CYBERÖVERVAKNING · SVENSKA

Incidentrespons i praktiken

Incidentrespons fungerar bäst när kontaktvägar, beslut och tekniska behörigheter redan är överenskomna. Då behöver teamet inte börja förhandla om ansvar mitt i en säkerhetshändelse.

PUBLICERAD	3 september 2026
FÖRFATTARE	Siren Tech
LÄSTID	7 min läsning

1. En signal behöver sammanhang

En teknisk signal är en utgångspunkt, inte ett färdigt incidentbeslut. Den behöver bedömas mot berörd enhet, identitet, tidpunkt och andra tillgängliga händelser innan rätt prioritet kan sättas.

2. Triage skiljer brus från avvikelse

Triage avgör om händelsen kan stängas, behöver följas eller ska eskaleras. Bedömningen och underlaget ska dokumenteras så att nästa person förstår vad som har observerats.

3. Mandatet styr åtgärden

Ett avtalat mandat kan tillåta att en endpoint isoleras, en indikator blockeras eller ett konto stängs av. Åtgärder utanför mandatet går till kundens utsedda beslutsfattare.

För varje åtgärdstyp bör avtalet ange vem som beslutar, vem som utför, hur kunden kontaktas och vad som händer om kontaktpersonen inte svarar.

4. Återställning är en egen arbetsfas

Containment begränsar händelsen. Forensik och återställning kan kräva ytterligare arbete och ska därför vara tydligt inkluderat, begränsat eller separat offererat innan tjänsten startar.

5. Uppföljningen ska gå att använda

Efter incidenten behöver verksamheten förstå vad som hände, vilka åtgärder som genomfördes och vilka öppna risker som återstår. Uppföljningen ska leda till konkreta ägare och nästa steg.

Källor och vidare läsning

Se arbetsflödet

Boka säkerhetsbedömning

CYBER MONITORING · ENGLISH

Incident response in practice

Incident response works best when contact routes, decisions and technical permissions have already been agreed. The team then does not need to start negotiating responsibility in the middle of a security event.

PUBLISHED	3 September 2026
AUTHOR	Siren Tech
READING TIME	7 min read

1. A signal needs context

A technical signal is a starting point, not a complete incident decision. It must be assessed against the affected device, identity, time and other available events before the right priority can be set.

2. Triage separates noise from anomalies

Triage determines whether the event can be closed, needs monitoring or should be escalated. The assessment and supporting information should be documented so that the next person understands what has been observed.

3. The mandate governs the action

An agreed mandate may allow an endpoint to be isolated, an indicator to be blocked or an account to be disabled. Actions outside the mandate are referred to the customer's designated decision-maker.

For each type of action, the agreement should state who decides, who carries it out, how the customer is contacted and what happens if the contact person does not respond.

4. Recovery is a separate phase

Containment limits the event. Forensics and recovery may require additional work and should therefore be clearly included, limited or quoted separately before the service begins.

5. Follow-up must be usable

After the incident, the organisation needs to understand what happened, which actions were taken and which open risks remain. The follow-up should lead to concrete owners and next steps.

Sources and further reading

See the workflow

Book a security assessment