Základní prvky Security Operations Center (SOC) jsou lidé, procesy a technologie.

- Lidé: Lidé jsou klíčovým prvkem SOC, zahrnující tým bezpečnostních expertů, analytiků, incident response specialistů a dalších odborníků na bezpečnost, kteří monitorují a reagují na potenciální bezpečnostní hrozby. Lidé v SOC jsou odpovědni za analýzu a vyhodnocení bezpečnostních událostí, vyhledávání a odstraňování hrozeb, a poskytování rychlé a účinné odezvy na incidenty.
- Procesy: Procesy SOC zahrnují definování a implementaci bezpečnostních postupů, politik, standardů a směrnic, které řídí činnosti v rámci SOC. To může zahrnovat postupy pro monitorování, detekci, vyhodnocení, identifikaci a reakci na bezpečnostní události. Procesy také zahrnují evidenci incidentů, reporting, dokumentaci a sledování výkonu a efektivity SOC.
- Technologie: Technologie jsou klíčovou součástí SOC, zahrnující nástroje a systémy, které umožňují sběr, analýzu, detekci a reakci na bezpečnostní události. Mezi technologie používané v SOC patří například systémy na zachytávání a analýzu síťového provozu, bezpečnostní informační a událostní management (SIEM) nástroje, IDS/IPS systémy (Intrusion Detection/Prevention System), antivirusové programy, sandboxy pro analýzu podezřelých souborů a další.

Metody zachytávání síťového provozu zahrnují například:

- Port mirroring nebo SPAN (Switched Port Analyzer): Tato metoda umožňuje kopírování síťového provozu z jednoho nebo více síťových portů na jiný port, který je propojen s nástrojem na analýzu síťového provozu. Tím je umožněno zachycení a analýza síťového provozu bez přerušení běžného provozu na síťových zařízeních.
- TAP (Test Access Point): TAP je hardware, který umožňuje pasivní odposlech síťového provozu mezi dvěma síťovými zařízeními. Tím je zajištěno neintruzivní zachytávání síťového provozu bez ovlivnění běžného provozu na síťových zařízeních.
- Network Packet Brokers (NPB): NPB jsou speciální zařízení, která umožňují centralizovaný sběr, filtrování, analýzu a distribuci síťového provozu. NPB mohou být použity k zachycování síťového provozu z různých zdrojů a jeho předávání nástrojům na analýzu, jako jsou SIEM nástroje nebo IDS/IPS systémy.

Funkce běžných nástrojů bezpečnostního dohledu zahrnují:

- Zachytávání/analýza protokolů: Tyto nástroje umožňují sběr a analýzu síťových protokolů, jako jsou TCP/IP, UDP, DNS, HTTP, SMTP, FTP, a další. Pomáhají identifikovat podezřelou nebo škodlivou činnost na základě analýzy síťového provozu.
- Sběr informací o síťových tocích: Tyto nástroje monitorují a sbírají informace o síťových tocích, jako jsou zdrojové a cílové IP adresy, porty, protokoly, a další. Pomáhají identifikovat anomálie, jako jsou neobvyklé komunikace nebo nepovolené síťové toky.
- SIEM (Security Information and Event Management): SIEM nástroje sbírají, normalizují, korelují a analyzují data z různých zdrojů, včetně logů, událostí, a varování z různých systémů a zařízení v síti. Pomáhají identifikovat bezpečnostní incidenty a zjednodušují proces detekce, vyhodnocení a reakce na bezpečnostní události.

Příklady technologií komplikujících bezpečnostní dohled zahrnují:

- Šifrování komunikace: Šifrování komunikace mezi zařízeními nebo mezi síťovými prvky může znepřehlednit možnost zachytávání a analýzy síťového provozu, pokud nemáme odpovídající dešifrovací klíče.

- Použití virtuálních soukromých sítí (VPN): VPNs umožňují šifrovanou komunikaci mezi různými síťovými prvky, což může znepřehlednit možnost zachytávání a analýzy síťového provozu.
- Použití anonymizačních služeb nebo proxy serverů: Tyto služby nebo servery mohou maskovat skutečnou IP adresu a umožňovat anonymní komunikaci, což může znepřehlednit možnost identifikace a analýzy síťového provozu.
- Mobilní zařízení: Použití mobilních zařízení, jako jsou chytré telefony a tablety, přináší nové výzvy pro bezpečnostní dohled, protože provoz a data mohou být generována z různých míst a prostředí, což vyžaduje speciální metody pro sběr a analýzu dat.
- Internet of Things (IoT): Použití zařízení Internetu věcí, jako jsou senzory, zařízení pro sledování a další, přináší nové výzvy pro bezpečnostní dohled, protože tato zařízení mohou generovat velké množství dat a provozu, které je potřeba monitorovat a analyzovat.

Charakterizace typů dat pro bezpečnostní dohled zahrnuje:

- Alerty: Alerty jsou upozornění generovaná bezpečnostními nástroji na základě detekce potenciálně škodlivé činnosti. Alerty obsahují informace o události, která byla detekována, jako je typ útoku, zdrojová a cílová adresa, časové razítko a další relevantní informace.
- Session data: Session data zahrnují informace o síťové komunikaci mezi dvěma koncovými body, jako jsou zdrojová a cílová IP adresa, použitý protokol, porty, délka trvání spojení, přenesená data a další.
- Transakční data: Transakční data se týkají konkrétních transakcí nebo operací, které proběhly v síti, jako jsou přenosy dat, přístupy k systémům, autentizace uživatelů, a další.
- Data v plném paketu: Tato data obsahují kompletní síťový provoz, včetně všech paketů, které byly poslány nebo přijaty mezi dvěma koncovými body. Tato data umožňují detailní analýzu síťového provozu, ale mohou být objemná a náročná na analýzu.
- Statistická data: Statistická data jsou agregovaná data, která poskytují souhrnný pohled na různé aspekty síťového provozu, jako je objem dat, počet spojení, průměrná doba odezvy a další. Tyto data umožňují rychlý přehled o stavu sítě, ale nemusí poskytovat podrobnosti o jednotlivých událostech.
- Logy: Logy jsou záznamy událostí a činností v síťových zařízeních, aplikacích nebo systémech. Logy obsahují informace o provedených akcích, chybách, varováních, autentizaci uživatelů a dalších důležitých událostech, které se mohou použít pro analýzu bezpečnostních incidentů.

Přehled možných zdrojů pro sběr bezpečnostních dat zahrnuje:

- Síťové prvky: Síťové prvky, jako jsou firewally, směrovače, přepínače a další, generují logy a další data o síťovém provozu, které mohou být použity pro analýzu bezpečnostních incidentů.
- Bezpečnostní zař žízení: Bezpečnostní zařízení, jako jsou antivirové programy, antimalwarové programy, systémy detekce a prevence útoků (IDPS) a další, mohou generovat alerty, logy a jiná data o potenciálně škodlivé činnosti, která se dále používají pro bezpečnostní dohled.
- Aplikace: Aplikace, které se používají v síti, jako jsou webové servery, databázové servery, e-mailové servery a další, mohou generovat logy a další data o provozu a událostech, které se mohou použít pro analýzu bezpečnostních incidentů.
- Uživatelské zařízení: Uživatelská zařízení, jako jsou počítače, mobilní telefony, tablety a další, mohou generovat logy, session data a další data o síťovém provozu, která mohou být použita pro analýzu bezpečnostních incidentů, zejména v případě, kdy uživatelé provádějí potenciálně rizikové činnosti.
- Bezpečnostní informační a událostní management (SIEM) systémy: SIEM systémy jsou specializované nástroje pro sběr, normalizaci, korelaci, agregaci a analýzu bezpečnostních událostí a informací z různých zdrojů, jako jsou logy, alerty, session data a další. SIEM systémy mohou poskytovat komplexní pohled na bezpečnostní situaci s možností detekce a reakce na potenciální bezpečnostní hrozby.

Základní funkce SIEM (Bezpečnostní informační a událostní management) zahrnují:

- Sběr dat: SIEM systémy sbírají data z různých zdrojů, jako jsou logy, alerty, session data a další, a centralizují je do jednoho místa pro další analýzu.
- Normalizace dat: SIEM systémy normalizují data z různých zdrojů, které mohou mít různé formáty a struktury, do jednotného formátu, který umožňuje jejich další zpracování.
- Korelace dat: SIEM systémy analyzují data na základě definovaných pravidel a algoritmů pro detekci potenciálních bezpečnostních hrozeb. Data se korelují a porovnávají s předem definovanými vzory chování nebo pravidly, které mohou indikovat podezřelou činnost nebo útok.
- Agregace dat: SI EM systémy agregují data z různých zdrojů do jednoho místa a vytvářejí komplexní pohled na bezpečnostní situaci, což umožňuje identifikovat vzory a trendy v síťovém provozu a detekovat potenciální hrozby.
- Reporting: SIEM systémy poskytují různé možnosti generování reportů a vizualizace dat, které umožňují přehledně prezentovat výsledky analýzy a informovat o bezpečnostní situaci a událostech.
- SIEM systémy jsou klíčovým nástrojem pro bezpečnostní dohled, který umožňuje organizacím detekovat potenciální bezpečnostní hrozby, reagovat na ně a získávat důležité informace pro analýzu a řešení bezpečnostních incidentů.

Přehled možných zdrojů pro sběr bezpečnostních dat zahrnuje:

- Síťové zařízení: Například firewall, IDS/IPS, směrovače, přepínače a další síťová zařízení mohou generovat data o síťovém provozu, která jsou důležitá pro bez pečnostní dohled. Tato zařízení mohou poskytovat informace o provozu, který prochází sítí, komunikaci mezi systémy, a detekovat potenciální hrozby nebo anomálie.
- Bezpečnostní zařízení: Různá bezpečnostní zařízení, jako jsou antivirové programy, antimalwarové nástroje, bezpečnostní brány, a další, generují alerty a logy, které obsahují informace o podezřelých aktivitách, detekovaných hrozbách nebo jiných bezpečnostních událostech.
- Aplikační logy: Aplikace provádějící různé operace, jako jsou webové servery, databázové servery, emailové servery a další, generují logy obsahující informace o provedených akcích, přístupech, změnách a dalších událostech, které mohou mít bezpečnostní význam.
- Koncová zařízení: Koncové zařízení, jako jsou počítače, servery, mobilní telefony, a další, mohou generovat logy a alerty týkající se jejich činnosti, přístupů, komunikace a dalších bezpečnostních událostí.
- Cloudové služby: Cloudové služby, které organizace využívají pro uložení dat, zpracování nebo provozování aplikací, mohou poskytovat logy a alerty týkající se přístupů, změn konfigurace, komunikace mezi službami a dalších událostí souvisejících s bezpečností.
- Fyzické zabezpečení: Fyzické zabezpečení organizace, jako jsou kamerové systémy, detektory pohybu, přístupové karty a další zařízení, mohou poskytovat logy a alerty týkající se fyzického pohybu, přístupu a dalších bezpečnostních událostí.