observe it

people audit

INSIDER THREAT INTELLIGENCE - Cesta k vašemu bezpečnému IT

Společnost ObserveIT nabízí komplexní řešení v oblasti auditu a monitorování aktivit uživatelů, tzv Insider Threat Intelligence. Veškerá práce uživatelů, včetně administrátorů nebo služeb outsourcingových společností na počítačích nebo serverech, je automaticky zaznamenávána a může být zpětně přehrána v podobě video sekvence (videologů). Výhodu představuje generování textových logů i z aplikací, které žádné interní logy nemají. To výrazně usnadňuje vyhledávání požadovaných událostí.

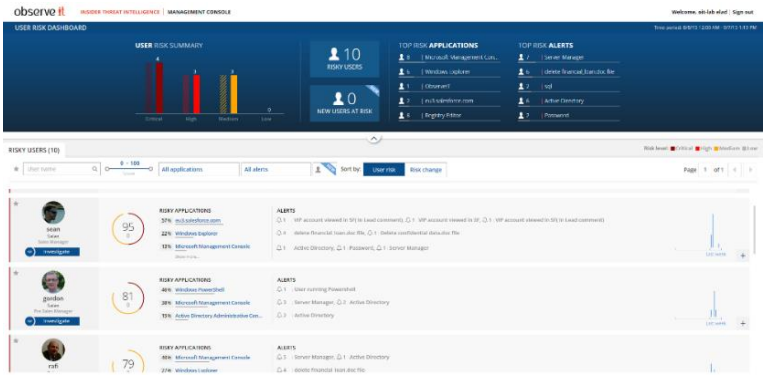
Jak řešení funguje?

Produkt ObserveIT identifikuje veškeré nové relace na serveru a přiřadí je k specifickému uživateli. Během relace jsou veškeré aktivity nahrávány přesně tak, jak je uživatel může vidět na své obrazovce. Kromě videozáznamu jsou veškeré události převáděny i do podoby textových logů pro snadné budoucí vyhledávání. Přehledné reporty následně chronologicky zobrazují seznam provedených akcí včetně odkazů pro přehrání příslušného videa. Monitorovat aktivity lze na širokém spektru protokolů a prostředí, které např. zahrnují: SSH, Remote Desktop Protocol (RDP), Telnet a prostředí VMware, Citrix.

Další výhody

Shoda se standardy – monitorování a audit lokálních a vzdáleně připojených uživatelů, včetně poskytovaletů servisních služeb pro prokázání shody s PCI, HIPAA, SOX a ISO 27001 standardy.

Insider Threat Intelligence – Jedinečný nástroj pro hodnocení rizikovosti uživatelů, který zároveň analýzu graficky reprezentuje v přehledných reportech. Každému uživateli je uděleno rizikové skóre na základě jeho aktivit. Administrátor má navíc možnost nahlédnout do skutečných aktivit uživatele a tak rozlišit, zdali se jedná o opravdu rizikové jednání, nebo běžnou aktivitu. Ihned lze proti rizikovému jedinci jednat – například mu odříznout session.



Nízké hardwarové nároky – velmi efektivní ukládání dat, méně než 250GB/rok při plném využití a v prostředí, kdy je sledováno až 1000 serverů. Agent na zařízení vyžaduje pouze 1-2% výkonu CPU a 10MB paměti během nahrávání relace. Je to především díky ukládaní videoformátů založených na screenshotech a také neukládání záznamu během nečinnosti uživatele, kdy se záznam zastaví a jeho obnovení nastane během UI aktivity, použitím klávesnice nebo myši.

Definice pravidel pro pořizování záznamů – možnost nastavení pravidel podle aplikací, uživatele, serveru, URL, různých skupin.

Získání komplexních metadat, která obsahují jméno uživatele, jméno aplikace, datum a čas, Window title, jméno procesu, přístup k souborům a adresářům, navštívené URL atd.

File Activity Monitoring (FAM) je funkcionalita, která umoňuje sledování souborů, které jsou stahovány/nahrávány v rámci webových aplikací (SharePoint, CRM, ERP, …). U stažených souborů dále monitoruje jejich pohyb, včetně vynesení pomocí podporovaných klientů cloudových úložišť (Dropbox, Google Drive, …).

Klíčové charakteristiky

- ⇒ Sofistikovaný systém pro audit: **videozáznam a textové logy všech aktivit uživatelů i z aplikací bez interních logů.**
- ⇒ Videozáznam nabízí detailní přehled o aktivitách uživatelů.
- ⇒ **Přiřazení identit administrátorů** ke skutečným uživatelům (v případě využití sdíleného účtu)
- ⇒ **Integrace řešení se SIEM** s možností doplnění logů a událostí do logů tam kde nejsou systémem nativně poskytovány
- ⇒ **Sledování** editace systémových souborů, změn v nastavení OS, příkazů v databázi, transakcí v SAP, přístupu ke sdíleným souborům nebo prohlížení stránek v CRM a ERP
- ⇒ **Podporované systémy:** Windows, Unix a Linux, (servery a desktop); Citrix a VMware
- ⇒ **Insider Threat Intelligence** provádí hodnocení rizikovosti uživatelů, na jehož základě každý uživatel získá agregované skóre.
- ⇒ **Dynamic Forensic video recording -** Během uživatelské relace sbírá pouze metadata a až na základě definovaného nestandardního chování spustí nahrávání (videolog).
- ⇒ **Detecting Data Loss –** pomocí agenta lze detekovat možnou exfiltraci kritických, nebo citlivých dat.
- ⇒ **Soft Prevention -** Pro vybraná pravidla popisující nestandardní chování uživatelů, je možné definovat vlastní upozornění a případně i s odkazem na platnou bezpečnostní politiku

Další důležité funkcionality

- ⇒ **Anonymizace osobních údajů –** Je možné konfiguračně vynutit anonymizaci osobních údajů a zřídit roli Privacy Officer, který schvaluje požadavky na odkrytí identity
- ⇒ **URL kategorizace –** Dostupných 27 URL kategorií, na základě kterých je možné definovat alertovací pravidla s následným vyhodnocením rizikovosti uživatelů.
- ⇒ **Monitorování tisku** – ObserveIT Agent umožňuje monitorovat tiskové úlohy
- ⇒ ObserveIT Agent pro **Mac OS X** – nyní v beta verzi

COMGUARD security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

observe it

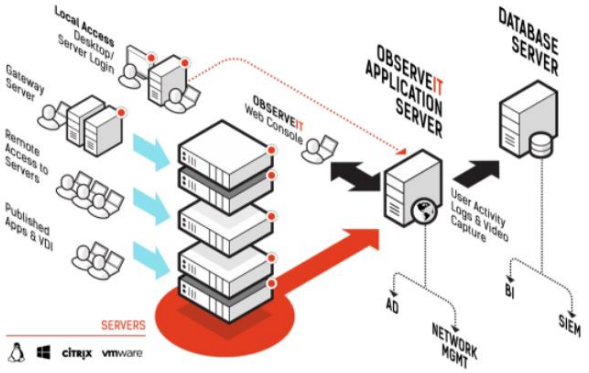
people audit

Záznamy ze všech typů přístupů - i přímo z fyzických strojů (např. Ctrl+Alt+Del log přímo na stanici), záznamy ze vzdálených přístupů (všechny typy protokolů).

Monitorování změn v nastavení síťových zařízení – ObserveIT umožňuje snadné sledování změn v nastaveních a přesné určení osoby, která je provedla a kdy. Dále dovoluje definovat vlastní alerty, které se spouští dle předem stanovených pravidel.

Threat Detection Console – napomáhá administrátorům odhalit potencionální problémy a hrozby. Tato konzole poskytuje přehledné tabulky, které popisují trendy v oblastech:

- **Aktivity během nočních hodin a víkendů** – zobrazuje počet přihlášení mimo běžných pracovních hodin. Tato tabulka napomáhá odhalit neautorizovaná nebo škodlivá přihlášení k monitorovaným systémům.
- **Aktuálně nejvíce aktivní počítače** – systémy, které mají aktuálně nejvíce aktivních relací.
- **Užívání nejméně frekventovaných aplikací** – tabulka aplikací, které jsou nejméně využívány, napomáhá odhalit potencionálně nebezpečné programy.
- **Užívání nejméně frekventovaných počítačů** – tabulka počítačů, které jsou nejméně využívány, napomáhá odhalit jejich potencionálně nebezpečné využití.
- **Užívání nejméně frekventovaných přihlašovacích údajů** – tabulka přihlašovacích údajů, které jsou nejméně využívány, napomáhá odhalit jejich potencionálně nebezpečné využití.
- **Přihlášení stylem LeapFrog** – instance, ve které se uživatel přihlasí k monitorovanému PC a z něho se připojí k dalšímu monitorovanému PC. Tato tabulka odhaluje potenciálně neautorizované přístupy k zabezpečeným systémům.
- **Vzdálený přístup** – tabulka napomáhá odhalit uživatele, kteří nemají oprávnění se vzdáleně připojit.



Audit aktivit v databázích – veškeré aktivity v databázích mohou být monitorovány pomocí ObserveIT a veškeré SQL dotazy lze filtrovat dle databáze, času, uživatele, serveru, ID nebo jakéhokoli textu používaného v dotazech. Pro přístup uživatelů k databázi je využíván gateway server, na kterém je nainstalován ObserveIT agent a nástroj na správu databází.

Integrace s tiketovacími systémy – tato integrace poskytuje další možnost, jak rozšířit bezpečnost a monitorování. ObserveIT nabízí již vestavěnou integraci s některými tiketovacími systémy, např. ServiceNow nebo umožňuje implementovat speciální konektory podle aktuálních požadavků zákazníků.

Pokud se administrátor nebo poskytovatel servisních služeb pokouší připojit k monitorovanému serveru, je vyzván, aby zadal číslo daného ticketu, které je nejprve ověřeno a až následně je dané osobě umožněn přístup k danému serveru. Zároveň se i do tiketovacího systému umístí přímý odkaz na video, které obsahuje nahranou celou relaci odpovídající danému číslu tiketu.

Monitorování privilegovaných uživatelů – pokud administrátoři sdílejí své přihlašovací údaje, může být vyžadována další forma autentizace, kde zadají své uživatelské ID. Tyto přihlašovací údaje lze provázat např. s Active Directory nebo mohou být spravovány lokálně z konzole ObserveIT. Tento mechanismus dovoluje využívat sdílené administrátorské účty a přitom identifikovat konkrétního uživatele.

Audit a reporty – webová konzole ObserveIT nabízí řadu možností jak procházet, hledat nebo vytvářet reporty a exportovat zdrojová data s ohledem na aktivity uživatelů. Generátor reportů obsahuje přednastavené vzory včetně možnosti tvorby vlastních reportů na základě uživatelů/skupin uživatelů, serverů/skupin serverů, času, aplikací atd. Reporty je možné vytvořit na vyžádání nebo je pravidelně zasílat emailem odpovědné osobě. Veškeré monitorované relace mohou být podrobně prohlíženy dle jednotlivých akcí a lze např. přehrát i video, které se týká pouze dané aktivity a nikoli celé zaznamenané relace.

Archivace – ObserveIT má zabudovanou funkcionalitu archivace, kdy mohou být data přesunuta do sekundární databáze. Archivaci lze provést manuálně nebo v předem naplánovaných časových intervalech. Archivační proces přesouvá pouze videa, která vyžadují nejvíce prostoru, ale metadata zůstavájí dostupná pro vyhledávání.

Upozornění na monitorování – uživatelé mohou být upozorněni, že jsou monitorováni. Příslušná zpráva se zobrazí ihned po přihlášení a lze vyžadovat i potvrzení od uživatele. Text upozornění je možné upravit dle požadavků zákazníka.

SOCIETE GENERALE	Allianz	SAMSUNG	Coca-Cola	vodafone
BNP PARIBAS	ING	SIEMENS	xerox	FUJITSU
UBI Banca	BLACKROCK	Cisco webex	SANOFI	T-Mobile
中国建设银行	ups	BT	IBM	orange

COMGUARD
security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz