Security Information and Event Management

Advania erbjuder *SIEM SaaS- Security Information and Event Management* som genom en komplett uppsättning moduler skyddar kundens miljö genom att övervaka, identifiera och analysera potentiella hot och avvikelser i realtid.

Cyberkriminaliteten och hoten gentemot företag och organisationer har ökat markant de senaste åren, varpå intrång har blivit allt mer komplexa och svåra att upptäckta. Detta har kommit att bidra till en kostsam historia, både ekonomiskt och anseendemässigt, för verksamheter som drabbats. Inga tecken tyder på att trenden kommer att vända, utan företag och organisationer kommer snarare bli tvungna att i allt högre utsträckning skydda sin verksamhet såväl tekniskt som organisatoriskt.

Advania erbjuder SIEM, en tjänst som gör det möjligt att motverka potentiella hot redan innan de får fäste inom verksamheten. Detta sker genom ständig realtidsövervakning av aktiviteter inom system, nätverk, brandväggar, databaser och applikationer. SIEM samlar in, analyserar, eventhanterar, loggar och korrelerar data för att identifiera trender och spåra avvikelser. Systemet har genom dessa funktioner förmåga att upptäcka potentiella säkerhetshot och genast larma för dessa, samtidigt som det filtrerar bort data som är irrelevant eller som inte utgör någon fara. Vidare omvandlas loggarna i realtid till information som är lätt att utläsa och som finns samlad på ett och samma ställe vilket skapar förutsättningar för ett snabbt agerande.

Varför SIEM?

Frågan som många verksamheter ställer är - vi har redan diverse skydd i form av brandväggar, virusskydd och annat. Varför ska vi satsa på SIEM?

Det är nästintill omöjligt att fullt ut skydda sin verksamhet från intrång. För att tjänster i form av brandväggar, virusskydd och liknande ska kunna ge ett fullbordat skydd kommer de behöva vara så begränsande att användarna kommer få svårt att utföra sitt arbete. Istället behöver man anpassa dessa skydd så att verksamheten kan leva ut sin fulla potential, vilket då även öppnar upp för hot. SIEM fungerar vid sidan av dessa skydd och detekterar och analyserar de externa hot som föreligger. Tjänsten upptäcker även potentiella hot inom verksamheten genom att identifiera avvikande eller skadliga användarmönster som inte överensstämmer med verksamhetens användarpolicy.

Tjänstepaket

Advania erbjuder SIEM utifrån olika tjänstepaket vilket gör det möjligt att anpassa tjänsten efter verksamhetens behov. Tjänsten kan innebära allt från att Advania utbildar utvalda verksamhetsrepresentanter inom SIEM för att sedan självständigt nyttja tjänsten, till att Advania bistår med ett SOC-team som managerar och monitorerar tjänsten. Tjänsten kan även kompletteras med Sårbarhetskanning vilket stärker tjänsten ytterligare. Detta genom att identifiera säkerhetsrelaterade sårbarheter inom verksamhetens IT-system.

advania

Affärsnyttor

Effektivisering
SIEMs förmåga att omvandla loggar, som annars är nästintill omöjliga att mänskligt tolka i realtid, till information som är lätt att utläsa samt att prioritera de hot som faktiskt utgör fara för verksamheten reducerar såväl tid- som resursåtgång vad gäller identifiering och hantering av de hot som föreligger.

Lagring
Advanias SIEM- tjänst inkluderar även säker lagring. Vilket gör det möjligt att analysera tidigare händelser i ett senare skede.

Automatiserade åtgärder
Genom tjänsten kan även initiala åtgärder, i form av bland annat nekad åtkomst, automatiseras vilket både påskyndar hanteringen av hot och reducerar potentiell skada.

Compliance
SIEM-tjänstens loggar bidrar till spårbarhet som utgör en viktig aspekt för informationssäkerheten och som i många fall utgör ett externt krav gentemot de allra flesta verksamheter, i form av bland annat GDPR. SIEM bidrar till att personuppgifts-och information läckage förhindras och incidenthantering effektiviseras. Vidare skapar tjänsten en ökad trygghet vad gäller hantering av personuppgifter och annan skyddsvärd information genom att samla bevis för compliance samt generera anpassade rapporter som underlättar vid audit.

Vid frågor, kontakta:
FREDRIK MÖLLER
Business Area Manager
fredrik.moller@advania.com