CYBERÖVERVAKNING · SVENSKA

Onboarding av cyberövervakning

Onboarding av cyberövervakning är både teknisk och organisatorisk. Datakällor ska anslutas, men lika viktigt är att beslutsvägar och ansvar fungerar när en relevant händelse upptäcks.

PUBLICERAD	3 september 2026
FÖRFATTARE	Siren Tech
LÄSTID	5 min läsning

Inventera det som ska omfattas

Samla en aktuell bild av användare, Windows-, macOS- och Linux-enheter, Microsoft 365- och Google Workspace-miljöer samt loggkällor som kan bidra med säkerhetssignaler. Markera vad som är verksamhetskritiskt.

Verifiera licenser och teknisk åtkomst

Kontrollera vilka Microsoft- och Google-licenser som finns, vilka funktioner de ger och vem som äger administrationen. Åtkomst ska begränsas till det som krävs och kunna granskas och återkallas.

Utse kontaktpersoner och ersättare

Dokumentera vem som kontaktas för tekniska frågor, verksamhetsbeslut och ledningseskalering. Ange ersättare och en väg framåt när ordinarie kontakt inte svarar.

Besluta responsmandatet

Gå igenom åtgärd för åtgärd: isolering av endpoint, blockering av indikator, avstängning av konto och andra relevanta insatser. Ange vilka som får ske direkt och vilka som kräver godkännande.

Testa innan överlämning

Bekräfta att överenskomna datakällor skickar information, att kontaktvägen fungerar och att ansvariga förstår rapportering och eskalering. Dokumentera avvikelser innan tjänsten går in i normal drift.

Källor och vidare läsning

Läs om Siren Techs cybersäkerhet

Boka en onboarding-bedömning

CYBER MONITORING · ENGLISH

Onboarding cyber monitoring

Onboarding cyber monitoring is both a technical and organisational process. Data sources must be connected, but it is equally important that decision paths and responsibilities work when a relevant event is detected.

PUBLISHED	3 September 2026
AUTHOR	Siren Tech
READING TIME	5 min read

Inventory what will be covered

Create an up-to-date view of users, Windows, macOS and Linux devices, Microsoft 365 and Google Workspace environments, and log sources that can contribute security signals. Mark what is critical to the business.

Verify licences and technical access

Check which Microsoft and Google licences are available, which functions they provide and who owns the administration. Access should be limited to what is required and must be reviewable and revocable.

Appoint contacts and deputies

Document who is contacted for technical questions, business decisions and management escalation. Specify deputies and a path forward when the regular contact does not respond.

Decide the response mandate

Review each action: endpoint isolation, indicator blocking, account suspension and other relevant measures. State which actions may happen immediately and which require approval.

Test before handover

Confirm that the agreed data sources send information, that the contact route works and that those responsible understand reporting and escalation. Document deviations before the service enters normal operation.

Sources and further reading

Read about Siren Tech's cybersecurity services

Book an onboarding assessment