OBSERVEIT NABÍZÍ KOMPLEXNÍ ŘEŠENÍ V OBLASTI AUDITU A MONITOROVÁNÍ AKTIVIT UŽIVATELŮ.

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. Výhodu představuje generování textových logů i z aplikací, které žádné interní logy nemají. To výrazně usnadňuje vyhledávání požadovaných událostí.

Charakteristika řešení

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

Cílová skupina

Větší organizace vyžadující dohled nad tím, co správci skutečně dělají, úřady podléhající Zákonu o kybernetické bezpečnosti, organizace jejichž dodavatelé či partneři přistupují vzdáleně do jejich systému apod.

PODPOROVANÉ PLATFORMY

- Microsoft Windows Server 2008/2008 R2/2012/2012 R2, Windows Vista, Windows 7, Windows 8, 8.1 a Windows 10.
- Solaris 10 (updates 7-11) a Solaris 11 (updates 1-3)
- RHEL/CentOS 5.10-5.11, RHEL/CentOS 6.6-6.8 a RHEL/CentOS 7.0-7.2
- Ubuntu 12.04., 14.04 a 16.04
- Oracle Linux 4.8-4.9, 5.10-5.11, 6.6-6.8 a 7.0-7.2
- SLES SuSE 11 SP2-SP3 a SLES SuSE 12
- AIX 6.1, AIX 7.1 a AIX 7.2
- HP-UX 11.23 a 11.31
- Debian 6, 7 a 8 (32-bit/64-bit)
- Amazon Linux AMI 2015.03

Přínosy

Shoda se standardy - monitorování a audit pro prokázání shody s PCI, HIPAA, SOX a ISO 27001 standardy a naplnění konkrétních požadavků nařízení GDPR na zohlednění rizik zpracování osobních údajů (OÚ), jako např. náhodné nebo protiprávní zničení, pozměňování, neoprávněné zpřístupnění zpracovávaných OÚ, na zajištění zpracování pouze oprávněnými osobami, prokazatelnost a vedení záznamů o činnostech zpracování OÚ. Monitorování změn v nastavení síťových zařízení - snadné sledování změn v nastaveních a přesné určení osoby, která je provedla a kdy.

Nízké hardwarové nároky - velmi efektivní ukládání dat, méně než 250GB/rok při plném využití a v prostředí, kdy je sledováno až 1000 serverů.

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

Záznamy ze všech typů přístupů - i přímo z fyzických strojů, záznamy ze vzdálených přístupů.

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

- Aktivity během nočních hodin a víkendů
- Aktuálně nejvíce aktivní počítače
- Užívání nejméně frekventovaných aplikací
- Užívání nejméně frekventovaných počítačů
- Užívání nejméně frekventovaných přihlašovacích údajů
- Přihlášení stylem LeapFrog
- Vzdálený přístup

Audit aktivit v databázích - aktivity v databázích mohou být monitorovány a veškeré SQL dotazy lze filtrovat dle databáze, času, uživatele, serveru, ID nebo jakéhokoli textu používaného v dotazech.

Integrace s tiketovacími systémy - ObserveIT nabízí již vestavěnou integraci s některými tiketovacími systémy, např. ServiceNow, nebo umožňuje implementovat speciální konektory podle aktuálních požadavků zákazníků.

Monitorování privilegovaných uživatelů - pokud administrátoři sdílejí své přihlašovací údaje, může být vyžadována další forma autentizace - zadání uživatelského ID. Tento mechanismus dovoluje využívat sdílené administrátorské účty a současně identifikovat konkrétního uživatele.

Audit a reporty - ObserveIT nabízí řadu možností jak procházet, hledat nebo vytvářet reporty a exportovat zdrojová data. 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.

Archivace - ObserveIT má zabudovanou funkcionalitu archivace, kdy mohou být data přesunuta do sekundární databáze. Archivační proces přesouvá pouze videa, která vyžadují nejvíce prostoru, ale metadata zůstávají dostupná pro vyhledávání.