

Projektová dokumentace

***„Vybudování JCE IB SOŠ INFORMATIKY A SPOJŮ A SOU
KOLÍN - zpracování projektové dokumentace“***

TECHNOLOGICKÁ ČÁST JCE IB

D.1.4.9. Technologie a řešení JCE IB

***D.1.4.9.18. LOG MANAGEMENT A MANAGEMENT
BEZPEČNOSTNÍCH UDÁLOSTÍ (LM A SIEM) - CYLAB***

Zpracoval:

Petr Lacina

18 LOG MANAGEMENT A MANAGEMENT BEZPEČNOSTNÍCH UDÁLOSTÍ (LM A SIEM) - CYLAB

18.1 POPIS

Pro účely výuky bude začleněna technologie Log Managementu a SIEM (Security Information and Event Management). LM a SIEM jsou specializovaná bezpečnostní řešení, která umožňují sbírat, korelovat a analyzovat události ze všech možných vrstev IT infrastruktury. SIEM a LM řešení jsou nedílnou součástí monitoringu kybernetické bezpečnosti v rámci komerčních společností i ve veřejné správě.

Řešení Log Management, v rámci projektu, je uvažováno s konfigurovatelným uživatelským oddělením rolí s využitím silných šifrovacích metod a ochranou logů před neoprávněným přístupem k citlivým datům.

V rámci CYLAB je plánován provoz řešení v rámci virtualizace, která má pro tyto účely dostatečné kapacity. Vybrané řešení tedy musí umožňovat nasazení jako virtuální appliance.

18.2 LOG MANAGEMENT

Log Management je řešením, které umožňuje seskupovat provozní záznamy HW zařízení, OS a aplikací na jednom místě, ve sjednoceném formátu, se zachováním jejich dostupnosti, důvěrnosti a integrity. Díky přehlednému webovému rozhraní pro vyhledávání, přizpůsobitelným reportům a statistikám, umožňuje Log Management snazší práci s logy při analýze, a to jak za účelem auditu, tak i pro zajištění každodenního provozu.

Ve výuce umožní žákům pochopit princip a způsoby sběru a vyhodnocení logových údajů v rámci celé infrastruktury CYLAB. Žáci se seznámí nejen s danou technologií, která je na vrcholu pyramidy kybernetické bezpečnosti, ale i se způsoby zpracování dat, jejich logického třídění a vzájemného korelování. Umožní jim tak využít znalosti získané v rámci dalších předmětů, jako je matematika, výpočetní techniky a programování.

18.3 ŘEŠENÍ SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) V PROSTŘEDÍ CYLAB

Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí je známý pod zkratkou SIEM (Security Information and Event Management) a provádí management bezpečnostních informací a událostí.

Jedná se o analytický nástroj vytvářející závěry o bezpečnostní situaci v reálném čase, který musí velmi rychle analyzovat získaná log data o následcích s informacemi o možných příčinách. Aby SIEM plnil svoji úlohu, je nutné zajistit základní kontrolu a monitoring bezpečnosti dané infrastruktury, integrovat vhodné zdroje Log informací – vazba na Log Management. Samotný SIEM pouze identifikuje bezpečnostní události a incidenty na základě poskytnutých informací z bezpečnostní infrastruktury.

Např. pokud bezpečnostní infrastruktura neobsahuje skener zranitelností, tak SIEM nedokáže rozlišit, jestli nálezy IDS/IPS jsou věrohodné nebo false positive. Proto musí řešení SIEM umožňovat integraci s dalšími komponentami bezpečnostní infrastruktury tak, aby byl při maximální efektivitě zajištěn sběr všech potřebných informací pro detekci bezpečnostních incidentů.

18.4 SPECIFIKACE MINIMÁLNÍCH POŽADAVKŮ TECHNICKÉHO ŘEŠENÍ

18.4.1 Vlastnosti řešení Log Management

Požadovaná funkcionalita	Specifikace minimálních požadavků
Forma obsluhy	Řešení musí být konfigurovatelné a ovládané přes webové GUI rozhraní.
Počet podporovaných zdrojů log. událostí	1000 IP adres
Komponenta Log Managementu musí mít garantovanou licenci pro:	zpracování 250 EPS nebo 6 GB/day
Provedení	Virtuální appliance: Pro účely navrženého řešení budou zadavatelem poskytnuty zdroje na jeho virtuální platformě
Podpora zapojení pro High Availability, tj. vysoká dostupnost.	
Podpora vstupních protokolů (sources ~ zdrojů log záznamů) a přenosu dat.	SNMP, syslog: - UDP (dle RFC 3164), - TCP, - IETF (RFC 5424) + TLS
Aktivní sběr logů z databází.	přes ODBC, minimálně MSSQL, MYSQL, ORACLE
Podpora BUFFER/CACHE na výstupu jak u Agentu, tak pro RELAY, a také pro Server/Appliance.	
Podpora výstupních protokolů (destinations ~ umístění log záznamů).	syslog (UDP, TCP, IETF). zápis logových dat napřímo do databází (ODBC). zápis logových dat do JSON formátu. SNMP Trap.
Řízení přístupů (AAA) - řízení přístupu na úrovni jednotlivých úložišť (logspace).	
Zálohování, Archivace, Export, Sdílení log dat	Nezávislé zálohovací politiky jak pro konfiguraci, tak pro jednotlivá úložiště (logspace). Nezávislé archivační (data retention) politiky pro jednotlivá úložiště log dat. Podpora exportu/sdílení log dat v originálním i ve strukturovaném tvaru.
Řešení není provázáno na SIEM a je plně nezávislé jak fyzicky tak logicky na SIEM řešeních.	Nejedná se tedy o ALL-IN-ONE řešení, s konfigurací pro Log Management.
Rychlé vyhledávání na základě fulltext indexace (vyhledávání bez nutnosti tvorby parserů).	Velké objemy dat se neprohledávají formou „grep like“ prohledávání po řádcích.

Peering - možnost propojit více Log Management serverů a vyhledávání nad nimi přes jedno rozhraní.	Podpora minimálně 20 peerů.
Peering - definice vyhledávacích filtrů a „pohledů“ nad „peeringovými“ servery. Podpora přístupů pro pohledy (co pohled to jiná skupina uživatelů).	Podpora minimálně 20 peerů.
Možnost vyhledávání přes REST API rozhraní.	
Všechny potřebné komponenty HW i SW musí být součástí dodaného systému LM, včetně databáze.	
Log Management je fyzicky i logicky nezávislý na SIEMu. Při nedostupnosti SIEMu je Log Management plně funkční a obsahuje všechny logy v RAW formátu. Při nedostupnosti Log Managementu je SIEM plně funkční a obsahuje všechny potřebné logy v normalizovaném formátu. Vrstva zajišťující sběr je fyzicky i logicky nezávislá na LM a SIEM. Při nedostupnosti jak SIEM tak LM vrstva nadále funguje nezávisle a zajišťuje jak sběr logů tak je možné ji konfigurovat.	
Log Management je rámci celkového řešení integrován se SIEM. Je tedy možné se ze SIEM konzole překlíkem („drill down“) dostat do Log Managementu.	
Všechny požadované funkce se spravují a využívají přes společnou řídicí konzoli (dále jen „Centrální správa“), která je rovněž přístupná přes webové rozhraní z fyzického i virtuálního PC s využitím Internet Exploreru 11.0 a novějších, nebo jiným podobným způsobem. Prezentace dat musí být provedena v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformě nezávislé a plně funkční na platformách Windows, Linux, Apple OS.X.	
Systém LM musí umožňovat přihlašování pomocí lokálních účtů pro případ neaktivního propojení s AD.	
Řešení musí umožnit přístup více uživatelů současně, a to jak na úrovni přístupu ke vstupním/zdrojovým datům systému, tak i k incidentům. Přístup uživatelů musí být založen na volně definovaných, oddělených rolích s možností granularního přidělování práv v rámci každé role, dle zdrojových dat, identifikace monitorovaných zařízení, skupin zařízení a serverů, typu vstupních dat, apod. Role nesmí být vázány na AD, musí být spravovány interně.	
Řešení musí podporovat nebo být rozšiřitelné pro kompletní oddělení skupin uživatelů k odlišným datům a konfiguracím, kdy jednotlivé instance mohou mít možnost vlastní konfigurace a správy (multi-tenant přístup) a samostatných oddělených logspace.	Min 10 tenantů.
Řešení musí nativně podporovat protokoly IPv4, IPv6, jak při normalizaci vstupních dat, tak i při komunikaci se zdroji dat.	
Systém LM musí mít srozumitelně a prokazatelně deklarováno vedení licenční politiky, a to včetně uvedení funkcionalit, které nejsou součástí základní licence a zda a za jakých podmínek je možné je dokupovat.	

Komponenta sbírající logy, musí být schopna trvale zpracovávat 10000 EPS bez jakýchkoliv výkonnostních nebo licenčních omezení.	
Komponenta Log Managementu musí mít garantovaný výkon pro zpracování 10000 EPS.	
Systém dále musí umožnit uchovávání logů formou záloh a zejména musí umožnit obnovení vybraných částí logů a jejich zpřístupnění přes Centrální správu LM.	
Licence musí obsahovat možnost minimálně 1000 sběrných konektorů, včetně vlastních custom logů (možnost doplnit další lokality, zdroje událostí, atd).	
Licence musí obsahovat možnost sbírat všechny typy výrobcem podporovaných zdrojů událostí a vlastních custom logů.	
Vrstva sběru logů musí podporovat načítání log souborů (jedno a víceřádkové textové logy), kde tyto soubory budou mít stanovenou strukturu a význam dat.	
Vrstva sběru logů musí podporovat načítání logů z databáze (zejména Microsoft SQL a Oracle), kde tyto logy budou mít stanovenou strukturu a význam dat.	
Vrstva sběru logů musí umožňovat načtení a zpracování jakýchkoli typů logů, i z vlastních aplikací, tato možnost musí být k dispozici bez součinnosti výrobce nebo dodavatele řešení. Kvalita výstupu a možnosti využití musí být stejné jako v případě standardně podporovaného zdroje logů.	
Komponenta sbírající logy je musí posílat dále zašifrované a komprimované a musí umožňovat regulovat šířku užívaného pásma.	
LM systém musí podporovat pravidelné automatické přesuny dat z interního do externího úložiště, resp. archivu podle definovaných pravidel, a bez vzniku neautorizovaných změn dat;	
LM musí ukládat data v komprimované podobě pro úsporu diskové kapacity, a to v rámci interního i externího úložiště;	
LM systém musí umožňovat snadnou obnovu historických dat z archivů pro zpětnou analýzu;	
LM systém musí poskytovat mechanismus detekce neautorizovaných změn dat (kontrola integrity) v souborech systému LM;	
Systém LM musí poskytovat reporty i ve formě grafů a tabulek.	
Systém LM musí vytvářet reporty ve formátech PDF, HTML a CSV, popř. dalších.	
Systém LM musí obsahovat analytické nástroje umožňující např. reportování, forenzní analýzu, analýzu změn, statistické reporty nad aktuálními i historickými daty.	
Systém LM musí podporovat možnost zobrazit Log záznam v původní formě, jak byl přijat, tzn. raw-message.	

Systém LM musí podporovat automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému.	
Řešení poskytuje funkci event. managementu (práce s událostmi ve formě strukturovaných eventů)	Součástí dodávky je sada parserů pro obvyklá zařízení klasických ICT výrobců
Vrstva sběru (zpracování, parsování, normalizace,...) je logicky i fyzicky oddělená od centrální komponenty LM (server zajišťující uložení a vyhledávání)	
Záruka a servisní podpora	Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5.

18.4.2 Vlastnosti SIEM

Požadovaná funkcionalita	Specifikace minimálních požadavků
Všechny potřebné komponenty HW i SW musí být součástí dodaného systému SIEM (HW appliance), včetně databáze.	
Log Management je fyzicky i logicky nezávislý na SIEMu. Při nedostupnosti SIEMu je Log Management plně funkční a obsahuje všechny logy v RAW formátu. Při nedostupnosti Log Managementu je SIEM plně funkční a obsahuje všechny potřebné logy v normalizovaném formátu. Vrstva zajišťující sběr je fyzicky i logicky nezávislá na LM a SIEM. Při nedostupnosti jak SIEM, tak LM, vrstva nadále funguje nezávisle a zajišťuje jak sběr logů tak je možné ji konfigurovat.	
Log Management je v rámci řešení integrován se SIEM. Je tedy možné se ze SIEM konzole překlikem („drill down“) dostat do Log Managementu.	
Rozhraní všech komponent systému SIEM je dostupné v českém nebo anglickém jazyce. Provozní dokumentace je k dispozici v českém jazyce, ostatní buď v jazyce českém anebo anglickém.	
Každé dodávané zařízení musí (v případě on-premise nebo hybridního řešení)	Požaduje se dodání virtuální appliance
Všechny požadované funkce se spravují a využívají přes společnou řídicí konzoli (dále jen „Centrální správa“), která je rovněž přístupná přes webové rozhraní z fyzického i virtuálního PC s využitím Internet Exploreru 11.0 a novějších, nebo jiným podobným způsobem. Prezence dat musí být provedena v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformě nezávislé a plně funkční na platformách Windows, Linux, Apple OS.X.	
Centrální správa systému SIEM musí podporovat GUI (Grafické uživatelské rozhraní), a skriptovací nástroje.	
Veškerá konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů, atd., musí probíhat z grafického rozhraní systému SIEM.	
Správa uživatelů systému SIEM musí být integrovatelná s Microsoft Active Directory a RADIUS, tj. systém k přihlášení využívá doménové účty s využitím SSO.	
Systém SIEM musí rovněž umožňovat přihlašování pomocí lokálních účtů pro případ neaktivního propojení s AD.	
Řešení musí umožnit přístup více uživatelů současně, a to jak na úrovni přístupu ke vstupním/zdrojovým datům systému, tak i k incidentům. Přístup uživatelů musí být založen na volně definovaných, oddělených rolích s možností granulárního přidělování práv v rámci každé role, dle zdrojových dat, identifikace monitorovaných zařízení, skupin zařízení a serverů, typu vstupních dat, apod. Role nesmí být vázány na AD, musí být spravovány interně.	
Řešení musí podporovat nebo být rozšiřitelné pro kompletní oddělení skupin uživatelů k odlišným datům a konfiguracím, kdy jednotlivé instance mohou mít možnost vlastní konfigurace a správy (multi-tenant přístup).	Min 10 tenantů.

Systém SIEM musí vyhledávat dle klíčových slov (řetězců) v názvech zdrojů, v korelačních pravidlech v uložených log záznamech a v auditních log záznamech systému (tedy vyhledávání v konfiguračních položkách a v „contentu“).	
Systém SIEM musí zaznamenávat vlastní auditní logy po nastavitelnou dobu a tyto musí být chráněny proti modifikaci.	
Řešení musí nativně podporovat protokoly IPv4, IPv6, jak při normalizaci vstupních dat, tak i při komunikaci se zdroji dat.	
Systém umožňuje exportovat/importovat své nastavení do/ze souboru (definice dashboardů, reportů a korelačních pravidel – tedy „contentu“).	
Systém musí obsahovat plně integrovaný nástroj pro řízení celého životního cyklu incidentu (ticketing).	
Pro účely sběru dat budou zadavatelem poskytnuty zdroje na jeho virtuální platformě. Uchazeč vyspecifikuje požadavky na virtuální prostředí.	
Systém SIEM musí mít srozumitelně a prokazatelně deklarováno vedení licenční politiky, a to včetně uvedení funkcionalit, které nejsou součástí základní licence a zda a za jakých podmínek je možné je dokupovat.	
Systém SIEM nesmí být licenčně omezen na počet generujících zařízení/zdrojů logů, na počtu evidovaných aktiv a na počtu uživatelů/konzolí.	
Komponenta SIEM musí mít garantovanou licenci pro zpracování min. 250 událostí za sekundu (dále jen „EPS“) v rámci celodenního průměru, která musí být rozšiřitelná na 5000 EPS v celodenním průměru bez nutnosti upgradu HW, jen pomocí aktivace licence.	Min 250 EPS
Komponenta SIEM musí být schopna nárazově (minimálně po dobu 72h) zpracovat 7500 EPS, bez jakýchkoliv výkonnostních nebo licenčních omezení, včetně zachování plné funkcionality u všech komponent (bez ztráty logů), přičemž dodané řešení musí zajistit zpracování logů nejpozději v minutách od jejich vzniku.	
Systém SIEM nesmí technicky limitovat počet událostí (například při překročení licence nebo výkonu zakoupeného řešení) za určité časové období, aby nedošlo k jejich zahození.	
Kapacita interního úložného prostoru systému SIEM musí umožnit interně uchovat normalizované log záznamy po dobu min. 4 měsíců.	
Systém dále musí umožnit uchovávání obou formátů logů formou záloh (archivace), a zejména musí umožnit obnovení vybraných částí logů a jejich zpřístupnění přes Centrální správu SIEM.	
Výkonnost systému musí být dostatečná nejen pro sběr a korelaci logů, ale i pro přípravu reportů a alertů. Alert musí být zaslán nejpozději do 3 minut od vzniku, report obsahující 1000 řádek musí být vytvořen do 10 minut od začátku generování.	
Systém SIEM musí podporovat současnou práci min. 10 uživatelů.	Min 10 uživatelů současně.
Licence musí obsahovat možnost minimálně 1000 sběrných konektorů, včetně vlastních custom logů (možnost doplnit další lokality, zdroje událostí, atd).	
Licence musí obsahovat možnost sbírat všechny typy výrobcem podporovaných zdrojů událostí a vlastních custom logů.	

SIEM musí umožňovat používání regulárních výrazů na straně agentů (pokud budou využity) i serveru systému SIEM.	
SIEM musí umožňovat Normalizaci/Parsování bezpečnostních událostí v systému SIEM do jednotného formátu (centrální logy musí mít stejný formát ze všech zdrojů) a doplnění o další detailní informace (např. doplnění jména uživatele na základě uživatelského účtu, doplnění jména stanice na základě IP adresy apod.).	
SIEM musí umožňovat kategorizaci logů, kterou poskytuje univerzální taxonomii nezávislou na výrobci zdroje události, aby bylo možné homogenně vyhledávat, reportovat nebo porovnávat události z různých zařízení bez nutnosti detailní znalosti konkrétního logu.	
SIEM musí umožňovat vyhodnocovat i vlastní provozní logy	
SIEM musí umožňovat zobrazení a změnu nasazených korelačních pravidel, včetně pravidel dodaných výrobcem.	
SIEM musí umožňovat export a import pravidel i parserů.	
SIEM musí umožňovat definování / přidávání vlastních korelačních pravidel a log parserů bez nutnosti spolupráce s dodavatelem nebo výrobcem, např. pomocí wizardu nebo regulárních výrazů.	
SIEM musí umožňovat real-time korelaci a korelaci v časovém okně několika hodin mezi událostmi z různých zdrojů (libovolných a nezávislých zdrojů předávajících data do systému).	
SIEM musí umožňovat korelaci událostí dávkově importovaných do systému SIEM, tj. korelaci událostí, které nejsou zařazovány real-time, ale např. prostřednictvím importů logů 1x denně (scheduler correlations). SIEM umožní ověření nového korelačního pravidla proti historickým datům.	
SIEM musí umožňovat automatické stanovení závažnosti událostí např. na základě předchozí činnosti zdroje / cíle nebo jiných dostupných informací.	
SIEM musí umožňovat vyhledávání anomálií v událostech (např. nárůst počtu neúspěšných pokusů o přihlášení v určitém čase, neúspěšné pokusy o přihlášení v mimopracovní době apod.) nebo datových tocích (např. neobvyklé toky dat).	
SIEM musí umožňovat ukládání logů v systému SIEM ve tvaru, ve kterém je možné jejich prohledávání, tj. minimálně musí poskytovat vyhledávání na základě regulárních nebo logických výrazů podle času a klíčových slov (např. jmen uživatelů, čísel /jmen událostí apod.).	
SIEM musí umožňovat vyhledávání logů/eventů na základě „full-text“ indexace.	
SIEM musí umožňovat na jakoukoliv událost navázat automatickou akci: - notifikaci přes mail s možností definovat pravidla pro zasílání na různé adresy podle kritičnosti, zdroje apod. - spuštění externího skriptu.	
SIEM musí poskytovat zabudovanou "security knowledge" tj. předdefinovaná pravidla rozpoznávání a zpracování událostí a jejich pravidelné aktualizace od výrobce, min 4x ročně. Musí obsahovat minimálně: - Generické politiky	

<ul style="list-style-type: none"> - Generická korelační pravidla - Generické předdefinované reporty, pokud budou k dispozici 	
<p>SIEM musí obsahovat komplexní sadu funkcionalit a přednastavených korelačních pravidel, které řeší klasické hrozby a bezpečnostní rizika i sofistikované bezpečnostní problémy z různých oblastí:</p> <ul style="list-style-type: none"> - útoky robotů, červů a virů (včetně chyb antivirů); - neoprávněný přístup k aplikacím (ověřování uživatelů, změny administrace a konfigurace); - chyby a změny v sítích (chyby a stavy síťových zařízení); - monitorování serverů a desktopů (administrace privilegovaných uživatelů, přístupy a změny konfigurace, odmítnutá připojení, úspěšné a chybné přihlašovací aktivity, varování systémů IPS/IDS a využívání šíře pásma); - uchvácení šíře pásma a porušení platných zásad (úspěšná a chybná přihlášení do systému, změny hesla, změny konfigurace); - masivní šifrování dat (ransomware); - vědomá snaha nebo neuvědomělá činnost vedoucí k odcizení nebo znehodnocení důvěrných dat (porušení logů SIEM, DLP události, porušení časových razítek apod.); - a další. 	
Řešení SIEM musí umět porovnat neobvyklý počet určitých událostí oproti jinému období z minulosti – base line analýza.	
Systém SIEM musí být schopen provázet několik přístupových záznamů tak, aby byl schopen rozpoznat "admin hopping" = přihlášení z bodu A do D přes prostředníky B a C, za předpokladu, že přímý přístup není dovolen.	
Reportovací nástroj musí podporovat trendový reporting nad velkými objemy dat ve velkém časovém období (1 rok) a tvorbu vlastních agregačních (sumarizačních) tabulek s možností nastavit různé sumarizační časové rámce (minimálně hodiny, dny).	
Systém SIEM musí poskytovat reporty i ve formě grafů a tabulek.	
Systém SIEM musí vytvářet reporty ve formátech PDF, HTML a CSV, popř. dalších.	
Systém SIEM musí umožňovat export dat ve formátu XML nebo CSV.	
Systém SIEM musí obsahovat analytické nástroje umožňující např. reportování, forenzní analýzu, analýzu změn, statistické reporty nad aktuálními i historickými daty.	
Systém SIEM musí poskytovat pro každého uživatele vlastní personalizovaný dashboard.	
Drill-down analýza v GUI tj. od obecnějších informací vedou linky na konkrétnější informace (např. z reportu o počtu bezpečnostních událostí podle jednotlivých typů OS je možné na jeden klik dostat report o počtu bezpečnostních událostí na jednotlivých hostech s daným OS a dále pokračovat na report o počtu bezpečnostních událostí v jednotlivých aplikacích / lozích / zdrojích na daném hostu apod.).	
Systém musí podporovat automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému.	

Autentizace musí být oddělená od autorizace. Tj. Při autentizaci vůči AD je autorizace řízená uvnitř SIEM pomocí rolí a ne pomocí skupin v AD.	
Systém musí podporovat režim vysoké dostupnosti HA (High availability). Jak v režimu active-active, tak active-passive.	
Součástí SIEM nástroje je i komplexní řešení SOAR bez omezení na počet akcí nebo uživatelů.	
Řešení musí poskytovat out-of-the box pracovní toky (Workflows) na automatizaci standardních toků incidentů (Incident flows) pro různé kategorie incidentů jako DDoS, Phishing, Malware...	
Řešení musí poskytovat možnost graficky vytvářet pracovní toky (Workflow) anebo aktivity.	
Řešení musí podporovat sdružení aktivit Incident Response podle fází a schopnost stanovit pořadí aktivit, které se mají dokončit.	
Řešení musí podporovat automatizované specifikování reakčních aktivit nebo aktivity na základě a/nebo podmínek	
Řešení musí, byť schopné notifikovat zainteresovaných lidí (Tvůrce incidentu, Analytik...) o průběhu incidentu (např. při aktualizaci, označení v části incidentu, přiřazení aktivity na dokončení)	
Řešení musí nabízet produktové a konfigurovatelné funkce Reportingu a Dashboardy.	
Řešení musí poskytovat obohacení založené na typických interních údajích společnosti (např. Informace o aktivitách, uživatelích, odděleních, rolích).	
Řešení musí integrovat informace od interních a externích poskytovatelů (např. Threat Intelligence Feeds, nástroje SIEM, Endpoint).	
Řešení musí podporovat integraci s agnostickým přístupem.	
Řešení musí nabízet plně zdokumentované REST API.	