Security Operations by Aderian®

PREDICT PROTECT RESPOND

De flesta företag upptäcker IT-attacker för sent.

Vi hjälper organisationer att upptäcka, förstå och stoppa cyberhot innan de påverkar verksamheten. Genom 24/7 SOC-övervakning, avancerade penetrationstester och vår APS-tjänst (Attack Prediction Service) arbetar vi proaktivt för att minska risker och stärka säkerheten i hela IT-miljön. Från identifiering av sårbarheter till aktiv incidenthantering - vi hjälper er att ligga steget före angriparna.

Våra tjänster

- SOC - Bemannad övervakning av IT-miljön 24/7
- Early Warnings - (Attack Prediction Service)
- Penetrationstest - vi utsätter IT-miljön för simulerade attacker

Security Operations by Aderian®

Security Operations Center (SOC) är en modern och högtillgänglig säkerhetstjänst för att identifiera och åtgärda säkerhetsincidenter i kundens IT-miljö.
Tjänsten är bemannad av operatörer 24/7/365 som analyserar säkerhetshändelser och tar relevanta mitgeringsåtgärder för att avbryta den pågående incidenten eller minska skadan mot kundens IT-miljö. Tjänsten bygger på molnbaserad säkerhetsfunktionalitet i Microsofts ekosystem och operatörerna arbetar i kundens egna IT-miljö.

Fördelar för er som kund

- 24/7 övervakning av säkerhetshot - Kontinuerlig bevakning av er IT-miljö för att snabbt upptäcka misstänkt aktivitet och pågående attacker.
- Snabbare upptäckt och respons - Minskar tiden från attack till åtgärd och begränsar påverkan på verksamheten.
- Proaktivt skydd mot moderna cyberhot - Identifierar risker, avvikelser och attacker innan de utvecklas till allvarliga incidenter.
- Ökad trygghet och kontroll - Ger bättre insyn i säkerhetsläget och hjälper er fatta rätt beslut vid incidenter.
- Tillgång till säkerhetsexpertis - Ni får ett dedikerat säkerhetsteam utan att behöva bygga upp en egen SOC-organisation internt.
- Rapportering kvartalsvis - insyn i olika säkerhetshändelser.
- Enkel prismodell med tydliga avgränsningar

Security Operations by Aderian

Early Warnings

Upptäck risker innan de blir incidenter

Många cyberattacker börjar långt innan någon märker något. Det kan handla om exponerade system, läckta lösenord eller leverantörer som blivit utsatta för intrång. SOA Early Warning hjälper er att upptäcka och prioritera dessa risker i tid - innan de utvecklas till säkerhetsincidenter som påverkar verksamheten. Tjänsten kombinerar attackyteanalys, dark web-bevakning, leverantörsövervakning och expertanalys för att ge er en tydlig och kontinuerlig bild av organisationens cyberexponering.

Fördelar för verksamheten

Tidigare varningssignaler - Identifiera risker innan de leder till incidenter.

- Mindre brus och färre falsklarm - Vi filtrerar och prioriterar det som verkligen är relevant.
- Tydligare beslutsunderlag - IT och ledning får en gemensam och begriplig riskbild.
- Starkare proaktiv säkerhet - Kompletterar SOC, MDR och EDR genom att fokusera på risker innan attacker sker.

Vad tjänsten innehåller

Extern attackyteanalys - Vi analyserar hur er organisation ser ut från en angripares perspektiv och identifierar:

- Exponerade system och tjänster
- Kända sårbarheter
- Felkonfigurationer och onödiga exponeringar
- Ni får en prioriterad bild av vilka risker som bör hanteras först.

Bevakning av läckta konton och lösenord

Vi övervakar om användarkonton eller inloggningsuppgifter kopplade till era domäner förekommer i dataläckor eller kriminella miljöer. Det gör att ni kan agera snabbt genom exempelvis lösenordsbyten, spärrning av konton eller förstärkt övervakning.

Security Operations by Aderian

Early Warnings

Upptäck risker innan de blir incidenter

Leverantörsbevakning

Era leverantörer är en del av er säkerhetsrisk. Om en partner drabbas av intrång kan även er verksamhet påverkas. Vi bevakar utvalda leverantörer och varnar vid relevanta incidenter, läckor eller ransomware-angrepp.

Expertgranskade larm och rekommendationer

Målet är inte fler larm - utan rätt larm. Alla fynd analyseras och prioriteras av säkerhetsspecialister för att minska brus och ge tydliga rekommendationer kring vad som bör åtgärdas först.

Ni får regelbundna rapporter med:

- Exponerade system och risker
- Läckta konton eller inloggningsuppgifter
- Leverantörsrelaterade hot
- Prioriterade åtgärdsförslag
- Rekommendationer för IT och ledning

Rapporteringen är anpassad för både tekniska team och beslutsfattare.

Passar särskilt bra för organisationer som

- vill få bättre kontroll över sin externa attackyta
- saknar tid eller specialistkompetens för kontinuerlig omvärldsbevakning
- arbetar med regulatoriska krav som NIS2
- behöver tydligare underlag för ledning, revision eller cyberförsäkring

Leverans och uppstart

Tjänsten levereras till ett fast månadspris och inkluderar bevakning, analys, rapportering och rekommendationer enligt överenskommen omfattning. Första rapporteringen sker normalt inom fem veckor från beställning.

Security Operations by Aderian

Penetrationstestning

Identifiera säkerhetsbrister innan angriparna gör det

Vi hjälper er att upptäcka sårbarheter och risker i er IT-miljö genom kontrollerade penetrationstester. Syftet är att visa hur en angripare skulle kunna ta sig in, sprida sig eller påverka verksamheten samt ge tydliga rekommendationer för hur säkerheten kan stärkas. Varje uppdrag anpassas efter verksamhetens behov och omfattning.

Vad tjänsten kan omfatta - inventering och analys

Vi kartlägger och analyserar er IT-miljö för att identifiera exponerade tjänster, system och potentiella riskområden. Tillsammans fastställer vi sedan omfattning, metodik och testnivå utifrån verksamhetens behov.

Simulering av verkliga attacker

Vi genomför kontrollerade tester där vi agerar som en potentiell angripare för att identifiera säkerhetsbrister och bedöma hur väl miljön står emot cyberattacker.

Testerna kan omfatta:

- Operativsystem och servrar
- Webbapplikationer
- Nätverk och infrastruktur
- Social engineering och användarpåverkan

Test av spridning och åtkomst

Om sårbarheter identifieras testar vi även möjligheten för en angripare att:

- Höja sina behörigheter
- Sprida sig vidare i miljön
- Få åtkomst till känslig information

Alla tester genomförs kontrollerat och avbryts om det finns risk för negativ påverkan på drift eller verksamhet.

Security Operations by Aderian

Penetrationstestning

Identifiera säkerhetsbrister innan angriparna gör det

Bedömning av påverkan

Vi analyserar vilka konsekvenser en attack skulle kunna få, exempelvis:

- Datastöld
- Obefogad åtkomst
- Driftpåverkan eller avbrott

Rapportering och rekommendationer

Efter genomfört test får ni en tydlig rapport med:

- Identifierade sårbarheter
- Riskbedömningar
- Rekommenderade åtgärder
- Prioriterade förbättringsförslag

Resultatet presenteras även vid ett genomgångsmöte tillsammans med våra säkerhetsspecialister.

Säker hantering av information

All information som samlas in under uppdraget hanteras konfidentiellt och raderas permanent efter avslutat projekt.