



Cyberdefense



Säkra er OT-miljö



En strategisk guide

Vad beslutsfattare behöver veta om hur man stärker skyddet av OT i ett snabbt föränderligt hotlandskap.

02 OT-säkerhet är inte längre en ny fråga - det är en affärskritisk prioritet

03 OT-system finns överallt

04 Förstå grunderna

05 Vanliga riskfaktorer inom OT-säkerhet

06 Varför OT-säkerhet är viktigare än någonsin

07 De största utmaningarna

08 Att överbrygga klyftan: Samordna IT och OT för bättre säkerhet

09 Vikten av OT-specifik styrning

10 Attackvektorer och bästa praxis

11 Viktiga steg mot proaktiv och helhetsorienterad OT-säkerhet

14 Förstå AI:s roll i en sammankopplad industri

15 Så här hjälper vi dig

17 Framåtblick: Så framtidssäkrar du

18 Förbered dig för nästa våg av OT-cyberhot

19 Hur NIS2 påverkar era säkerhetsbehov

21 Från bedömning till åtgärd: Bygg en strategisk OT säkerhetsresa

22 Ackrediteringar och meriter

23 Orange Cyberdefense - vilka är vi?

Från bedömning till åtgärd: Bygg en strategisk OT säkerhetsresa

21



17

Framåtblick:
Så framtidssäkrar du

OT-säkerhet **är inte längre** en ny fråga - det är en affärskritisk prioritet

Det sker en omfattande digital omställning i Sverige inom infrastruktur och industri sektorer. När fler organisationer omfamnar uppkoppling och automation, blir systemen som styr fysiska system och maskiner – även kallat Operational Technology (OT) – alltmer integrerade med IT-nätverk. Detta skapar stora möjligheter, men utsätter också organisationer för nya och allt större cyberrisker.

En framgångsrik attack på OT-system få verkliga konsekvenser – från stoppad produktion till hot mot samhällstjänster. I dagens hotlandskap är OT-säkerhet inte bara en teknisk fråga. Det är en strategisk prioritet som förtjänar full uppmärksamhet från både företagsledare och styrelser.

Oavsett bransch är det avgörande att se över sina OT-miljöer för att skydda intäkter, rykte och motståndskraft. Denna guide erbjuder strategiska insikter, verkliga exempel och konkreta rekommendationer som hjälper dig att fatta välgrundade beslut för att stärka din organisations långsiktiga säkerhetsläge.

Oavsett om du precis har påbörjat din resa eller vill stärka befintliga insatser, hoppas vi att denna guide kommer att inspirera till handling och stödja din strategiska plan mot att skapa en mer motståndskraftig organisation.

Vi måste agera nu.



Kåre Nordström
Managing Director
Orange Cyberdefense Sweden

OT-system finns överallt

Vi tenderar ofta att tänka på "Operational Technology" som teknik som styr industriell bearbetning och produktion – vilket namnet antyder. Men OT omfattar mycket mer än så.

Faktum är att OT-system finns i många olika typer av branscher och organisationer.



Vad är OT-säkerhet?

Till skillnad från traditionella IT-system, som uteslutande hanterar data och applikationer, är OT-system direkt involverade i kontroll och övervakning av fysiska operationer. Dessa system finns överallt, både inom offentlig och privat sektor. Till exempel i produktion, eldistribution, energihantering, vattenrening, ventilation, värme, kyla, tryckluft och mycket mer.

OT-säkerhet fokuserar på att skydda systemen från cyberhot som kan orsaka driftstörningar, utrustningsfel eller säkerhetsrisker. En högre nivå av OT-säkerhet krävs även för att uppfylla nya lagkrav såsom NIS2 och DORA.

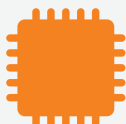


Hur och varför IT- och OT-säkerhet skiljer sig

	IT Security	OT Security
Tillgänglighetskrav	Medel – viss fördröjning accepteras	Väldigt hög
Krav i realtid	Fördröjningar accepteras	Kritisk
Komponentlivslängd	3-5 år	Upp till och över 20 år
Tillämpning av patchar eller ändringar	Regelbunden / schemalagd	Långsam / sällsynt / kräver underhållsfönster
Säkerhetstestning / granskning	Schemalagd och obligatorisk	Schemalagd och obligatorisk
Säkerhetsmedvetenhet	Hög / mogen	Ökande
Huvudfokus	Dataskydd, sekretess	Säkerhet, tillgänglighet
Miljö	Kontorsnätverk, molnsystem	Produktions- och driftnätverk, äldre automationsmiljöer, operativa stödsystem
Risker	Dataintrång, systemavbrott	Utrustningsfel, produktionsstopp, fysiska och miljörelaterade säkerhetsrisker
Säkerhetsstrategi	Schemalagd patchning, mikrosegregering, automatiserade åtgärder	Begränsad patchning, systemsegmentering, manuellt granskade åtgärder

Vanliga riskfaktorer inom OT-säkerhet

Föråldrade system



— Många OT-system körs på **gammal mjukvara** som saknar moderna säkerhetsfunktioner. De är dessutom svåra att uppdatera eller patcha, vilket gör dem extra sårbara.

Säkerhet är en eftertanke

— Historiskt har många OT-system utvecklas med fokus på **tillgänglighet och effektiv drift** - inte säkerhet.



Brist på överblick



— Det saknas ofta tillräcklig synlighet över vilka säkerhetsåtgärder som finns eller saknas i OT-miljön.

Otillräcklig kunskap om regulatoriska krav

— Tillgänglighet och **“att hålla produktionen igång”** prioriteras ofta före standarder (t.ex. NIST SP 800-82, IEC 62443, NIST CSF 2.0, ISO 27001/2). Detta kan leda till brister i styrning, policyhantering och regelefterlevnad.



Otydlig definition av OT

— **Sekundära system** med kritisk betydelse förbises ofta och saknar skydd. Några exempel är Windows-servrar som används av OT-system, OT-relaterade Wi-Fi-nätverk, kylsystem i serverrum, MES-system och fastighetsautomationssystem.



Begränsad eller obefintlig patchning

— Till skillnad från IT-system kan **OT-system inte uppdateras regelbundet** på grund av driftkritiska begränsningar. Vissa OT-system kan inte patchas alls – risken för avbrott är för stor om uppdateringar tillämpas utan omfattande tester.



Sårbar fjärråtkomst

— Ökad uppkoppling mot externa parter och leverantörskedjor **ökar exponeringen mot cyberhot**.



Fysiska konsekvenser

— **Attacker mot OT** kan leda till säkerhetsrisker för personal, miljöskador och total produktionsstopp.



Varför OT-säkerhet är viktigare än någonsin

Traditionellt har cyberkriminella lärt sig att utnyttja svagheter i IT-säkerheten för att ta sig förbi yttre skydd och få tillgång till värdefulla digitala tillgångar som kan krypteras, stjälas eller förstöras. Digitala tillgångar och immateriella rättigheter som kunddata eller kritisk infrastruktur är särskilt utsatta mål.

Vi ser nu även att högkänsliga och affärskritiska OT-miljöer blir uppenbara mål, främst på grund av den ökade kommunikationen mellan IT- och OT-nätverk.



Med ökade krav på OT-säkerhet – som i NIS2, IEC 62443, NIST CSF, ISO 27001/2 och CIS – är efterlevnad inte längre valfritt. Organisationer måste proaktivt implementera säkerhetsåtgärder för att möta dessa krav, bygga resiliens och stärka förtroendet – för att undvika driftstopp, säkra kontinuitet, undvika sanktionsavgifter och skydda förtroendet hos kunder, medborgare och andra intressenter.

Konsekvenserna av otillräcklig OT-säkerhet kan vara:

- **Kostsamma driftstopp**
Välkoordinerade cyberattacker kan stoppa produktionen helt, vilket leder till stora intäktsförluster och skadat varumärke.
- **Säkerhetsrisker**
Attacker mot OT-system kan orsaka fysisk skada på personal eller leda till miljöskador.
- **Regelbrott och sanktionsavgifter**
Bristande efterlevnad av säkerhetskrav kan leda till böter och negativ publicitet.
- **Störningar i samhällskritisk infrastruktur**
Cyberattacker riktade mot OT-system i viktiga sektorer kan orsaka omfattande driftavbrott, fysisk skada och ha påverkan på samhället – genom att slå ut elnät, vattenförsörjning eller transporter.



Vi har nu fått en uppdaterad överblick över vår OT-miljö och identifierat förbättringsmöjligheter inom OT-säkerheten. Samtidigt ser vi stor potential för både förenkling och förbättring av hantering och användning av flera olika system på ett relativt enkelt och kostnadseffektivt sätt. Verkligen en win-win för alla.

— Patrick Gillmor, Automation and Process Engineer, Renova Miljö AB

Renova Miljö AB

Renova Miljö AB är ett bolag som specialiserar sig på avfallshantering och miljötjänster. De fokuserar på hållbar avfallsinsamling, återvinning och destruktion för att stödja miljöskydd och resurseffektivitet. Renova är en samhällskritisk aktör med höga krav på OT-säkerhet.

Inför kraven i NIS2 gav Renova uppdraget till Orange Cyberdefense att genomföra en bedömning av OT-säkerhetsmognad – med syfte att identifiera förbättringsområden och öka medvetenheten hos ledningen.



De största utmaningarna inom OT-säkerhet

Föföruftsedda driftstopp med stora ekonomiska konsekvenser

För många verksamheter är drifttid direkt kopplat till intäkter. Även om många attacker börjar i IT-miljön, ser vi en ökande trend där OT-system angrips direkt.

Lyckas attacken kan det stoppa produktion, orsaka förseningar i leveranskedjan och leda till kontraktbrott med böter som följd. Till skillnad från IT-incidenter, som ofta "bara" leder till data-förlust, kan OT-attacker orsaka fysiska störningar i produktion och infrastruktur.

Inom offentlig sektor kan bristande OT-säkerhet leda till störningar i samhällsviktiga funktioner med omfattande följdverkningar. Cyberattacker mot offentlig infrastruktur blir alltmer sofistikerade, ofta genom att utnyttja kopplingarna mellan IT och OT.

Lyckade attacker kan slå ut elnät, förorena vatten, stoppa kollektivtrafik eller lamslå räddningstjänst. Lösning: Få en tydlig förståelse för hur IT- och OT-system är sammankopplade – det möjliggör att OT-funktioner kan fortsätta även under IT-incidenter.

Brist på kvalificerade OT-säkerhetsexperten

Efterfrågan på OT-säkerhetsspecialister överstiger utbudet. Det är svårt att hitta personal med djup kunskap både inom cybersäkerhet och industriella processer, vilket försvårar implementeringen av effektiva skydd.

Kommunikationsklyftan mellan IT och OT

En av de största utmaningarna är bristen på samarbete mellan IT- och OT-team. IT fokuserar ofta på dataintegritet och konfidentialitet, medan OT fokuserar på tillgänglighet och säkerhet.

Detta leder ofta till:

- Motstridiga säkerhetsprioriteringar
- Djupgående organisatoriska hinder
- Försenad incidentrespons
- Otydligt ansvar för OT-säkerhet
- Olika syn på risk och tekniska begränsningar
- Begränsad kompetens över domängränser
- Att det saknas enhetlig styrning och ansvarsfördelning

Leverantörsrisker och sårbarheter i leveranskedjan

OT-miljöer är beroende av komplexa leveranskedjor: externa partners, tredjepartsleverantörer, entreprenörer och äldre utrustning. Angripare utnyttjar ofta dessa externa kopplingar för att ta sig in. Organisationer bör därför:

- Uppdatera kravspecifikationer och inköpskrav gällande OT-säkerhet.
- Granska och förbättra serviceavtal med tredjepartsleverantörer – och införa tydligt ansvar för säkerhet vid leveranser, underhåll och ändringar.
- Säkerställa att tredje part följer säkerhetspolicys och krav på ett dokumenterbart sätt.
- Implementera strikt åtkomstkontroll för tredje part.
- Etablera säker övervakning och detektion som flaggar för avvikelser i leveranskedjan.
- Kräva SBOM (Software Bill of Materials) från leverantörer – för att få insyn i vilka programkomponenter som ingår i system och produkter, vilket underlättar sårbarhetshantering och incidentrespons.

Lär känna en av våra nordiska OT-säkerhetsexperten



Andreas Jacobsson | OT Solution Architect

Andreas har över 25 års erfarenhet från livsmedelsindustrin, med expertis inom underhåll, projektledning och OT/ICS-nätsäkerhet. Han designar säkra OT-infrastrukturer som stödjer både verksamhetsmål och driftskrav, genomför omfattande säkerhetsbedömningar och säkerställer efterlevnad av branschstandarder. Andreas är en frekvent talare på cybersäkerhetsevener där han förklarar komplexa OT-utmaningar på ett begripligt sätt.

Att överbrygga klyftan: Samordna IT och OT för bättre säkerhet

Noggrann riskhantering är ryggraden i alla säkerhetsstrategier. Det gäller både IT och OT, och båda bör betraktas i relation till varandra. Men det är lättare att säga än att göra, eftersom IT- och OT-säkerhet i de flesta fall befinner sig på mycket olika mognadsnivåer.

Faktum är att OT-säkerheten ofta byggs nästan från grunden, medan IT-säkerhet förfinats över decennier. Denna grundläggande skillnad förstärks av den historiska skiljelinjen mellan IT- och OT-team.

Starkare OT-säkerhet börjar med lokal ansvarsfördelning och globala standarder

En bra strategi är att utse lokala medarbetare som ansvariga för OT-säkerheten på plats, samtidigt som man etablerar ett globalt OT-säkerhetsteam för att utveckla en policy, processer och standarder i nära samarbete med IT.

Viktiga komponenter av en effektiv OT säkerhetsstrategi:

- Skapa separata men nära samordnade säkerhetspolicys för OT och IT
- Främja kommunikation och samarbete
- Uppmuntra regelbunden dialog mellan OT- och IT-team
- Genomför gemensamma IT/OT-riskbedömningar för att identifiera gemensamma sårbarheter
- Samordna incidenthanteringsplaner mellan IT och OT
- Gemensam utbildning med IT- och OT-personal för att bygga ömsesidig säkerhetsmedvetenhet
- Sätt säkerhetsmål och nyckeltal (KPI:er) för både IT och OT
- Standardisera säkra protokoll och autentisering i OT-system där det är tillämpligt

”

I dagens sammankopplade värld är OT-säkerhet inte längre bara en operativ fråga – det är en viktig del av företagsstrategin. Därför måste ledare prioritera resiliens, främja samarbetet mellan IT och OT, och integrera säkerhet i själva kärnan av digital transformation.

Andreas Jacobsson | OT Solution Architect



Vikten av OT-specifik styrning

Eftersom OT skiljer sig från IT på många kritiska sätt går det inte att bara kopiera IT-åtgärder rakt av.

Istället krävs ett OT-specifikt styrningsramverk som effektivt hanterar OT-säkerhetsrisker.

”

När digitaliseringen accelererar ligger en organisations verkliga styrka i dess förmåga att skydda sin kritiska infrastruktur. För företagsledare är det avgörande att anta en holistisk, riskbaserad OT säkerhetsstrategi – för kostnaden av att inte agera är helt enkelt för hög. Framtiden tillhör dem som agerar nu.”

Kåre Nordström | Managing Director



Ett starkt och modernt OT-ramverk bör inkludera:

- En tydlig metod för ledningens övervakning av OT-säkerhetsrutiner.
- Kontinuitetsplanering för OT-system, inklusive strategier för återställning vid händelser.
- Implementering av lokala OT-specifika dokument såsom:
 - OT-säkerhetspolicy
 - Återställning efter en händelse
 - Incidenthanteringsplan
 - Business Continuity-plan
- Regelbundna riskbedömningar i OT-miljöer för att identifiera sårbarheter och prioritera åtgärder.
- Tillgångsregister och klassificering av alla OT-system för att stödja riskbaserat beslutsfattande.
- Utbildning skräddarsydd för OT-personal för att främja en stark cybersäkerhetskultur.
- Övervaknings och avvikelседetektionssystem anpassade för OT-specifika trafikmönster och protokoll.
- Ändringshanteringsprocesser anpassade till OT-miljöer för att säkerställa säkra och kontrollerade uppdateringar.
- Utnämning av en Designated OT Security Officer (DSO) med ansvar för att övervaka OT-cybersäkerhetsstrategin.
- Etablering av lokala ansvarsroller och fortsatt utveckling av ett centralt/globalt OT säkerhetsteam. Detta team bör underhålla och utveckla säkerhetsmallar, policies, procedurer, namngivningskonventioner etc., och samarbeta nära med driftställen och IT
- Införande av en dedikerad roll som OT Site Responsible, med ansvar att övervaka hela produktionsnätverket på plats.

OT-säkerhet i praktiken:

Attackvektorer och bästa praxis

OT-miljöer utvecklas ofta organiskt genom att nya system och komponenter successivt läggs till utan en sammanhållen, övergripande säkerhetsarkitektur.

Denna organiska tillväxt gör det svårt att behålla synlighet, konsistens och kontroll över den totala angreppsytan, som ofta utnyttjas via attackvektorer som:

- Phishing via e-post till IT-enheter som också används för OT
- Social Engineering
- Angrepp i leveranskedjan
- Opatchade IT system integrerade med OT
- Otillräcklig nätverkssegmentering
- Svagt skyddade trådlösa nätverk
- Malware och ransomware
- Flyttbar media
- Felaktiga fjärråtkomstkonfigurationer
- Insiderhot

Best practice

En stark OT-säkerhet bygger på riskbaserad identifiering av all mission kritisk teknik. Under det arbetet kan stödsystem lätt förbises. Om en produktionslinje är helt beroende av en serverpark – då är även dessa servrar OT. Men kan de fungera utan kylsystemet i serverrummet? Nej? Då ska även kylningssystemet betraktas som missionkritisk OT och skyddas därefter.

Så vad kan du göra för att reducera riskerna i era komplexa OT-miljöer och undvika de vanligaste attackvektorer — samtidigt som du bygger en motståndskraftig säkerhetsprofil?

Ha koll på dina OT-system

Alla enheter som upprätthåller/ styr produktion, tillgänglighet och säkerhet måste identifieras och skyddas som OT.

Synlighet är nyckeln

Med god insyn i OT-säkerheten kan du snabbare upptäcka avvikande mönster och misstänkta aktiviteter. Det underlättar också effektiv segmentering och tillgångshantering. Synligheten bör inkludera alla OT-beroenden – allt från faktureringsystem till Wi-Fi, servrar eller kylsystem.

Segmentera dina nätverk

Att separera IT och OT minskar angreppsytan och hindrar spridning av cyberhot mellan miljöer. Segmentering av OT-nätverk bör bygga på noggrant utförda riskbedömningar.

Förstärk fjärråtkomstkontroller

Använd multifaktorautentisering (MFA) och rollbaserad åtkomst för att begränsa exponering mot obehöriga användare.

Inför processer för att hantera sårbarheter

Ha effektiva rutiner för att hantera sårbarheter – genom patchning, kompensationsåtgärder eller borttagning av funktioner. Patchning är inte alltid enda lösningen.

Kontinuerlig övervakning och hotdetektion

Distribuera OT-specifika övervakningslösningar för att upptäcka avvikelser och potentiella hot i realtid.

Implementera ett riskhanteringsramverk

Planera och schemalägg regelbundna riskbedömningar. Dessa behövs för att identifiera sårbarheter och hot – och säkerställa att strategin ständigt anpassas till nya risker.

Definiera roller och ansvar

Effektiv OT-säkerhet kräver tydliga roller och ansvar. Vem äger säkerheten i OT-miljön? Finns processer för incidenthantering? Se till att både IT- och OT-team har gemensam förståelse för säkerhetsmålen och samarbetar för att uppnå dem. Tydligt ansvar ökar effektivitet och minimerar att kritiska åtgärder förbises.



Viktiga steg mot proaktiv och helhetsorienterad OT-säkerhet

Av uppenbara skäl är OT ett attraktivt mål, och moderna organisationer bör agera därefter när utbytet av data mellan IT och OT intensifieras.

En reaktiv hållning – att vänta på attack och sedan reagera – är en farlig strategi som sannolikt leder till omfattande skada: operativt, miljömässigt, ekonomiskt och genom förlorat anseende.

Även om dedikerade OT-attacker än så länge är mindre vanliga än attacker mot IT, är det klokt att fokusera på förebyggande åtgärder mot det som komma skall.

Använd ett etablerat säkerhetsramverk

En av de mest effektiva metoderna att säkra OT är att anta beprövade ramverk såsom CIS, NIST CSF 2.0, ISO 27001/2, ISO 27005, IEC 62443. Dessa ger en strukturerad metod för att skydda industriella kontrollsystem (ICS).

Dessa ramverk hjälper organisationer att identifiera sårbarheter, införa riskhanteringsprocesser och upprätthålla en enhetlig säkerhetsprofil över OT-miljöer – även i internationella sammanhang. De ger också ett gemensamt språk och standardiserade procedurer – vilket är avgörande för god kommunikation mellan IT och OT.

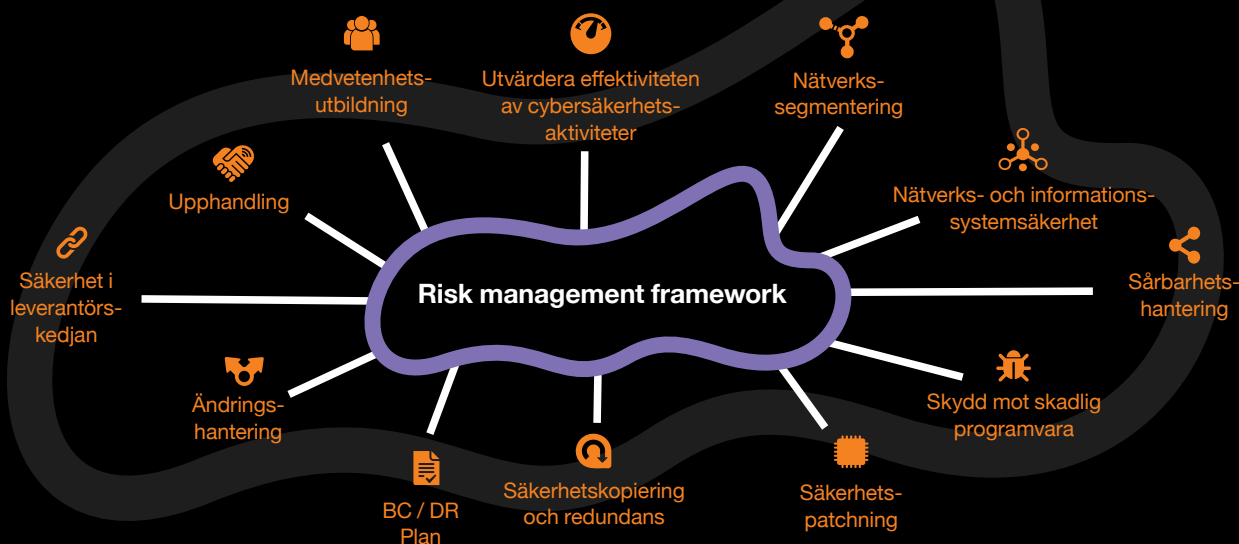
Basera er OT-säkerhet på riskhantering

Att kunna gradera säkerhetsnivån utifrån verksamhetsmål och tillgängliga resurser är nyckeln till framgång. Det bör innehålla:

- **Kontinuerlig övervakning och förbättring** av OT-säkerhetsläget för att säkerställa att det följer utvecklande hot och affärs mål.
- **Register över alla OT-tillgångar** för att identifiera och klassificera kritiska system och sårbarheter.
- **Riskbedömning av potentiella effekter** av cyberhot mot kritiska operationer.
- **Prioritering av säkerhetsinvesteringar** baserat på riskanalyser för att skydda de mest kritiska och utsatta tillgångarna.



En riskbaserad strategi är avgörande för OT-säkerhet



Skydda fjärråtkomst och tredjepartsintegrationer

— Många cyberattacker har sitt ursprung i osäkra fjärrkopplingar eller tredjepartsleverantörer. För att begränsa dessa risker bör organisationer:

- Välja endast en lösning för fjärråtkomst för all support och fjärrkonfiguration.
- Lösningen bör ha övervakad åtkomst och möjlighet att spela in alla sessioner med loggning, godkännande och stöd för MFA.
- Segmentera åtkomst baserat på roller och behov.
- Begränsa fjärråtkomst till tidsbegränsade sessioner.
- Inventera och riskklassa alla tredjepartsaktörer med OT-åtkomst.
- Använd samma fjärråtkomstlösning för intern kommunikation från IT till OT.
- Inför MFA för fjärråtkomst.
- Ingen nätverksåtkomst – använd bara applikationsåtkomst.
- Övervaka fjärråtkomst för misstänkt aktivitet
- Använd godkännandeflöde för fjärråtkomst.

Implementera nätverkssegmentering och flera försvarslager

— Traditionella platta OT-nätverk är mycket sårbara för cyberhot eftersom de ofta ger full åtkomst till alla tillgångar. Genom att införa nätverkssegmentering och flerskiktade säkerhetskontroller minskas risken markant:

- Säkerställ kommunikationsvägarna mellan segment för att bevara realtids-prestanda och säkerhetsintegritet.
- Skapa säkerhetszoner för att begränsa laterala rörelser och isolera kritiska tillgångar.
- Separera IT- och OT-nätverk för att minska angreppsyta.
- Använd brandväggar, Intrusion Prevention Systems (IPS) anpassade för OT och Intrusion Detection Systems (IDS) för att övervaka och kontrollera nätverkstrafik.
- Inför rollbaserad åtkomstkontroll för att begränsa obehörig åtkomst till kritiska system.

Fokusera på medarbetar-medvetenhet och utbildning

— Mänskliga misstag är fortfarande en av de största sårbarheterna inom OT-säkerhet. Kontinuerlig utbildning och träning hjälper anställda att känna igen och reagera på hot på ett effektivt sätt:

- Implementera medvetenhetsutbildning.
- Regelbunden utbildning för personal som hanterar OT-system krävs, för att säkerställa att de kan känna igen och reagera på potentiella hot effektivt.
- Utveckla tydliga protokoll för incidenthantering som vägleder anställda i händelse av attack.
- Använd "tabletop"-övningar (simulerade scenarioövningar).

Kontinuerlig övervakning och hotintelligens

— En proaktiv inställning kräver realtidsövervakning och hotintelligensbaserad detektion. Denna strategi inkluderar:

- Övervaka OT-system för anomalier, hot och prestanda – detta är kritiskt för tidig upptäckt.
- Regelbunden testning och revision av OT-system för att säkerställa att de förblir säkra och motståndskraftiga.
- Passiv skanning och, om möjligt, aktiv detektion med hjälp av samma övervakningsverktyg på OT-enheter.
- Inför övervakning av skadlig kod – särskilt på tillgångar med hög risk för infektion.
- Övervaka obehöriga anslutningar och enheter för att säkerställa full insyn; verktyget bör se all trafik.
- Loggning och övervakning av nätverks- och infrastrukturaktivitet för att upptäcka potentiella säkerhetsintrång.
- Övervakning av obehörig mjukvaruinstallation eller användning, på OT system.

Förbered din krishantering och planera för återhämtning

— Tid är avgörande – särskilt inom OT där en god säkerhetsstrategi måste inkludera planer för att återgå till normal drift så snabbt som möjligt.

- Utveckla en väl definierad incidenthanteringsplan för att upptäcka, reagera på och återhämta sig från cyberincidenter.
- Identifiera, bedöm och analysera risker för att förstå hot, sårbarheter och potentiella effekter – inte bara från cyber-attacker utan även naturkatastrofer, våld på arbetsplatsen, dataintrång och mer.
- Utnäm n nyckelpersoner som ansvariga för incidenthantering och krishantering.
- Definiera tydliga procedurer för hantering av specifika incidenter, inklusive steg för hur hoten identifieras, hur ni hindrar spridning, effektbedömning, kommunikation med intressenter och återställning av verksamheten.
- Rapportera alla betydande cybersäkerhetsincidenter som påverkar OT-system till relevanta myndigheter.
- Etablera kommunikationsprotokoll för incidentteamet, intressenter, anställda, kunder och media. Definiera tydligt vem som har ansvar för kommunikation under en kris, vilken information som ska delas och hur.
- Testa incidenthanteringsplanen regelbundet för att identifiera svagheter eller luckor. Genomför tabletop-övningar och simuleringar för att pröva planens effektivitet. Uppdatera planen baserat på resultat, lärdomar och förändringar i organisation eller bransch.

Ransomwareattacken mot Colonial Pipeline: En varning för OT-säkerhet

Den 7 maj 2021 tog hackergruppen DarkSide sig in i nätverket hos det amerikanska företaget Colonial Pipeline.

Enligt rapporter initierades attacken via användningen av ett komprometterat VPN-lösenord utan multifaktorautentisering.

100 gb data stals, och gruppen lät sedan köra ransomware som krypterade viktiga filer, inklusive sådana relaterade till fakturering och redovisning.



Attacken exponerade kritiska sårbarheter mellan IT- och OT-miljöer, och belyste särskilt de allvarliga följderna av svaga åtkomstkontroller och otillräcklig autentisering. Händelsen visade hur cyberkriminella kan använda IT-system för att ställa till med störningar i viktiga OT-operationer, med omfattande drift. En avgörande lärdom var det akuta behovet att implementera stark multifaktorautentisering (MFA) över alla fjärråtkomstpunkter, särskilt VPN, för att minska risken för komprometterade behörigheter.

Som svar har både statliga myndigheter och privata organisationer tagit konkreta steg för att stärka OT-säkerheten, förstärkt av officiella direktiv och expertråd:

Skärpta regulatoriska krav:

Kort efter attacken utfärdade USA en order om förbättrad cybersäkerhet, som kräver högre standarder, bl.a. för zero trust arkitektur, MFA, kryptering, incidentrapportering och förbättrad riskhantering med särskilt fokus på OT.

Utökade riktlinjer för CISA:

Cybersecurity and Infrastructure Security Agency (CISA) har publicerat flera rekommendationer som betonar vikten av nätverkssegmentering, multifaktorautentisering, realtidsövervakningsverktyg och robusta åtkomstkontroller för OT-nätverk för att begränsa malwarespridning, reducera attackytor och möjliggöra kontinuerlig detektion av anomalier.

Rekommendationer från polismyndigheter:

FBI har lyft fram hotet från ransomware mot OT-system och uppmanar organisationer att anta stark åtkomsthantering, incidenthanteringsplanering och regelbunden medvetenhetsutbildning – som en del av deras OT-säkerhetsstrategier – för att ansvariga för OT-säkerhet ska få bättre utbildning om nya hot och best practice.

Olika åtgärder som fokuserar på samarbete mellan myndigheter, branschorganisationer och cybersäkerhetsleverantörer har också implementerats för att möjliggöra snabbare respons och bättre återhämtning vid incidenter. Koordinerade responsramverk har utvecklats för att förbättra beredskap och motståndskraft.

Alla dessa insatser syftar till att minska sannolikheten och effekten av framtida attacker, med betoning på hur avgörande det är att betrakta OT-säkerhet som en affärskritisk prioritet.

Sammanfattningsvis markerar utvecklingen ett tydligt skifte – att erkänna OT-säkerhet som en väsentlig del av organisations-övergripande riskhantering. Attacken mot Colonial Pipeline fungerade som en väckarklocka och ledde till konkreta förbättringar i cybersäkerheten inom branscher med OT-miljöer.

Förstå AI:s roll i en sammankopplad industri

Industri 4.0 medför ökad uppkoppling och komplexitet, då den fysiska och digitala världen smälter samman genom molntjänster, dataanalys och autonoma system. I detta föränderliga landskap är artificiell intelligens (AI) inte längre valfri – det är en strategisk nödvändighet. För att OT-säkerheten ska hänga med måste vi skifta från statiska kontroller till intelligenta, lärande skyddslösningar.

AI möjliggör realtidsanalys och beslutsfattande på sätt som traditionella metoder inte kan. Istället för att förlita sig på fördefinierade regler och manuella granskningar lär AI sig vad som är "normalt" och flaggar avvikelser som kan indikera en cyberattack, funktionsfel eller insiderhot. Detta blir särskilt viktigt när driftssystem blir mer självoptimerande och mindre beroende av mänsklig övervakning.

Men vi måste också inse att AI används av angripare för att skapa malwar, anpassar sig till sin miljö och riktar in sig på kritisk infrastruktur med precision. För att ligga steget före måste vi anta AI med samma ambition och tillämpa den i detektering, respons och strategisk prognostisering.

Utan framåtblickande säkerhet blir löftet om Industri 4.0 till en risk. Men med rätt användning av AI kan OT-miljöer bli mer motståndskraftiga, adaptiva och säkrare än någonsin tidigare.

Framöver måste ledare inom industri och kritisk infrastruktur ställa sig frågor såsom:

- Hur kan vi säkerställa att vår säkerhet lär, inte bara övervakar?
- Hur tränar vi AI på rätt data – och skyddar den datan från manipulation?
- Vad händer när beslutsfattande automatiseras – och hur bibehåller vi spårbarhet och kontroll?
- Hur kan vi använda AI för att minska responstider utan att tappa helhetsbilden?
- Hur säkrar vi digitala tvillingar, autonoma system och självoptimerande fabriker?

”

Orange Cyberdefense's långa erfarenhet inom OT var ovärderlig – deras djupa förståelse skapade förtroende, uppmuntrade öppen dialog och engagemang genom hela bedömningsprocessen, vilket naturligt ledde till kompetenslyft och en korrekt nulägesbild av vår industriella miljö

— Fawzi Aiboud Nygren, BISO, Volvo Group Trucks Operations

Volvo Group Trucks Operations

Volvo Group Trucks Operations är en division inom Volvo Group som tillverkar och säljer lastbilar, samt hanterar logistik och reservdelar under flera globala varumärken, såsom Volvo, Mack Trucks och Renault Trucks. Verksamheten erbjuder ett brett utbud av tung- och medeltunga lastbilar för olika transport och logistiktillämpningar.

Inför införandet av NIS2 beslutade Volvo Group Trucks Operations att låta Orange Cyberdefense göra en mognadsbedömning av OT-säkerhet på tio strategiskt utvalda anläggningar. Målet var att få bättre insikter i nuvarande OT-miljö och arbeta mer systematiskt med en riskbaserad ansats inom hela organisationen.

V O L V O



Vi hjälper dig stärka din OT-säkerhet

Managerade OT-säkerhetstjänster

Våra managerade OT-säkerhetstjänster är utformade för att erbjuda kontinuerligt skydd, realtidsövervakning, hotdetektion och incidenthantering – samtidigt som dina OT-system förblir säkra.

Detta inkluderar:

- Managerad brandvägg för OT
- Managerad industriell säkerhet [Identify]
- Managerad industriell säkerhet [Detect]
- Managerad hotdetektion [log] IT / OT-mönster
- Managerad end point-skydd för OT

Vår expertis sträcker sig över olika vertikaler och sektorer, och vi erbjuder en rad tjänster utvecklade för att skydda såväl fysiska som digitala aspekter av OT-miljöer enligt högsta marknadsstandard.

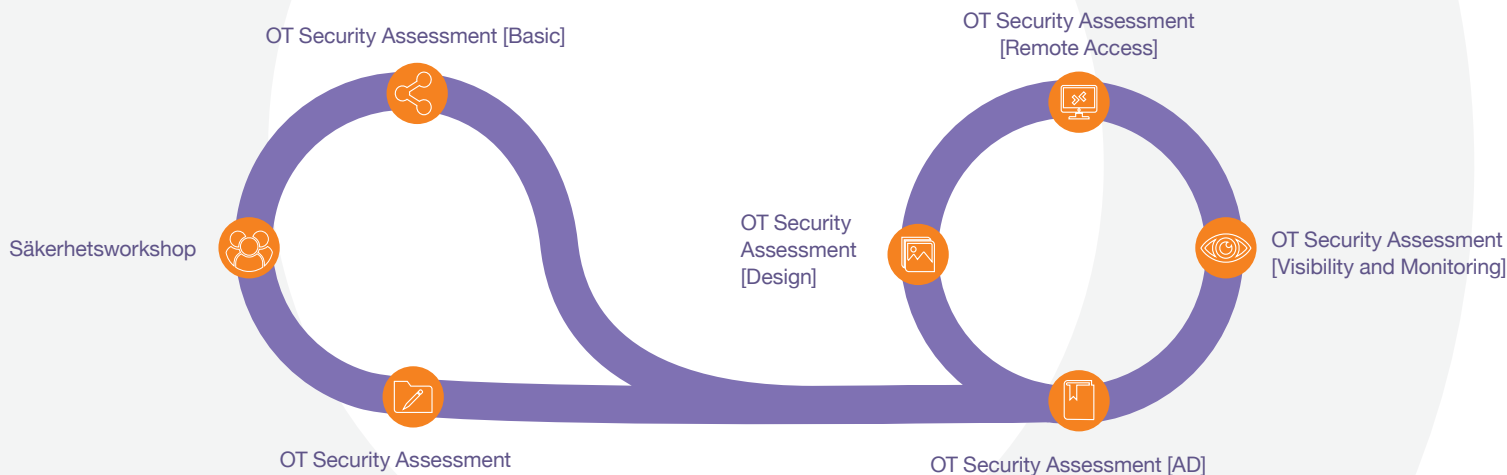
Advisory OT Security Services

I en tid när många organisationer kämpar med att rekrytera och behålla duktiga OT-säkerhetsspecialister erbjuder vi en alternativ väg. I Norden har vi byggt ett starkt team av erfarna säkerhetskonsulter redo att hjälpa till att höja ert försvar avsevärt.

Några nyckeltjänster från våra säkerhetskonsulter:

- GRC för OT
- OT Security Officer som en tjänst

Vår OT-nulägesanalys



Lär känna en av våra nordiska OT-säkerhetsexperten



Aastha Rohilla | OT/ICS Security Consultant

Som säkerhetskonsult arbetar Aastha med att utvärdera, bygga och utveckla säkerhetsinfrastrukturer samt ge strategisk rådgivning som stödjer kundernas affärsmål.

Aastha har erfarenhet av att arbeta med nätverks- och molnbaserad säkerhet och har en bred förståelse för informationssäkerhet, från nätverk och programvara till IT-rätt och organisatorisk säkerhet. Med sin kombination av tekniskt djup och strategiskt perspektiv bidrar Aastha till att skapa lösningar som stärker både säkerhet och verksamhetsnytta.

OT-nulägesanalyser – ett viktigt första steg i rätt riktning

Medan IT-säkerheten haft flera decennier på sig att mogna, vilar ofta behovet för OT-säkerhet på en mycket mindre standardiserad grund av oöverskådade legacy system och låg nätverkstransparens.

Frågan "vad kommunicerar med vad och varför?" är avgörande för att komma rätt ut ur startblocken.



”

16

Vägen till en motståndskraftig och säker framtid vilar på strategisk vision och beslutsam handling. OT säkerhet är inte bara en IT fråga – det är en kärnaffärsrisk som kräver ledarskap, samarbete och framåtblickande tänkande.

Martin Blak | Senior Trusted Advisor

Nulägesanalys med säkerhetsstatus och rekommendationer

- Få djupare insikter om er säkerhetsstatus och mest angelägna säkerhetsbehov
- Ta nästa steg i att identifiera och prioritera hur ni bäst förbättrar er OT-säkerhetsnivå
- Göra en säkerhetsanalys av er OT-nätverkssammanhang
- Förstå medarbetarnas och leverantörers medvetenhet och mognadsnivå

Vad vi gör:

- Inledande kickoff med dina ansvariga experter
- Utförlig informationsinsamling genom intervjuer och dokumentgranskning
- Site walkdowns
- Granskning av OT-nätverkssäkerhetsdesign baserat på insamlad information
- Detaljerad bedömningsrapport med lista över tillgångar, sårbarheter, hot och handlingsbara rekommendationer inom områdena människor, processer och teknik

Vad du får ut av det:

- Insikt i er OT-säkerhetsstatus
- Datadriven analys med praktiska rekommendationer för att förbättra OT-säkerheten
- En bedömningsrapport som beskriver det vi upptäckt, insikter och rekommendationer



Värdefulla säkerhetsinsikter
Bedömningsmetoder baserade på
branschstandarder



Handlingsbara rekommendationer



Skräddarsydd rapport



Tillgång till specialister
inom OT-säkerhet



Erkänd aktör
Orange Cyberdefense är en ledande
Managed Security Service Provider

OT Showroom upplevelsen i Lyon

På Orange Cyberdefense's OT Showroom i Lyon erbjuder vi en omfattande, skräddarsydd, interaktiv och praktisk upplevelse där beslutsfattare kan se OT-säkerhet i praktiken. Denna unika anläggning visar de senaste säkerhetsteknologierna och erbjuder en realtidsdemonstration av hur våra lösningar fungerar för att skydda kritiska system. Besökare kan delta i praktiska övningar, observera simulerade cyberattacker och lära sig hur man hanterar säkerhetsutmaningar i sina egna miljöer.



Framåtblick: Så framtidssäkrar du

När företag fortsätter att digitalisera och anta ny teknik måste säkerheten utvecklas för att möta framväxande hot i det snabbt föränderliga hotlandskapet.

Djupare integration mellan IT och OT

— När företag ökar kommunikationen mellan IT och OT för effektivitet och data-delning ökar också de säkerhetsrisker som följer med integrationen. Effektiva säkerhetsstrategier måste sömlöst funka för båda världarna.

Strängare regulatoriska krav

— Framtida regelverk ställer ökade krav på **säkerhet i OT-miljöer**. Organisationer måste agera inte bara för att skydda sin drift, utan också för att möta juridiska och compliancekrav.

Kompetensbrist och utbildning

— Eftersom OT-säkerhet blir mer komplex, växer behovet av specialiserad kompetens. Organisationer måste investera i utbildning och rekrytering av medarbetare med kunskap i både IT och OT.

Arkitektoniska skiften

— Koncept som **Zero Trust** tillämpas även i OT-miljöer. Detta kräver både tekniska och organisatoriska anpassningar för att säkerställa att ingen enhet eller användare implicit har förtroende att få tillgång till kritiska resurser.

Tillväxt av IoT och Industri 4.0

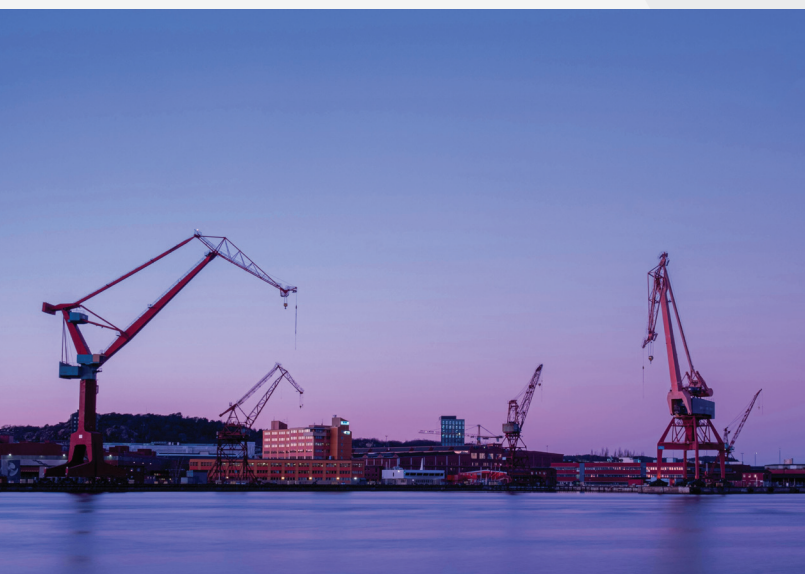
— Ökningen av IoT-enheter i industriella miljöer ställer nya krav på säkerhet. **Fler uppkopplade enheter utökar attackytan** och kräver avancerade skyddsåtgärder.

Avancerade hot och attackvektorer

— Cyberkriminella blir mer sofistikerade och använder tekniker som ransomware och leveranskedjeattacker för att attackera OT-miljöer. Framtida säkerhetssystem måste kunna hantera dessa utvecklade hot.

AI och IoTs påverkan på OT säkerhet

— AI och IoT är dubbelsidiga svärd inom **OT-säkerhet**. Medan de möjliggör högre driftseffektivitet, introducerar de också nya sårbarheter. AI-driven prediktivt underhåll och IoT-enheter kan utnyttjas om de inte är ordentligt säkrade. Eftersom IoT-enheter sprids i industriella miljöer blir **skyddet av dessa enheter allt viktigare**.



Förbered dig för nästa våg av OT-cyberhot

- Ett systematiskt och kontinuerligt cybersäkerhetsprogram
- Konstant bedömning av risker, IT/OT säkerhetsinsatser och måluppfyllnad
- Efterlevnad av regleringar
- Investeringar i säkerhetsteknik som kan följa den snabba förändringstakten
- Antagande av en säkerhetsmodell som antar hot både internt och externt
- Säkerställ att det finns ett kontinuerligt utbildningsprogram för personal – särskilt för dem som ansvarar för OT system – så att de hålls uppdaterade med de senaste säkerhetsmetoderna och trenderna



Att genomföra en nulägesanalys handlar inte bara om att identifiera säkerhetssluckor – det handlar om att bygga en motståndskraftig grund för framtiden. Genom att utvärdera vår OT-säkerhet har vi kunnat genomföra meningsfulla förbättringar och säkerställa starkare försvar och att vi uppfyller kraven för NIS2 och NIST.

— Julian Beauregard Camp, Subject Matter Expert OT, EcoDataCenter

EcoDataCenter

EcoDataCenter är en datacenterleverantör som fokuserar på hållbar och energieffektiv infrastruktur. De erbjuder säkra, tillförlitliga hostinglösningar med fokus på att minimera miljöpåverkan genom användning av förnybar energi och innovativa kyltekniker.

År 2021 bad EcoDataCenter Orange Cyberdefense att bedöma dess OT-säkerhet och använde kunskapen för att genomföra förbättringar. Bedömningsprocessen upprepades 2024 för att utvärdera och få en uppdaterad nulägesbild av mognadsgraden.

EcoDataCenter



Hur NIS2 påverkar era säkerhetsbehov

NIS2-direktivet har lagstadgats av 27 EU länder. Eftersom direktivet riktar sig särskilt mot organisationer som arbetar med kritisk infrastruktur har det stort fokus på krav för OT-säkerhet.

Tekniska och metodologiska krav ur OT-perspektiv:

01

OT-säkerhetspolicy

02

OT-
riskhanteringspolicy

03

Incidenthantering

05

Säkerhet i
leveranskedjan

04

Business
continuity /
krishantering
med OT-fokus

06

Säkerhet i
OT-nätverk och
OT-system

07

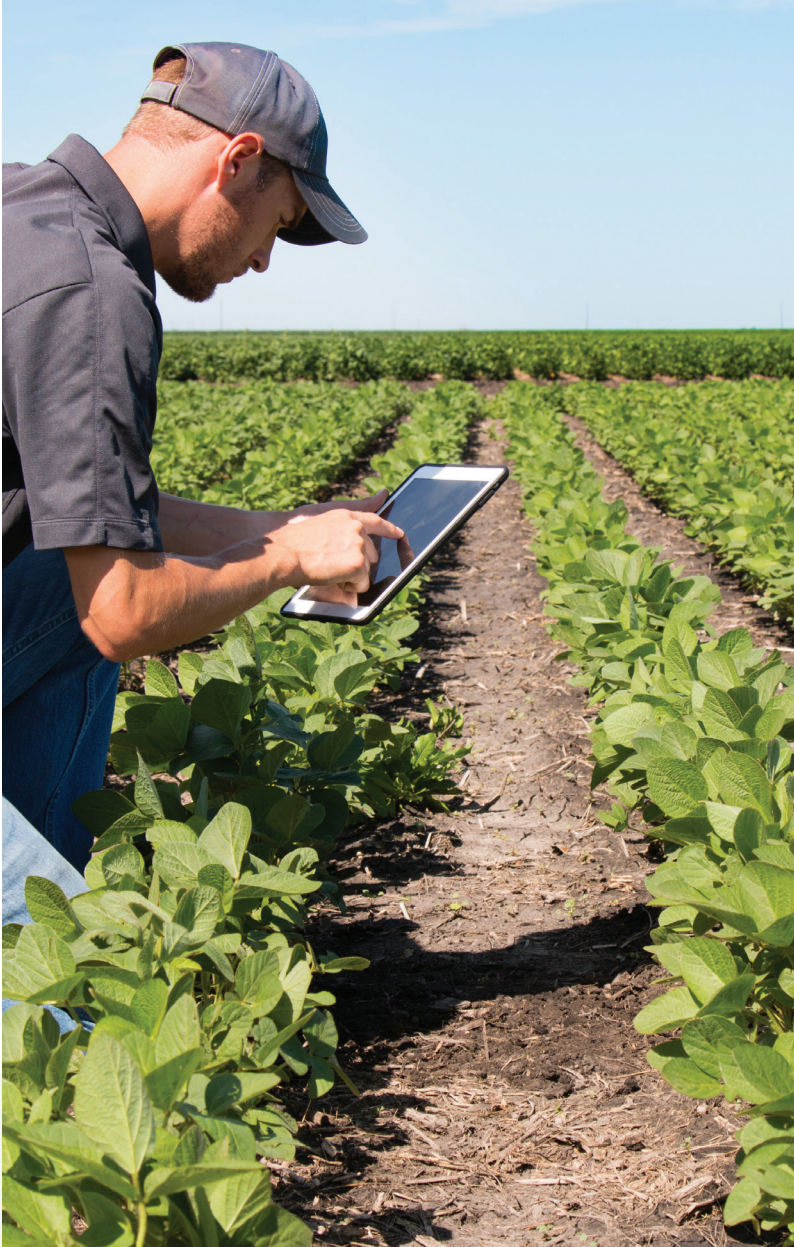
Utvärdera
effektiviteten i
OT-cybersäkerhets-
riskhantering

Lär känna en av våra nordiska OT-säkerhetsexperten



Carsten Lyth | Business Area Manager, OT Security

Carsten har mer än 30 års erfarenhet av att arbeta med OT-system inom industrisektorn. Han har haft olika roller, bland annat projekt-ingenjör, chef för teknikverksamhet och ledarskapspositioner där han lett tekniska projekt och organisationer i komplexa och krävande industriella miljöer. Hans omfattande bakgrund har gett honom djup förståelse för kunders varierande processer, tekniska miljöer och affärskritiska behov – från verkstadsgolvet till ledningsnivå. Han har också arbetat som chef för standardisering och fokuserat på industrisamarbete och utveckling av gemensamma riktlinjer och tekniska standarder. De senaste tre åren har Carsten varit chef för OT-säkerhet på Orange Cyberdefense, där han hjälper kunder att förstå, skydda och utveckla sina industriella system i en alltmer digitaliserad och hotutsatt värld.



”

Effektiv OT-säkerhet är en affärsmöjliggörare, inte bara en teknisk nödvändighet. Den kräver visionärt ledarskap, proaktiv riskhantering och ett enhetligt angreppssätt över alla nivåer i organisationen. De som leder med förutseende kommer att skydda sina verksamheter och säkra sin konkurrenskraft.

Carsten Lyth | Business Area Manager, OT Security

08

Grundläggande cyberhygien och säkerhetsutbildning

10

Säkerhet i personalresurser (HR) inom OT

09

Kryptografi

11

Åtkomstkontroll

12

Hantering av OT-tillgångar

13

Miljö och fysisk säkerhet kopplad till OT

Från bedömning till åtgärd: Bygg en strategisk OT säkerhetsresa

Denna färdplan ska anpassas efter affärsmålen, adressera de mest kritiska sårbarheterna och beskriva de steg som krävs för att uppnå en säker OT-miljö.

Börja med att bedöma det aktuella säkerhetsläget, identifiera kritiska tillgångar och implementera en riskhanteringsmodell. Färdplanen bör sedan utvecklas över tid för att ta hänsyn till ny teknik, förändrade affärsbehov och framväxande hot.

Viktiga insikter för beslutsfattare

För beslutsfattare är förståelsen för OT-säkerhetens betydelse det första steget mot att skapa en motståndskraftig och säker industriell miljö. Några nyckelpunkter:

- OT-säkerhet är inte valfri – det är avgörande för affärskontinuitet och riskhantering
- Ett nära samarbete mellan IT och OT team är en förutsättning för framgång
- Framtidssäker OT-säkerhet kräver kontinuerliga investeringar i teknik, utbildning och incidenthantering

Så kommer du igång med OT säkerhet

Om du befinner dig i början av din OT nulägesanalys bör du starta med att bedöma din nuvarande riskbild. Samarbeta med experter för att identifiera potentiella sårbarheter och börja implementera rätt lösningar för att skydda din OT miljö. Använd resurser som:

- OT säkerhetsbedömningar
- Ethical Hacking
- Managerade säkerhetstjänster

Stärk OT-säkerheten genom efterlevnad och ledarskap

Med införandet av NIS2 direktivet har kraven på OT-säkerhet skärpts avsevärt – särskilt vad gäller styrning, riskhantering, regelefterlevnad och incidenthantering. För många organisationer innebär detta att man behöver ta tag i äldre industriella miljöer som aldrig designats för dagens cybersäkerhetskrav.

Trots investeringar i ny teknik och ökad effektivitet är den befintliga infrastrukturen ofta fortsatt sårbar. Här blir ledarskapsengagemang en kritisk framgångsfaktor. Organisationer som hanterar OT-säkerhet som en strategisk styrelsefråga upplever färre intrång, snabbare respons och bättre kontroll över sin riskexponering.

Samtidigt innebär integreringen av OT och IT stora affärsfördelar – men även nya säkerhetsutmaningar. Genom att integrera säkerheten i den övergripande företagsstyrningen stärker man inte bara regelefterlevnaden (t.ex. NIS2), utan förbättrar även motståndskraften och minskar antalet incidenter. De mest mogna organisationerna rapporterar genomgående färre säkerhetshändelser – ett tydligt bevis på att en strategisk, ledarskapsdriven ansats ger resultat.

Viktiga insikter:

- NIS2 ställer striktare krav på OT säkerhet – särskilt inom styrning, regelefterlevnad och riskhantering
- Äldre OT miljöer utgör en betydande säkerhetsrisk och kräver proaktiva åtgärder
- Ledarskapsdriven strategi för OT säkerhet ger färre incidenter och ökad motståndskraft
- IT/OT integration skapar affärsnytta men kräver aktiv säkerhetshantering

Varför är det så viktigt att göra rätt från början?

Misstag i de inledande faserna kan skapa sårbarheter som är svåra och kostsamma att åtgärda senare. En strukturerad start hjälper dig att:

- Identifiera och prioritera risker
- Förhindra dyra misstag
- Skydda personal och processer
- Säkerställa driftkontinuitet
- Uppfylla regelverk
- Bygga en stark säkerhetskultur

Ackrediteringar och meriter

I cybersäkerhetsbranschen är internationella certifieringar en tydlig indikation på kompetens, tillförlitlighet och kvalitetsnivå.



Erkänd branschledare

Orange Cyberdefense har upprepade gånger blivit erkänd som ledare inom Managed Detection and Response (MDR) av ledande analytiker som Gartner, Forrester, IDC, Omdia och Everest Group. Dessa utmärkelser bekräftar vår tekniska kompetens, kundnöjdhet och operativa leveransförmåga.



Beprövade standarder

Vi följer globala standarder såsom ISO, SOC2 och CREST – vilket säkerställer att våra säkerhetsrutiner är robusta och transparenta. Dessa omfattar allt från incidenthantering till hotintelligens och kontinuerlig förbättring. Vår efterlevnad av dessa standarder garanterar att våra tjänster håller högsta kvalitet.



En pålitlig partner

Att välja Orange Cyberdefense innebär att samarbeta med en cybersäkerhetspartner som är erkänd för sin integritet, expertis och sitt engagemang att skydda kunder globalt. Våra långsiktiga samarbeten med ledande säkerhetsorganisationer är ett bevis på vårt fokus på kvalitet och ansvar.

**Vi siktar på de
högsta standarderna
för kvalitet.**

**Men ta inte bara vårt
ord för det.**

Gartner

Gartner listade Orange Cyberdefense som en representativ leverantör i Market Guide för Managed Detection and Response, Managed Security Services, Digital Forensics & Incident Response, Threat Intelligence och OT-säkerhet.

OMDIA

Omdia betraktar Orange Cyberdefense som en ledare inom globala IT-säkerhetstjänster: "Leverantören har visat stort engagemang, strategisk vision och kapacitet att leverera lösningar inom olika end-to-end säkerhetstjänstkategorier, inklusive moln, endpoint, OT, SASE, infrastruktur och säkerhetsintelligens."

FORRESTER

Forrester rankar Orange Cyberdefense som en ledare. Enligt Forrester-rapporten: "Orange Cyberdefense imponerar på sina kunder med högkvalitativa tekniska tjänster. Orange Cyberdefense fortsätter att utöka sina kapabiliteter inom molnsäkerhet och Managed Detection and Response."

IDC

IDC placerar Orange Cyberdefense i kategorin Ledare i IDC Marketscape: European Managed Detection and Response Services 2024 Vendor Assessment. "Orange Cyberdefense erbjuder ett omfattande utbud av hanterade och professionella säkerhetstjänster, vilket gör det möjligt för dem att hjälpa organisationer att heltäckande minska cybersäkerhetsrisker."

Everest Group RESEARCH

Everest Group erkände Orange Cyberdefense som ledare inom Managed Threat Detection. I sin forskning bedömer Everest Group 27 MDR-everantörer globalt som ingår i MDR Services PEAK Matrix® Assessment.



Cyberdefense - vilka är vi?

Global positioning

Orange Cyberdefense är en ledande europeisk aktör inom cybersäkerhet och hanterade säkerhetstjänster – med över 25 års erfarenhet. Vi levererar rådgivning, lösningar och tjänster till kunder världen över, och är erkända av bl.a. Gartner, Forrester och IDC som en av världens främsta MSS leverantörer.

Vår globala Threat Intelligence avdelning består av 250+ analytiker, spridda över:

- 17 Security Operations Centers (SOCs)
- 15 CyberSOCs
- 11 Computer Emergency Response Teams (CERTs)
- 4 scrubbing center för att hantera DDoS attacker

Vi samlar och analyserar data från över 500 informationskällor – dygnet runt, året om.

Lokal förankring i Norden

I Norden består vårt team av cirka 500 medarbetare fördelade mellan kontor i:

- Köpenhamn & Århus (Danmark)
- Stockholm, Malmö, Göteborg & Sundsvall (Sverige)
- Oslo (Norge)

Våra kunder inkluderar multinationella företag, offentliga

En global tillväxtresa

- +3 100 anställda globalt
- 50 000 kunder världen över, varav 6 000 är större företag
- Stabil ekonomisk tillväxt över tid
- Global omsättning 2024: 1,2 miljarder euro

En del av Orange Group

Orange Cyberdefense är en del av den globala franska telekommunikationskoncernen Orange, som har:

- 137 000 anställda
- 296 miljoner kunder världen över
- Global omsättning 2024: 40,3 miljarder euro

För mer information:

orangecyberdefense.com/se

Kontakta oss

✉ info@se.orangecyberdefense.com

☎ +46 10 202 20 13

