žádná data. Rozhodli jste se tedy, že budete monitorovat Endpoint. K nainstalování agenta je potřeba zjistit jaká architektura a distribuce je na něm nainstalovaná.

Na úvodní stránce Dashboardu, kam jste se přihlásili najdete odkaz na instalaci agenta, který vás odkáže na návod k instalaci, můžete k němu referovat. Zatím agenta neinstalujte, ale určete potřebné parametry – resp. Architekturu a distribuci endpointu kam agenta budete instalovat.

Flag: Název architektury, na které stojí Ubuntu a jeho distribuce nainstalované na endpointu. Flag napište jako „architektura_distribuce“

úkol 3

SIEM agent slouží k monitorování koncového zařízení. Komunikuje se serverem a posílá data skrz šifrovaný tunel do serveru. Wazuh agent má několik vlastností, které nám mohou pomoci při monitorování velkého počtu zařízení.

Jeho standardním účelem je sběr logů, monitoruje systém a sbírá data o systému a jeho nastavení, detekuje malware a umožňuje vzdálenou reakci ze serveru (izolaci zařízení od sítě, blokování IP adres apod.) a mnoho dalších užitečných funkcí.

Nainstalujte agenta na zařízení podle návodu Wazuh. Ověřte si, zda je zařízení připojeno a podívejte se jaké logy vám přicházejí.

Jaká událost vám chodí každou minutu? Podívejte se na její detaily.

Flag: Z jakého souboru, který agent monitoruje, tento log přišel? Vložte pouze název samotného soubor.

úkol 4

Agent monitoruje některé logy bez potřeby nastavování. Může se však stát, že je potřeba monitorovat i jiné logové soubory nebo použít agenta k monitorování logů ze zařízení, které na sobě agenta mít nemůže z technických důvodů. Používá tak monitorované zařízení jako prostředníka.

Nutné je také podotknout, že agent nemonitoruje logy zpětně a bude do serveru posílat logy, které přijdou po zapnutí monitoringu.

Zkusíme si nastavit monitoring Apache serveru. Nejdřív je potřeba jej nainstalovat:

```
sudo apt install apache2
```

Naštěstí pro nás má Wazuh zabudovaný pravidla pro Apache, dále tak stačí jen nastavit monitoring!

Flag: Název útoku probíhající na endpointu? Zadejte malým písmenem ve formátu: nazev_utoku

úkol 5

Bezpečnostní pravidla nebo také detekční pravidla jsou definované vzory sloužící k detekci různých typů bezpečnostních událostí a hrozeb na sledovaných systémech. Tyto pravidla jsou klíčovou součástí SIEM, a tedy i SOC, protože umožňují identifikovat podezřelé nebo nebezpečné aktivity a reagovat na ně.

Existuje mnoho druhů pravidel: detekce intruzí (IDS), pravidla pro auditování systému, pro detekci škodlivého softwaru, sledování integrity souborů a další.

Podívejte se na pravidla detekce a upravte pravidlo s id: 31106 tak, aby jeho závažnost byla rovna úrovni 12. Původní pravidlo:

```
<group name="web,accesslog,">
<rule id="31106" level="10">
<if_sid>31103, 31104, 31105</if_sid>
<id>^200</id>
<description>A web attack returned code 200 (success).
</description>
<mitre>
<id>T1190</id>
</mitre>
<group>attack,pci_dss_6.5,pci_dss_11.4,gdpr_IV_35.7.d,
nist_800_53_SA.11,nist_800_53_SI.4,tsc_CC6.6,tsc_CC7.1,
tsc_CC8.1,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
</rule>
</group>
```

Referujte k dokumentaci zde: https://documentation.wazuh.com/current/user-manual/ruleset/custom.html

Group name označuje, pod jakou skupiny pravidlo spadá. Následuje hlavička pravidla, kde je id a závažnost. If_sid je označení pravidel, na které pravidlo navazuje nebo s ním souvisí nebo z něj vychází. 31103 je pravidlo, které již známe – jedná se o neúspěšný pokus o SQL injection. Id nám určuje, že při parsování logu se díváme po vráceném kódu 200 ze serveru. Mitre se odkazuje na MITRE ATTACK, což je platforma, která shromažďuje a kategorizuje různé typy strategií, technik a postupů, které používají kybernetičtí útočníci.

Po nastavení, v terminálu zadejte příkaz:

```
cat /home/endpoint/testing_logs.log >>
/var/log/apache2/access.log
```

Využijte vašeho nastavení a vyfiltrujte logy podle závažnosti alertů!

Flag: Kolik logů úrovně 12 a více přišlo do SIEM z vloženého souboru? (Vyfiltrujte pryč logy s rule.id 100010)

úkol 6

Vraťme se zpátky k útoku který, jak můžeme vidět, stále na endpointu probíhá.

L1 je z velké části odpovědný za monitoring a vyhodnocování událostí, může taky mít na starost prvotní reakce, záleží na tom, jak má organizace definované vlastní postupy a smluvní podmínky se třetími stranami.

Zaměřme se tedy na monitoring a vyhodnocování událostí. V Dashboardu je grafické zobrazení statistik, když vyfiltrujete daný útok (v tomto případě id 31103), zobrazí grafy statistiky závislé na filtrování.

Z grafů můžeme jasně vidět (hlavně z prvního a posledního), že události se objevují v pravidelném intervalu. Pokud máte problém události v grafu vidět zkuste změnit časový rozsah např. na třicet minut.

Tento vzorec nám napovídá, že útok může být prováděn pomocí skriptu. Kdyby byl útok prováděn ručně, byl by vzorec daleko nahodilejší. Stejné by to bylo, pokud by epizody přišli ve velkém množství v krátkém intervalu těsně za sebou.

Flag: Kolikrát přišla (nebo by podle statistiky mohl přijít) tato stejná událost během třiceti minut.

úkol 7

Vidíme, že události chodí neustále dokola a nevypadá to, že by v blízké době přestaly. Proto by bylo potřeba tuto událost reportovat.

Reportování je velmi důležité nejen uvnitř firmy, ale i mimo ni. Organizace tímto způsobem podává informace svým zákazníkům nebo subjektům, které dohlíží. Analytici z vyšších úrovní nebo jiné týmů použijí tuto dokumentaci jako referenci při bližším zkoumání.

Tví kolegové pro tebe jeden takový report připravili. Podívej se do přílohy a dokumentaci si prohlédni. Jedná se o prvotní report o události, jedná informace tam chybí, místo ní tam jsou jen „****“. Doplňte ji, aby byl report kompletní!

Flag: chybějící informace

úkol 8

Jedna z možností, jak reagovat na různé epizody, je možnost nastavení automatické odpovědi své vlastní, kterou si sami nastavíte, nebo defaultní, které má Wazuh v sobě už zabudované.

Zabudované odpovědi ve Wazuhu jsou například: firewall-drop, který přidá IP adresu do deny listu. Disable-account pro uživatele a zablokuje jej. Odstranění škodlivého souboru nebo třeba restart, který restartuje agenta nebo server.

Podíváme se na automatický restart agenta. Pokaždé když je provedena změna v dohlíženém souboru, musíme agenta restartovat. Normálně bychom to prováděli ručně.

Na Wazuh1 zadejte: *„vim /var/ossec/etc/ossec.conf“* - jedná se o konfigurační soubor serveru A do sekce <ossec_config> vložte tento text, který nám říká, že pokud nastane pravidlo 100009, má se provést restart na lokálním zařízení:

```
<active-response>
    <command>restart-wazuh</command>
    <location>local</location>
    <rules_id>100009</rules_id>
  </active-response>
```

Poté zadejte příkaz: *„vim /var/ossec/etc/rules/local_rules.xml“* a přidejte nové pravidlo:

```
<group name="restart,">
<rule id="100009" level="5">
    <if_sid>550</if_sid>
    <match>ossec.conf</match>
    <description>Changes made to the agent configuration file
    - $(file)</description>
  </rule>
</group>
```

Toto pravidlo se odkazuje na pravidlo 550, které se vyvolá, pokud se změní checksum nějakého souboru. Pokud se tak stane u ossec.conf, vyvolá se pravidlo 100009.

Pak zadejte: *„sudo systemctl restart wazuh-manager“* a přesuňte se na endpoint.

Zde zadejte: *„vim /var/ossec/etc/ossec.conf“* A do <syscheck> sekce vložte:

```
<directories realtime="yes">
/var/ossec/etc/ossec.conf
</directories>
```

Čímž zapnete monitoring tohoto souboru. Restartujete wazuh-agenta: *„sudo systemctl restart wazuh-agent“* a od této chvíle se bude restartovat sám. :) Zkuste si znovu otevřít soubor a změnit jej. Třeba dát do komentáře smajlíka. Vraťte se do Dashboardu a podívejte se na logy. Pokud jste vše nastavili správně, vyvolá se pravidlo 100009, 506 a 503.

Flag: hodnota rule.mitre.tactic v logu pravidla 506. Napište vše malým jako: název_taktiky

4.3.2 Závěrečný test

Odpovědí může být jedna nebo více. Správné odpovědi zde nejsou uvedeny.

Otázka 1 (2 bodů):

Log management je:

- Ukrývání citlivých informací o počítači
- Manažer jménem Log.
- Management podle ideálu LOG.
- Proces sbírání, ukládání a zpracování logů.

Otázka 2 (2 bodů):

Wazuh je:

- SIEM (Security Information and Event Management)
- Asijské jídlo
- Antivirus
- Malware

Otázka 3 (4 bodů):

Wazuh agent:

- Monitoruje koncové zařízení
- Krade přihlašovací údaje
- Odstraňuje tracking cookies
- Komunikuje se serverem skrz šifrovaný tunel

Otázka 4 (2 bodů):

Detekce incidentů je:

- Nastavování přístupových práv
- Proces porovnávání korelace logů s nastavenými pravidly
- Šestý smysl novinářů detekovat závažné události ve světě
- Šifrovaná komunikace

Otázka 5 (2 bodů):

Detekční pravidla jsou:

- Pravidla jak se chovat v laboratorním prostředí
- Postupy a pravidla, jak reagovat bezpečnostní událost
- Definované vzory sloužící k detekci různých typů bezpečnostních událostí a hrozeb
- Společností neuznávaná kapela

Otázka 5 (1 bodů):

Je “Functional Impact” součástí reportingu?

- ANO
- NE

4.4 Scénář 2.

Problematika SOC obsahuje i práci analytiků, kteří nástroje využívají a kterému se věnuje tento scénář, tedy analytické činnosti. Nástroje jsou identické s prvním scénářem. Topologie, kterou si můžeme prohlédnout na obrázku Obr 4.3 se liší.

Základní topologie je stejná, liší se však o třetí stroj, který hráč nevidí a ani k němu nemá přistup. Tento stroj slouží pro vyvolání incidentů na endpointu. V původním konceptu se měly logy vkládat skriptem na endpointu, případně pak vkládat vlajky.

Tento postup byl však nakonec odložen ze dvou důvodů. První byla možnost chyby, respektive vynechání některých událostí, které by mohly být důležité nebo by vytvořili neautentický výsledek. Druhý důvod byl, že script by byly uloženy na zařízení, kde má hráč administrátorská práva. Respektive mu v rámci hry je poskytnuto administrátorské heslo pro oba stroje, aby mohl plnit některé úkoly. Pokud by se tak dostal ke všem skriptů, mohl by odhalit flagy bez toho, aniž by prošel úkoly žádoucím způsobem.

Do topologie byl tak přidán útočící stroj "attacker", který simuluje útoky. Topologie pro tento scénář si lze prohlédnout na obrázku Obr. 4.3. Jeden útok, který je ve skutečnosti falešný poplach a je ve hře konceptován jako údržba nebo plánovaná práce, má script uložen na endpointovém zařízení.

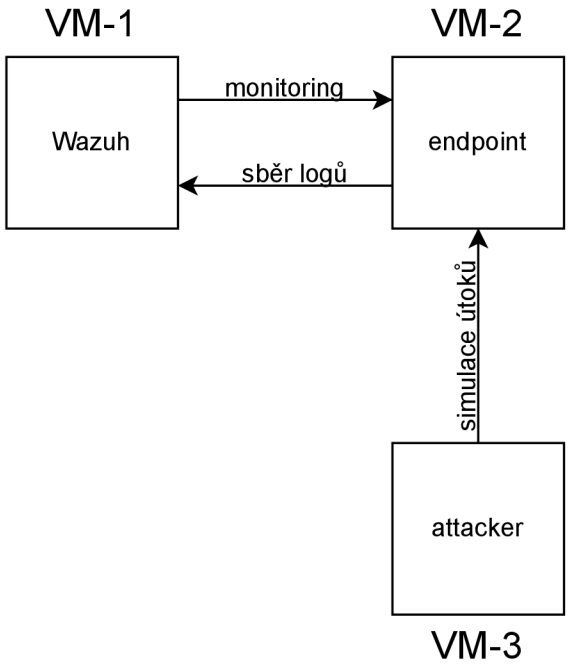
Cílem scénáře je přimět hráče aby se zamyslely nad tím, co jim události v SIEM říkají o tom, co se děje na zařízení. Pro tento účel se zvolily útoky, které jsou obecně známe a studenti s nimi velmi často přijdou do styku v průběhu studia. Mezi tyto útoky patří například brute-force nebo SQL injection.

4.4.1 Zadání úkolů

úkol 1

Sedíte si na pohodlné židli v operačním středisku a prohlížíte si příchozí události. Čas od času na vás nějaký z vašich spolupracovníků mrkne a řekne vám, co máte dělat a čeho si všímat. Jste zde ve firmě přece jen krátkou chvíli. Po asi půl hodině za vámi někdo přijde, abyste se podívali na události 31103.

Z úvodního stránky přejděte do „security event“.



Obr. 4.3: Upravená topologie pro druhý scénář

Tab. 4.2: Přehled témat 2. scénáře, kterými by měl hráč projít a jejich bodové hodnocení

	Téma	Body
`úkol 1`	Analýza L1	7
`úkol 2`	Analýza L1	7
`úkol 3`	Analýza L1	14
`úkol 4`	Analýza L2	18
`úkol 5`	Analýza L2	18
`úkol 6`	Analýza L2	18
`-`	závěrečný test	18

Firma, pro kterou tento dohled provozujete si zaplatila dohled nad jejich webovým serverem. Protože se nedávno stala obětí úspěšného SQL injection, přeje si, aby se jí reportovaly veškeré události s tímto spojené. Je potřeba jim tedy poslat report! Přeškrtnutá políčka značí informace, které nemáte k dispozici.

Využijte informace z logu a doplňte chybějící políčka v reportu označená *****.

Flag: chybějící informace ve formátu (1)_(2)_(3). Pište pouze malými písmeny.

úkol 2

Poslali jste report a doufáte, že bude vyplněn správně, aby vám váš manager nepřišel dát další školení o tom, jak report vyplňovat. Koukáte do SIEMu, když tu najednou vidíte, podezřelé aktivity – změny souborů, rušení souborů... atd.

Když si tak sedíte a koukáte kolem, zjistíte že tu sedíte úplně sami. Pár kolegů šlo na oběd a jeden šel řešit něco s technikem z jiného týmu.

Co teď? Co když tam někdo provádí něco, co nemá? Vzpomněli jste si, co vám řekl váš manager: „Když si nejsi jistý, raději ten report udělej a dej to L2 analytikovi." No, nic jiného nezbývá.

Podívejte se na logy, které přišli po SQL útoků. Hledáte logy s rule.id = 553,554,550 Použijte informace z logů a reportu a doplňte chybějící políčka v reportu označená ****.

Flag: chybějící informace ve formátu (1)_(2).Pište pouze malými písmeny.

úkol 3

Vypadá to, že je vše v pořádku. Vaši kolegové se vrátili, a když jste jim řekli, jak jste postupovali, poklepali vás po rameni. „Raději mít jistotu!" řekli, „L2 analytik se na to podívá."

Spokojeně se tedy vrátíte k práci, když co to! Vypadá to, že vaše dohlížené zařízení je pod brute force útokem. Vyděšeně jste se podívali na svého kolegu, který vás uklidil, že přece mají nastavený automatickou obranu (automatic response) proti takovému útoku. Akorát nikde nevidíte událost, která by indikovala, že by se taková obrana spustila.

Řeknete to ostatním a ti odpoví, ať se podíváte do konfigurace.

Flag: Jak vypadá nastavení automatic response na serveru?

úkol 4

Rychle jste tedy kontaktovali analytika na L2, který se na to podívá. O chvíli později za vámi přišel s potutelným úsměvem na rtech, že jej manager požádal, abyste si vyzkoušel práci na L2. Dal vám jen jednu radu, a to podívat se na výsledek útoku (=jaké události se stali hned po útoku). On prý jde zatím najít, proč není nastavená automatická reakce a poučit lidi, jak správně volit hesla.

Flag: Proveďte hlubší analýzu událostí a odhalte flag.

úkol 5

L2 vám jde skvěle! Analytik se proto rozhodl, že vás naučí ještě dalších pár věcí. Nedávno zaregistrovali události pro „port scan“ – tedy událost, která mapuje otevřené porty. Analytici musí projít porty na všech zařízení a podívat, jestli někde není potencionální riziko.

Analytik vám doporučil použít nmap, který najdete na Wazuh serveru a zkontrolovat endpoint, se kterým pracujete.

Flag: Proveďte analýzu otevřených portů, určete nebezpečný port a najděte flag!

úkol 6

Vypadá to, že na L2 si chvíli pobudete, ostatním analytikům se očividně hodí pomocná ruka. Po pár úkolech se vám dostane pod ruku váš vlastní report o podivných aktivitách na endpoint zařízení, který jste sami před tím napsali. Když vám kolegové říkali, že se na to podívá L2 analytik, nemysleli jste si, že to budete vy! Povzdechnete si a pustíte se do práce. Teď už víte, co máte dělat!

Flag: Proveďte analýzu událostí a odhalte flag.

4.4.2 Závěrečný test

Odpovědí může být jedna nebo více. Správné odpovědi zde nejsou uvedeny.

Otázka 1 (4 bodů):

L1 analytik je odpovědný za:

- Za dohled nad monitorovacími nástroji
- Aktivní reakci na útok
- Vyšetření rozsahu škod
- První vyšetření události

Otázka 2 (4 bodů):

L2 analytik je odpovědný za:

- Pokročilou analýzu událostí
- Aktivní reakci na útok
- Vyšetření rozsahu škod

- Technickou správu zařízení

Otázka 3 (2 bodů):

Telnet je nebezpečný protokol protože:

- Používá asymetrickou kryptografii
- Používá symetrickou kryptografii
- Nešifruje svůj provoz
- Používá zastaralé šifrování

Otázka 4 (2 bodů):

POP3s je šifrované spojení:

- Ano
- ne

Otázka 5 (2 bodů):

U Brute Force útoku nezáleží na tom, zda je přes Telnet nebo SSH:

- Ano
- Ne

Otázka 6 (4 bodů):

Pokročilá analýza portů může obsahovat:

- Analýzu síťového provozu na portu
- Určení otevřených portů a jejich bezpečnost
- Implementaci nastavení portů
- Analýzu omezení komunikace na portu např. firewallem

5 Vlastní impelementace scénářů

Tato část se zabývá samotnou implementací scénářů, respektive nastavením virtuálních strojů a dalších nástrojů, tak aby byl navržený scénář funkční.

5.1 Parametry Virtuálních strojů

VM-1 i VM-2 mají nastavený operační systém Ubuntu 22.04 [25], aby byla zajištěna podpora ze strany Wazuh, jak je v tabulce Tab. 3.1 v kapitole Wazuh.

Pro VM-1, kde je nainstalován Wazuh, byly parametry zvoleny následovně: 4GB RAM a 2 CPU. Jedná se o minimální parametry na kterých je schopen Wazuh fungovat za předpokladu, že je na něm nainstalovaný jak indexer, server tak i dashboard.

Ideální by bylo nastavit parametry na doporučené hodnoty 8GB RAM a 4 CPU. V potaz se však brala zátěž, kterou by takové parametry vytvořily na servery BUTCA v případě, že by hru zároveň hrálo např. 20 lidí, tedy možný ekvivalent jedné školní třídy.

Pro VM-2, sloužící jako endpointové zařízení, kde nejsou vyšší parametry potřeba, bylo zvoleno 2GM RAM a 1 CPU.

IP adresy byly zvoleny tak, aby se oba stroje nacházeli v jedné síti. Přehled parametrů lze najít v tabulce Tab. 5.1

Tab. 5.1: Přehled parametrů pro virtuální stroje.

Virtuální stroj	Název stroje	CPU	RAM(GB)	IP adresa
`VM-1`	Wazuh	2	4	10.10.2.15
`VM-2`	Endpoint	1	2	10.10.2.4

5.2 Skripty vyvolávající události

Všechny události, nebo logy, se kterými hráč pracuje v rámci scénářů, jsou vyvolávány nebo vkládány pomocí skriptů a časovány pomocí nástroje Cron.

Cron

Jedná se o program běžící na pozadí, který časuje spouštění příkazů, scriptů nebo programů. Tyto úkony se spouští automaticky bez zásahu uživatele. Jedná se tedy o systémový proces, který umožňuje spouštění jiných procesů v nastavené periodě.

První scénář

V prvním scénáři se skripty používají pro vytvoření vlastního upraveného logu, který hráči používají k ověření, že se nainstalovaný agent skutečné připojil a posílá data. Aby tento log byl vygenerován správně, musí být formát času a data na virtuálním stroji nastavený na anglický jazyk. Wazuh manager nerozpozná české datum a tak log nedokáže parsovat.

Druhou událost, kterou skript vyvolává je SQL injetion attempt, ve chvíli kdy ověří, že je nainstalovaný Apache2 server, respektive že existuje jeho log soubor, kde hráč nastavuje monitoring.

Výpis 5.1: Příklad implementace bash scriptu v prvním scénáři.

```
#!/bin/bash
tm=$(date '+%b␣%V␣%T')
echo "${tm}␣Initiate␣example[1]:Player␣hello␣there␣from
'10.10.2.4'" >> /var/log/auth.log

if test -f /var/log/apache2/access.log;
then
curl -XGET "http://10.0.2.4/users/?id=SELECT+*+FROM+users";
fi
```

Tento SQL injection je neúspěšný. Hráč však v pozdějším úkolu, kopíruje pomocí příkazu v terminálu obsah textového souboru s úspěšnými SQL injection do monitorováného log souboru. Jak tento log vypadá lze vidět ve výpisu 5.2. Jedná se plaintextový log, kde kód 200 ukazuje, že server dotaz přijal a vrátil zpátky data.

Výpis 5.2: Plantextový log úspěšného SQL injection na Apache serveru

```
192.0.12.7 - - [02/Apr/2024:09:05:42 +0200]
"GET␣/users/?id=SELECT+*+FROM+users␣HTTP/1.1" 200 3423
```

Druhý scénář

V druhé scénáři probíhají všechny události, které hráč vyšetřuje ve Wazuh, jako útoky simulované scriptem. Jeden script se nachází na endpointu a jeden na attackeru. Oba jsou nastavené pomocí cronu tak, aby se spustili při bootu zařízení.

Generované událostí je pak načasované pomocí příkazu "sleep" v samotném scriptu. Ve výpisu 5.3 je zobrazen script na endpointu.

Výpis 5.3: Příklad implementace bash scriptu v druhém scénáři na nedpointu.

```
#! /bin/bash
sleep 600
echo '###Dnes␣probehla␣automatizovana␣aktualizace␣pravidel.
Flag:␣false_positive' | cat - /etc/dovecot/dovecot.conf >
/etc/dovecot/temp && mv /etc/dovecot/temp
/etc/dovecot/dovecot.conf
sleep 20
echo "Tady␣flag␣neni,␣ale␣jsi␣blizko!␣Hledej␣dal" >>
/etc/dovecot/update_changes.txt
```

Útočící virtuální stroj simuluje dva útoky. Jeden na SQL injection, který byl v prvním scénáři. Další simulovaný útok je bruteforce, který je simulovaný pomocí "sshpass"

sshpass

Jedná se o nástroj, který umožňuje zadání hesla pro SSH připojení z příkazové řádky bez toho, aby vyžadovalo interaktivní zadání od uživatele. Používá se typicky ve scriptech a automatizovaných řešení, ačkoliv se nepovažuje za bezpečné, protože zobrazuje heslo přímo v kódu. [24]

Tento nástroj také umožňuje zadání dalších příkazů po přihlášení skrz SSH. Pomocí tohoto nástroje je několikrát vyvoláno neúspěšné SSH přihlášení a následované úspěšným přihlášení a manipulací souborů na endpointovém zařízení.

5.3 Nastavení Wazuh

Aby scénáře mohly fungovat, jak bylo zamýšleno, je potřeba provést dílčí nastavení pro každý scénář. Pro nastavování pravidel a konfiguračních souborů je používán XML. Jedná se o značkovací jazyk, kde lze vytvořit vlastní značky. Pro naše účely však není potřeba nové značky definovat a použijeme již předem definované, které implementuje Wazuh.

První scénář

V prvním scénáři se používá vlastní definovaný log. V tomto případě je tedy potřeba upravit jak parsování logu, tak nastavil vlastní pravidlo, aby jej mohl Wazuh zobrazit jako událost.

Nástroj, který parsuje logy se ve Wazuh nazývá decoder. Jeho implementaci najdeme ve výpisu 5.4

Výpis 5.4: Impelemtace decoderu pro vlastní log

```
<decoder name="example">
  <program_name>^example</program_name>
</decoder>

<decoder name="example">
  <parent>example</parent>
  <regex>Player hello there from '(\d+.\d+.\d+.\d+)'</regex>
  <order> srcip</order>
</decoder>
```

Nově definovaný decoder používá jako rodičovskou třídu již existující, který lze vidět ve výpisu jako první, <regex> značka určuje šablonu, kterou log má. "(\d+.\d+.\d+.\d+)" je proměnná složka a <order> určuje, jaký význam tato složka má. V tomto případě zdrojová IP adresa. Nastavení probíhá v souboru /var/ossec/ruleset/decoders.

Definici nového pravidla pro zobrazení pak můžeme vidět ve výpisu 5.5. Úprava probíhá v souboru /var/ossec/etc/rules/.

Výpis 5.5: Impelemtace pravidla pro vlastní log

```
<group name="custom_rules_example,">
  <rule id="100010" level="12">
  <program_name>example</program_name>
  <description>User logged</description>
  </rule>
</group>
```

Druhý scénář

Ve druhé scénáři je potřeba nastavit monitorování složek na straně agenta. Aby scénář byly pro hráče víc zajímavý a neobsahoval pouze prozkoumávání logů skrz Wazuh dasboard, bylo vypnuto zobrazování obsahu souborů v monitorovaných složkách. Wazuh tak v události nezobrazí, jaká změna proběhla a soubory musí hráči najít a otevřít sami.

Nastavení probíhá na endpointovém zařízení ve souboru /var/ossec/etc/ossec.conf a jeho implementace je ve výpisu 5.6. Důležitá je zde značka "report_changes" s atributem "no", která zakáže Wazuh aby zobrazil obsah documentů ve složce.

Výpis 5.6: Implementace FIM pro druhý scénář

```
<syscheck>
<directories check_all="yes" report_changes="no"
realtime="yes">/home/user/Documents</directories>
<directories check_all="yes" report_changes="no"
realtime="yes">/etc/dovecot/</directories>
</syscheck>
```

5.4 Report

V rámci rozhovorů s konzultantem z firmy se probíralo, co by ocenili, aby studenti znali, nebo se s tím setkali. Jedna z těchto věcí byl reporting. V rámci tvorby scénářů byla poskytnut šablona reportu, kterou si lze prohlédnout na obrázku 5.1

Report se vyskytuje v obou scénářích a je pokaždé upraven podle událostí nebo incidentu, kterých se týká. Hráči do něj doplňují dílčí informace, které hledají v událostech v SIEM.

Incident Management – Initial Ticket Information

Alert name:
Alert Category: (Credential Access, …)
Alert ID:
Functional Impact: None (None, Low, Medium, High)
Information Impact: None (None, Privacy Breach, Proprietary Breach, Integrity Loss)
Recoverability Effort: Regular (Regular, Supplemented, Extended, Not Recoverable)

Summary:
Origin of Alert: (Sentinel AAD SignInLogs, …)
Time of first alert to time of last alert: (mm/dd/yy – mm/dd/yy / ongoing)

Source Information
Number of systems impacted:
IP Address:
Hostname: N/A
MAC Address: N/A
Category of system: N/A
Physical location of system:
User on system at time of alert: N/A
Business Unit: N/A
Source Port: N/A
Protocol:
User Agent:

Destination Information
Number of systems impacted: N/A
IP Address: N/A
Hostname: N/A
MAC Address: N/A
Category of system: N/A
Physical location of system: N/A
Targeted Username:
Business Unit: N/A
Source Port: N/A
Protocol:
Service being targeted (incl. logon type, if relevant):

Contextual Investigation Notes:
Recent or relevant incidents relating to source or destination:
Open or unresolved incidents of the same type:
Connections attempted or completed (same source, port, protocol, service):

Recommendations:

Obr. 5.1: šablona reportu.

6 Testování v praxi

Aby mohlo být zhodnoceno, zda jsou scénáře vhodným výukovým materiálem a případně se odhalily možné nedostatky, bylo provedeno testování.

První testování probíhalo se studenty Univerzity obrany. Studenti si na VUT zkoušeli více scénářů z BUTCA platformy. Součástí měl být i scénář druhý, testování však narazilo na technické problémy.

Nejednalo se o chybu scénáře samotného. Problém nastal s Apache Gaucamole, které zajišťuje přístup na vzdálenou plochu skrz prohlížeč a je součástí samotné kybernetické arény. Rozvrh hrání všech scénářů se tak musel pozměnit a scénář implementovaný v této práci se stihl pouze částečně. Přistoupili jsme tak k alternativnímu testování.

6.1 Integrace do BUTCA a ověření funkčnosti

Osloveni byly studenti VUT-FEKT, zda by si chtěli scénáře vyzkoušet. Ze studentů se přihlásilo 9 osob. Dále bylo osloveno několik osob z firmy ANECT, která poskytovala konzultace při zpracovávání scénářů. Z této části se nám přihlásily 3 osoby. Celkově se tedy přihlásilo 12 lidí.

Testování vyžadovalo, aby každý měl svoje přihlašovací údaje. V případě studentů se jednalo o jejich VUT účty, pro externí hráče byly účty vygenerovány a poskytnuty přihlašovací údaje.

Aby hráči mohli přistupovat do sandboxům s virtuálními stroji, museli se připojit skrz VPN. Za tímto účelem jim byla poskytnuta identita BUTCA arény pro OpenVPN klient.

Hráčům se určily konkrétní dny, kdy byly oba scénáře dostupné a během toho určeného časy si je mohli kdykoliv zahrát.

6.2 Výsledky

Celkem z dvanácti lidí otestovalo 10 lidí scénář první a 7 lidí scénář druhý.

Údaje o hráčích jsou anonymizované. Jediný faktor, který je v tabulkách uveden, obsahuje zda jsou hráči studenti VUT označené v tabulkách jako "s" nebo externí hráči "e".

Pro každý scénář jsou rozebrány výsledky jednotlivě a porovnány mezi sebou. Na konci se hodnotí obtížnost scénářů.

6.2.1 Scénář první

Výsledky z her si lze prohlédnout v Tab.6.1, kde vidíme souhrn výsledků všech hráčů, kteří scénář testovali. Bodová chyba, které si zde můžeme všimnout vznikla u jedné otázky v závěrečném testu, kde byla správná odpověď označená jako chybná. Jedná se o chybu v implementaci v samotném rozhraní arény a ukázala se až při testování.

Tab. 6.1: Přehled výsledků pro první scénář.

Hráč	bodové výsledky úkolů	test	celkem	bodová chyba	s/e
`Max.body`	5, 10, 15, 15, 15, 2, 10, 15	13	100	-	-
`Hráč 1`	5, 10, 15, 15, 15, 2, 10, 15	11	98	2	s
`Hráč 2`	5, 10, 15, 15, 15, 2, 10 15	11	98	2	s
`Hráč 3`	5, 7.5, 15, 15, 15, 2, 10, 15	9	93.5	2	s
`Hráč 4`	5, 0, 15, 11.25, 15, 2, 10, 15	10	83.25	2	s
`Hráč 5`	5, 10, 15, 11.25, 0, 2, 0, 15	11	69.25	2	s
`Hráč 6`	5, 10, 0, 15, 15, 2, 10, 0	11	68	2	s
`Hráč 7`	5, 0, 15, 0, 0, 0, 0, 0	11	20	2	e
`Hráč 8`	5, 0, 0, 0, 0, 0, 0, 0	11	16	2	s
`Hráč 9`	5, 0, 0, 0, 0, 0, 0, 0	11	16	2	e
`Hráč 10`	5, 0, 0, 0, 0, 0, 0, 0	0	5	2	s

Nelze vyloučit, že hráč 1 a 2 by nedosáhli plného počtu 100 bodů. Graf na Obr. 6.1 zobrazuje celkový počet získaných bodů, jak hráči postupovali skrz úkoly a závěrečný test.

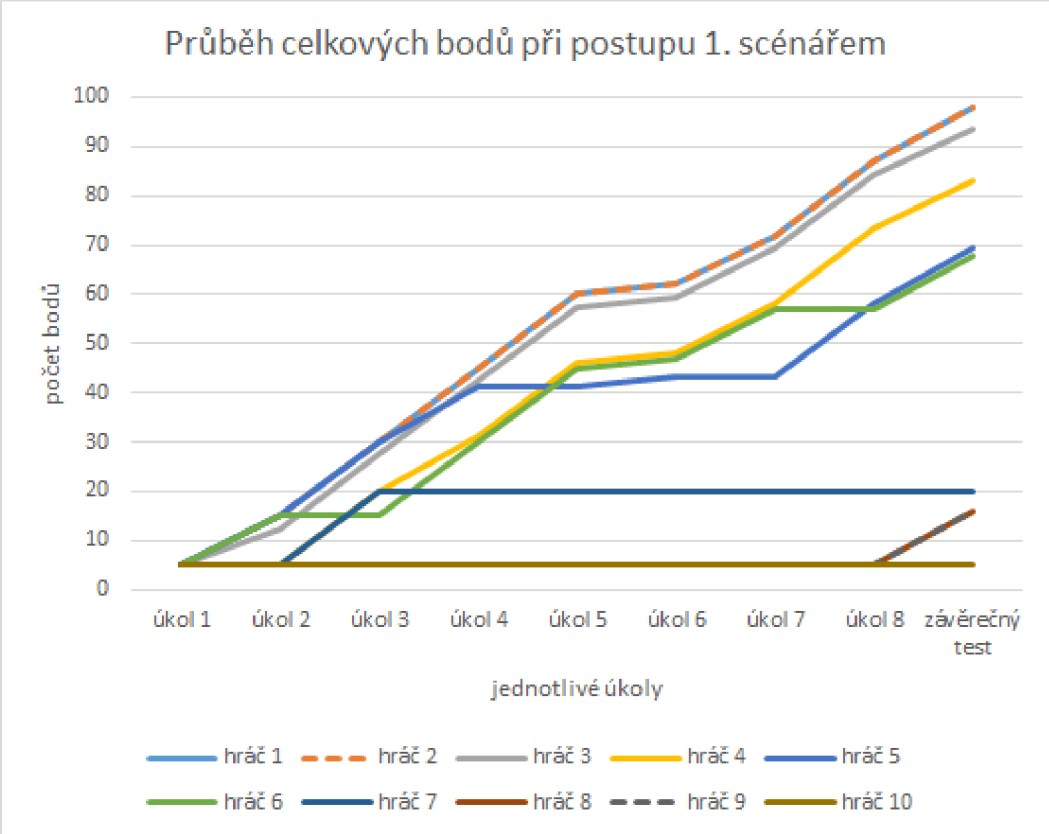
Žádný z hráčů neskončil na 0, všichni zvládli alespoň první úkol. Od dalších úkolů se výsledky začali silně lišit. Lze však pozorovat, že šest hráčů, tedy více jak polovina, získalo více jak 50 bodů. Průměr získaných bodů, je při zaokrouhlení na dvě desetinná místa 45,86 bodů.

Můžeme si všimnou, že externí hráči z firmy dosahovali nižších výsledků, ačkoliv byl předpoklad, že si povedou lépe, nebo budou v lepších výsledcích.

Tato situace mohla nastat z několika důvodů. První je povaha scénáře, která je z velké části implementační. Je možné, že studenti budou v rámci svých studií zvyklý na podobné úlohy a tedy jim přijdou povědomé.

Druhý důvod může být množství času, které tomu mohli externí hráči věnovat. Protože se netestovalo jednotně v jeden čas, ale v průběhu dnů, kdy si každý volil kdy bude scénář hrát, mohlo se jednat jednoduše o to, že scénáře potřebovali projít rychle.

Ověření těchto dvou aspektů by však vyžadovalo další testovaní s více hráči, protože takto malé množství osob není vypovídajícím faktorem. Podmínkou testování



Obr. 6.1: Graf průběhu první hry.

by taktéž měl být jednoznačně daný čas pro všechny, což by poskytlo lepší srovnání.

Tab. 6.2: Přehled průměru výsledků jednotlivých úkolů a testu pro první scénář

úkol:	1	2	3	4	5	6	7	8	test
Max.bodů	5	10	15	15	15	2	10	15	13
Průměr bodů	5	4,75	9	8,25	7,5	1,2	5	7,5	8,5
Průměr (%)	100	47,5	60	55	50	60	50	50	65,39

V tabulce Tab 6.2 jsou průměrné počty bodů a jejich procentuální reprezentace. Samotné průměry na první pohled neřeknou, v jakých úkolech si vedli lépe, protože jsou úkoly hodnocený rozdílným počtem bodů. Procentuální reprezentace je v tomto případě více vypovídající.

Nejnižší průměr je v úkolu 2. Jedná se o úkol, kde hráči hledají architekturu a distribuci operačního systému na endpointu. Vzhledem ke zpětné vazbě, kterou někteří hráči poskytli, je pravděpodobné, že jedním z aspektů je formát flagu. Úkol

sám od sebe není těžký. Wazuh dává na výběr jenom ze čtyř možností pro Linux. Problém je v tom, že Wazuh má název distribuce zkráceně např. jako DEB (Debian) nebo RPM (Red Hat distribuce), což navádí hráče k tomu, aby tam psali zkratku a nikoliv celý název. Řešením může být změnění flagu tak, aby akceptoval zkratku, ale v takovém případě nebude možné zadat celý název, a nebo dát výrazné upozornění pro hráče, aby distribuci zadávaly celým názvem.

6.2.2 Scénář druhý

Výsledky z hraní druhé scénáře si můžeme prohlédnout v Tab. 6.3, kde vidíme soubor všech hráčů, kteří hru zkoušeli. Hráčům byla ponechána stejná jména, jako měli v prvním testování, nebo přidána jako v případě Hráče 11, který předchozí scénář netestoval. Bodová chyba se zde nenachází.

Tab. 6.3: Přehled výsledků pro druhý scénář

Hráč	bodové výsledky úkolů	test	celkem	s/e
Max.body	7, 7, 14, 18, 18, 18	18	100	-
Hráč 11	7, 7, 14, 18, 18, 18	14	96	e
Hráč 10	5.25, 7, 10.5, 18, 18, 18	18	94.75	s
Hráč 2	7, 7, 14, 18, 18, 18	12	94	s
Hráč 1	7, 7, 14, 0, 18, 18	10	74	s
Hráč 5	0, 0, 10.5, 0, 13.5, 0	12	36	s
Hráč 4	5.25, 7, 0, 0, 4.5, 0	16.66	32.42	s
Hráč 8	0, 0, 0, 18, 0, 0	12.66	30.66	s

Nikdo z hráčů nedosáhl plného počtu bodů, ale celkový průměr je 64.69 bodů, který naznačuje, že hráč lze dosahovali lepších výsledků, než u scénáře předchozího. U prvního scénáře byl nejmenší dosažený počet bodů 5, u druhé vidíme nejmenší dosažený počet 30.66.

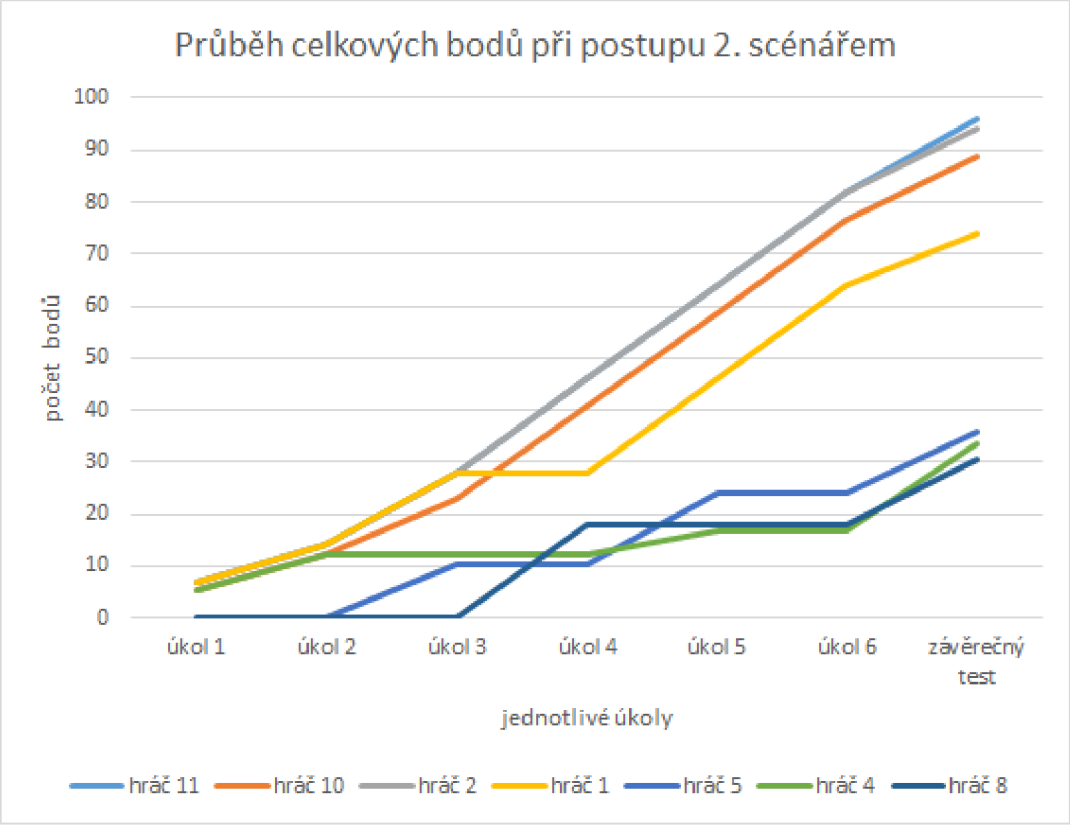
Tab. 6.4: Přehled průměru výsledků jednotlivých úkolů a testu pro druhý scénář

úkol:	1	2	3	4	5	6	test
Max.bodů	7	7	14	18	18	18	18
Průměr bodů	4,5	5	9	10,29	12,86	10,29	12,76
Průměr (%)	64,29	71,43	64,29	57,14	71,43	57,14	70,89

V Tab. 6.4 si můžeme prohlédnout průměry a jejich procentuální vyjádření. Vidíme, že nejhorších výsledků dosahovali hráči ve 4. a 6. úkolu. Tyto úkoly jsou dle

scénáře nejnáročnější, protože vyžadují hlubší analýzu logů ve Wazuh, aby odhalily všechny potřebné události. Jedná se tak o předpokládaný výsledek. Vzhledem k tomu, že průměr je stále nad polovinou bodů jednotlivých úkolů, nepředpokládá se, že by úkoly byly nepřiměřeně těžké.

Z grafu na Obr 6.2 jde vidět, že rozdíly mezi hráči nejsou tak výrazné. Můžeme si všimnout, že hráč, který v předchozím scénáři skončil jako poslední, se v druhém umístil v horních příčkách.



Obr. 6.2: Graf průběhu druhé hry.

Dále si lze povšimnout, že externí hráč byl jen jeden, ale umístil se jako první s největším počtem bodů. Můžeme se znovu zabývat tím, zda se jedná o povahu scénářem nebo časové možnosti. Vzorek je v tomto množství značně nevypovídající a nelze z něj tak vyvozovat závěry.

6.2.3 Obtížnost

U prvního scénáře není potřeba, aby hráč měl specifické znalosti v oblasti SIEM, Wazuh nebo kyberbezpečnosti. Veškeré postupy, které se ve scénáři nacházejí, a

které mají hráči implementovat jsou vyhledatelné v technické dokumentaci a na internetu.

Druhý scénář nutí hráče zamýšlet se nad událostmi, které se jim objevují ve Wazuh a jaké jsou jejich důsledky. Jde tedy o analytickou činnost. Správný postup je možné do jisté míry vyhledat, například jaký je průběh úspěšného brute-force útoku, samotné řešení však zůstává z velké části na hráčích.

Z tohoto důvodu byl první scénář označen jako lehčí a druhý scénář jako těžší.

Z výsledků, ale i ze zpětné vazby, kterou někteří hráči poskytli po dokončení scénářů, však vychází druhý scénář jako lehčí a první jako těžší a to zejména kvůli časové náročnosti. Dalším aspektem je, že pokud v prvním scénáři neimplementují některé části správně, může jim to přitížit v následujících úkolech.

6.3 Troubleshooting

Při testování se vyskytly komplikace s Wazuh. Pravděpodobně se jednalo o důsledek minimálních výpočetních prostředků na stroji, které způsobily, že přestal fungovat indexer a následně i Wazuh server.

Nejednalo se o chybu v samotném snapshotu virtuálních strojů, protože se tyto komplikace vyskytli v obou scénářích jen u některých sandboxů, zatímco nostatní fungovaly od začátku bez problémů.

Tato komplikace se dá vyřešit restartování obou těchto nefunkčních částí, pomocí příkazů:

Výpis 6.1: Příkazy pro restart nefunčních služeb Wazuh

```
sudo systemctl restart wazuh-indexer
sudo systemctl restart wazuh-manager
```

Z dlouhodobého hlediska by vhodnějším řešením bylo zvýšení výkonů virtuálních strojů na doporučené hodnoty, ovšem pouze za předpokladu, že se tak nevytvoří nepřiměřená zátěž na server BUTCA.

Závěr

Cílem práce bylo navrhnout dva scénáře pro výuku problematiky SOC v kontextu obrany proti kybernetickým útokům a hrozbám do herní platformy BUTCA.

Po odehrání scénářů by měl hráč chápat implementaci a principy, na který Security Operation Center stojí a jaká je náplň jejich práce v analytické činnosti.

V rámci práce byla analyzována problematika SOC a vysvětlena jaká je hierarchie v analytických úrovních, jaké jsou nejběžnější nástroje, které používá, a jaké aspekty by měla pokrýt. V praktické části byla navržena konstrukce scénářů za použití nejčastějších nástrojů, jako je Log Managment a detekce incidentů.

Z tohoto návrhu byly poté vytvořeny a implementovány dva scénáře do BUTCA platformy, které by měly pomoci hráčům pochopit principy SOC a jejich nástrojů. Tato znalost může pomoct hráčům rozvíjet jejich blue teamingové dovednosti a znalosti, tedy možnosti obrany proti útokům a kybernetickým hrozbám.

Dále proběhlo testování, které pomohlo odhalit chyby v implementovaných scénářích a dalo podměty k dalšímu zlepšení scénářů po technické stránce a poskytlo náhled do obtížnosti scénářů.

Veškeré stanovené cíle bakalářské práce tak byly splněny.

Literatura

[1] S. SCHINAGL, K. SCHOON AND R. PAANS, A Framework for Designing a Security Operations Centre (SOC). *48th Hawaii International Conference on System Sciences, Kauai, HI, USA,* 2015, pp. 2253-2262, ISBN:978-1-4799-7367-5

[2] D. SHAHJEE AND N. WARE, Designing a Framework of an Integrated Network and Security Operation Center: A Convergence Approach. *IEEE 7th International conference for Convergence in Technology (I2CT), Mumbai, India,* 2022, pp. 1-4, ISBN: ISBN: 978-1-6654-2168-3

[3] VIELBERTH MANFRED, GLAS MAGDALENA, DIETZ MARIETHERES, KARAGIANNIS STYLIANOS, MAGKOS EMMANOUIL, PERNUL GÜNTHER. *A Digital Twin-Based Cyber Range for SOC Analysts.* 2021 ISBN 978-3-030-81241-6.

[4] M. VIELBERTH, F. BÖHM, I. FICHTINGER AND G. PERNUL, Security Operations Center: A Systematic Study and Open Challenges, *in IEEE Access,* vol. 8, pp. 227756-227779, 2020,

[5] LI, BOWEN; PENG, XIN; XIANG, QILIN; WANG, HANZHANG; XIE, TAO; SUN, JUN; LIU, XUANZHE.Enjoy your observability: an industrial survey of microservice tracing and analysis. *Empirical Software Engineering.* 2022 ISBN: s10664-021-10063-9.

[6] MIRHEIDARI, S.A., ARSHAD, S., JALILI, R. Alert Correlation Algorithms: A Survey and Taxonomy. *Wang, G., Ray, I., Feng, D., Rajarajan, M. (eds) Cyberspace Safety and Security. CSS 2013. Lecture Notes in Computer Science, vol 8300. Springer, Cham.* 2013 ISBN:978-3-319-03583-3

[7] S. S. SEKHARAN AND K. KANDASAMY, Profiling SIEM tools and correlation engines for security analytics, *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India,* 2017, pp. 717-721, ISBN:978-1-5090-4442-9

[8] A. MADANI, S. REZAYI AND H. GHARAEE, Log management comprehensive architecture in Security Operation Center (SOC), *International Conference on Computational Aspects of Social Networks (CASoN), Salamanca, Spain,* 2011, pp. 284-289, ISBN:978-1-4577-1133-6

[9] ČESKO. Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).* In: Zákony pro lidi.cz [online].

Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181 Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181.[cit. 2023-11-10]

[10] STEVEWHIMS, *Windows Management Instrumentation - Win32 apps. Microsoft Learn.* 2023 Dostupné z: https://learn.microsoft.com/cs-cz/windows/win32/wmisdk/wmi-start-page.[cit. 2023-11-10]

[11] YELEVIN. Investigate incidents with Microsoft Sentinel.*Microsoft Learn.* 2022 Dostupné z: https://learn.microsoft.com/en-us/azure/sentinel/investigate-cases.[cit. 2023-11-10]

[12] Wolfe, L. *The five key components of Log management.* PeerSpot. 2023 [Online] ostupné z: https://www.peerspot.com/articles/the-five-key-components-of-log-management. [cit. 2023-11-10]

[13] ARFAN, S. *Log Files: Definition, Types, and Importance*, CrowdStrike. [Online.] 2021. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/observability/log-file/. [cit. 2023-11-10].

[14] ARFAN, S. *Log parsing: What is it and how does it work?* , CrowdStrike. [Online]2022 Dostupné z: https://www.crowdstrike.com/cybersecurity-101/observability/log-parsing/. [cit. 2023-11-10].

[15] MANAGEENGINE *Understanding correlation.* [Online] Dostupné z: https://www.manageengine.com/products/eventlog/help/StandaloneManagedServer-UserGuide/Real-timeEventCorrelation/correlation-concepts.html. [cit. 2023-11-10]

[16] MICROSOFT,*Co je SIEM? | Zabezpečení od Microsoftu.* [online] Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-siem. [cit. 2023-11-10]

[17] YELEVIN. *Microsoft Sentinel documentation. Microsoft Learn.* [Online] Dostupné z: https://learn.microsoft.com/en-us/azure/sentinel/. [cit. 2024-05-1].

[18] Wazuh. *Getting started with Wazuh, Wazuh documentation.*][Online] Dostupné z:

https://documentation.wazuh.com/current/getting-started/index.html. [cit. 2024-05-1].

[19] WAZUH. *Wazuh dashboard - Installation guide,Wazuh documentation.*[Online] Dostupné z: https://documentation.wazuh.com/current/installation-guide/wazuh-dashboard/index.html. [cit. 2024-05-1].

[20] WAZUH. *Wazuh indexer - Installation guide, Wazuh documentation.* [Online] Dostupné z: https://documentation.wazuh.com/current/installation-guide/wazuh-indexer/index.html. [cit. 2024-05-1].

[21] WAZUH. *Wazuh server - Installation guide, Wazuh documentation.* [Online] Dostupné z: https://documentation.wazuh.com/current/installation-guide/wazuh-server/index.html. [cit. 2024-05-1].

[22] WAZUH. *Wazuh agent - Installation guide, Wazuh documentation.* [Online] Dostupné z: https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html. [cit. 2024-05-1].

[23] VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ, *BUTCA - KYBERNETICKÁ ARÉNA | Ústav telekomunikací.*[online] Dostupné z: https://www.utko.fekt.vut.cz/butca-kyberneticka-arena. [cit. 2024-05-1].

[24] AMOANY, E. *SSH password automation in Linux with sshpass. Enable Sysadmin.* 2023 [Online] Dostupné z: https://www.redhat.com/sysadmin/ssh-automation-sshpass. [cit. 2024-05-1].

[25] ENTERPRISE OPEN SOURCE AND LINUX | UBUNTU. *Ubuntu.* [Online] https://ubuntu.com/

Seznam symbolů a zkratek

SIEM	Management bezpečnostních informací a událostí – Security Information and Event Management
SOC	Bezpečnostní operační středisko a událostí – Security Operation Center
CERT	Počítačový pohotovostní tým – Computer Emergency Response Team
ISD/IPS	Systém prevence a detekce intruzí – Intrusion Prevention System (IPS) / Intrusion Detection system (IDS)
PKI	infrastruktura veřejného klíče – public key infrastructure
WMI	Windows Managment Instrumentation
SNMP	Simple Network Management Protocol
HTTPS	Hypertext Transfer Protocol Secure
CEF	Commont Event Format
CEF	Windows Event Log
FIM	Monitorování integrity souborů – File Integrity Monitoring
BUTCA	Kybernetická aréna VUT – Brno University of Technology Cyber Arena
VM	Virtuální stroj – Virtual Machine
CSIRT	Tým pro reakci na počítačové bezpečnostní incidenty– Computer Security Incident Response Team

Seznam příloh