SOC+

Sikkerhetsovervåking
hele døgnet – hele året

ATEA

Atea SOC+

Med sikkerhetsovervåking fra Atea får du grunnleggende deteksjonsevne og evne til å reagere raskt på mistenkelig aktivitet. Du reduserer risikoen for økonomiske tap og tap av omdømme, og bedriften kommer raskere tilbake etter et sikkerhetsbrudd.

- **Digital vektertjeneste 24x7x365**
- **Tilgang til et av landets sterkeste sikkerhetsmiljøer**
- **Kontinuerlig oppfølging fra sikkerhetsrådgiver**

ATEA SOC+

Avansert sikkerhets-overvåking med NSM-godkjent hendelseshåndtering

Statistikk fra Ateas Incident Response Team (IRT) viser at det i 2021 var en femdobling i antallet sikkerhetshendelser. I dette trusselbildet er det viktigere enn noensinne å oppdage angrep så raskt som mulig for å begrense skadeomfanget.

Et cyberangrep kan få store konsekvenser, både kostnads- og omdømmemessig. Det er styrets og øverste leders ansvar å redusere risikoen for denne typen hendelser, men svært ofte har man ikke det som skal til for å unngå angrep eller for å begrense skadene etter et angrep. Sikkerhetsmyndigheter anbefaler derfor at man kjøper sikkerhetsovervåking og analysekompetanse hvis man ikke har det selv.

Hvis du ikke har en løsning der logger, alarmer og hendelser blir kontinuerlig fanget opp, undersøkt og forstått, står du dårlig rustet til å takle for eksempel digital utpressing.

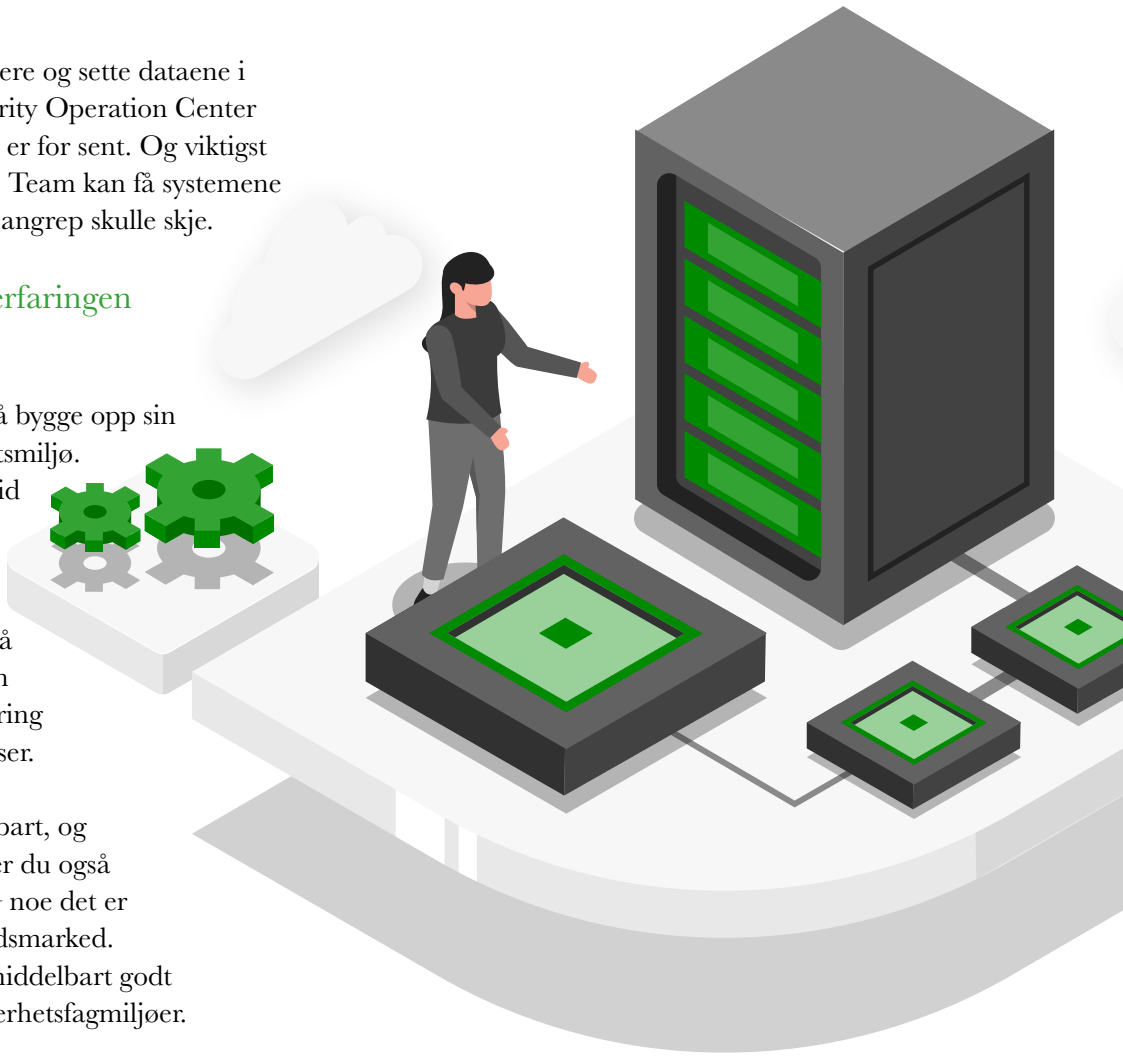
Ved å abonnere på vår digitale vektertjeneste Atea SOC+ kan du sove trygt om natten. Tjenesten gir bedriften en døgnbemannet digital vektertjeneste, og dekker blant annet:

- Bedriftens egen sikkerhetsrådgiver
- Innsamling av data fra alle relevante loggkilder
- Se dataene på tvers av systemer for å oppdage unormale hendelser
- Analyse av dataene for å se om noe krever oppfølging
- Hendelseshåndtering (IRT) – sikkerhetseksperter rykker ut hvis noe skjer

Ved å samle data, samt analysere og sette dataene i sammenheng, kan Ateas Security Operation Center (SOC) avdekke angrep før det er for sent. Og viktigst av alt: Vårt Incident Response Team kan få systemene fortest mulig opp igjen hvis et angrep skulle skje.

Du får aldri den samme erfaringen med en egen SOC

Enkelte store bedrifter velger å bygge opp sin egen SOC og et eget sikkerhetsmiljø. Det å gjøre alt selv er imidlertid ikke nødvendigvis den beste løsningen. Ofte er du bedre tjent med å out-source oppgavene, eventuelt gå for en hybridløsning hvor egen kapasitet for sikkerhetshåndtering suppleres med eksterne ressurser.



Å bygge en egen SOC er kostbart, og i tillegg til gode verktøy trenger du også å ansette sikkerhetseksperter – noe det er stor mangel på i dagens arbeidsmarked. Med Atea SOC+ nyter du umiddelbart godt av ett av landets sterkeste sikkerhetsfagmiljøer.

– Med en egen SOC får man aldri den samme erfaringen med å håndtere sikkerhetshendelser som om du kjøper det som en tjeneste. Vi opparbeider oss kontinuerlig erfaring ved å håndtere hendelser hos ulike kunder, som vi kan dra nytte av neste gang noe skjer, sier leder for Ateas Incident Response Team, Vegard Kjerstad.

Hva gjør en SOC?

En SOC (Security Operations Center) er en avdeling eller sentralisert funksjon i en virksomhet, som har som oppgave å overvåke IT-systemer og nettverk for sikkerhetsrelaterte hendelser. Formålet er å detektere og forhindre ondsinnet aktivitet, samt etterforske det som virker mistenkelig. Oppstår sikkerhetshendelser, for eksempel digital utpressing, er det SOC som tar de første grepene for å redusere skadeomfanget. Et Incident Response Team (IRT) rykker ut for å håndtere angrepet videre, og jobber med skadebegrensning, opprydding, og med å få systemene tilbake til normal drift så raskt som mulig. Med Atea SOC+ får du sikkerhets-overvåkningen levert som en tjeneste.

Slik fungerer Atea SOC+

SOC+ er en kostnadseffektiv døgnbemannet overvåkingstjeneste som baserer seg på Nasjonal Sikkerhetsmyndighets råd om IKT-sikkerhetstiltak.

Slik overvåker våre sikkerhetseksperter dine IT-systemer, avlaster IT-avdelingen og sørger for at du har de beste forutsetninger for å komme raskt i gang igjen etter et cyberangrep:

1 Innsamling av data fra alle relevante loggkilder

Loggdata fra servere, nettverk, brannmur, klienter og andre relevante kilder samles og overvåkes kontinuerlig av Ateas SIEM-verktøy (Security Information and Event Management).

2 Sette dataene i en sammenheng for å oppdage unormale hendelser

Dataene sammenstilles for å i sanntid oppdage alle unormale hendelser, aktiviteter og brukeratferd på tvers av alle systemer.

3 Analysere dataene for å se om noe krever oppfølging

Avanserte algoritmer, automatiserte regelsett, maskinlæring (ML) og kunstig intelligens (AI) brukes for å oppdage hendelser man ellers kanskje ikke ville oppdaget. Mistenkelige hendelser blir analysert og vurdert av våre sikkerhetseksperter, som avgjør om noe bør følges opp.

4 Sikkerhetseksperter hjelper til umiddelbart når noe skjer

Atea har et stort, profesjonelt team som jobber dedikert med IT-sikkerhet. Kombinert med vår brede ekspertise innenfor for eksempel nettverk og database, gjør dette at vi kan få systemene raskt opp igjen etter en sikkerhetshendelse.

5 Sikkerhetsrådgiver

Med SOC+ får bedriften sin egen sikkerhetsrådgiver, og gjennom månedlige møter og løpende dialog er du alltid oppdatert på trussel-bildet. Sammen med kunden vil sikkerhetsrådgiveren gå gjennom rapporter fra SOC og komme med forslag til forbedringstiltak.

Sertifiseringer

Atea IRT er godkjent av NSM. Elementene i SOC+ inneholder til enhver tid de gjeldende sertifiseringer, som blant annet ISO 27001 og ISO 9001, og Ateas ledelsessystem for miljø er sertifisert i henhold til ISO 14001:2015.

Atea jobber bevisst med miljørettede tiltak for kontinuerlig å redusere vårt eget CO2-utslipp. Vi kjøper opprinnelsesgaranti for all energi som forbrukes på våre datarom i Norge.

Vil du vite mer om Atea SOC+

og hvordan din bedrift kan få tilgang til landets ledende sikkerhetseksperter?

Ta kontakt på sikkerhet@atea.no for en uforpliktende prat

ATEA

atea.no/it-sikkerhet