GIDS

De complete gids voor incident response services

Reactietijd, kosten, NIST/SANS-fasen, retainer vs ad-hoc, NIS2-meldplicht en selectiecriteria. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Cyberincidenten in Nederland nemen toe, de schade stijgt en de meldplicht wordt strenger. Dit zijn de feiten die je moet kennen.

121

Unieke ransomware-incidenten in Nederland in 2024

NCSC Jaarbeeld Ransomware 2024 [1]

EUR 11,5M

Totale financiele schade door ransomware in Nederland (2025), was EUR 1,36M in 2024

NCSC Jaarbeeld Ransomware 2025 [2]

22 dagen

Mediaan dwell time in EMEA -- aanvallers zitten weken ongemerkt in je netwerk

[3]

EUR 270K

Gemiddelde schade per cyberincident voor Nederlands MKB

ESET/Hallo [4]

24 uur

NIS2-meldplicht: vroegtijdige waarschuwing binnen 24 uur na ontdekking

NCSC [5]

50--70%

Meerkosten bij ad-hoc IR ten opzichte van een retainer

[6]

5 dagen

Mediaan dwell time bij ransomware -- aanvallers werken steeds sneller

[3]

24%

Losgeld is slechts 24% van de totale kosten van een ransomware-aanval

ANP [7]

1. Wat is incident response?

Incident response (IR) is het gestructureerd reageren op een cybersecurity-incident -- van detectie tot herstel en evaluatie. Het doel: schade beperken, bewijs veiligstellen, systemen herstellen en herhaling voorkomen.

Bij een ransomware-aanval, datalek of geavanceerde inbraak heb je gespecialiseerde hulp nodig die 24/7 beschikbaar is. IR-dienstverleners combineren digitale forensische expertise (DFIR) met crisismanagement. Ze analyseren hoe een aanvaller is binnengekomen, stoppen de verspreiding, veiligen bewijs voor juridische procedures en helpen je systemen veilig te herstellen [8].

KERNBEGRIPPEN

- **Incident Response (IR)** -- Reactieve dienst bij een actief incident: crisisrespons, containment, forensics en herstel
- **DFIR** -- Digital Forensics & Incident Response: IR plus forensisch bewijs voor rechtszaken en rapportages
- **MDR** -- Managed Detection & Response: preventieve 24/7 monitoring als managed service
- **SOC** -- Security Operations Center: intern of extern team voor monitoring en first-line respons
- **CERT/CSIRT** -- Computer (Security) Incident Response Team: gecoordineerde incidentafhandeling, vaak sectoraal

Kernverschil: MDR is preventief (voorkomen dat het zover komt), IR is reactief (als het al mis is). DFIR voegt forensisch bewijs toe voor juridische doeleinden. In de praktijk bieden veel partijen beide als gecombineerd pakket [9].

2. Waarom is het belangrijk?

De vraag is niet of je wordt aangevallen, maar wanneer -- en of je dan voorbereid bent. Zonder incident response verlies je kostbare uren, bewijs en geld.

DE CIJFERS SPREKEN

In 2024 registreerde het NCSC 121 unieke ransomware-incidenten in Nederland, met ICT (24%) en handel (20%) als meest getroffen sectoren [1]. De totale financiele schade steeg van EUR 1,36 miljoen in 2024 naar EUR 11,5 miljoen in 2025 [2]. Per incident betaalt een gemiddeld MKB-bedrijf EUR 270.000 aan herstel, juridische kosten, stilstand en reputatieschade [4].

Losgeld is slechts het topje van de ijsberg: het vormt gemiddeld 24% van de totale kosten. De overige 76% bestaat uit productie-uitval, forensisch onderzoek, juridische kosten en klantverlies. De totale kosten zijn gemiddeld 7x hoger dan het betaalde losgeld [7].

NEDERLANDSE CASES

INCIDENT	WAT GEBEURDE ER	IMPACT
Universiteit Maastricht (2019)	Clop ransomware, 267 servers versleuteld in 30 minuten. Ransomware zat niet in IR-plan	~EUR 200.000 losgeld betaald (deels teruggevonden door OM in 2022) [10]
Gemeente Hof van Twente (2020)	RDP-poort open met zwak wachtwoord. Geen losgeld betaald	EUR 4,2 miljoen herstelkosten, bijna 2 jaar herbouw [11]
KNVB (2023)	LockBit-aanval, 300 GB data gestolen	~EUR 1 miljoen losgeld betaald [12]
VDL Groep (2021)	105 dochterondernemingen geraakt	Productie meer dan 1 maand stil, schade tientallen miljoenen [13]

> **Gemiddelde kosten zonder IR-plan**
>
> Organisaties zonder IR-plan betalen gemiddeld USD 5,29 miljoen per datalek. Met een geteste IR-plan en team liggen de kosten significant lager doordat je sneller containet en minder lang stilligt [14].

EMEA DETECTEERT TRAAG

De mediaan dwell time in EMEA bedraagt 22 dagen -- de langste van alle regio's en meer dan twee keer het globale gemiddelde van 11 dagen [3]. Bij ransomware werken aanvallers in 5 dagen van initial access tot

encryptie. Zonder voorbereiding is er nauwelijks tijd om te reageren. 77% van het Nederlandse MKB heeft in de afgelopen twee jaar te maken gehad met cybercriminaliteit [15].

3. Hoe werkt het?

Een incident response-traject volgt een gestructureerd stappenplan. Het meest gebruikte model is het SANS 6-fasenmodel, gebaseerd op het NIST SP 800-61 framework.

DE 6 FASEN (SANS-MODEL)

1 Preparation

DOORLOPEND (VOOR INCIDENT)

IR-plan opstellen, team samenstellen, tools klaarzetten, oefenen. Dit is de fase die bepaalt hoe snel je reageert als het zover is.

2 Identification

UREN TOT DAGEN

Incident detecteren, classificeren, scope bepalen. Hoe is de aanvaller binnengekomen? Welke systemen zijn geraakt?

3 Containment

UREN (SHORT-TERM: MINUTEN)

Geinfecteerde systemen isoleren van het netwerk (niet uitzetten!), verspreiding stoppen, bewijs veiligstellen. Forensische images maken.

4 Eradication

DAGEN

Malware verwijderen, backdoors dichten, root cause elimineren. Accounts resetten die mogelijk gecompromitteerd zijn.

5 Recovery

DAGEN TOT WEKEN

Systemen herstellen uit schone backups, monitoring intensiveren, gefaseerd terugbrengen in productie. Credential reset organisatiebreed.

6 Lessons Learned

1--4 WEKEN NA INCIDENT

Post-incident review, eindrapport, IR-plan aanscherpen. Wat ging goed, wat moet beter? [16]

RETAINER VS AD-HOC

KENMERK	RETAINER (JAARCONTRACT)	AD-HOC (EMERGENCY)
Responstijd	Gegarandeerde SLA (2--4 uur on-site)	Geen SLA, onboarding tijdens crisis (8--24 uur)
Uurtarief	Pre-negotiated, lager	50--70% duurder, emergency rates
Bekendheid met omgeving	Team kent je infra en processen	Moet alles leren tijdens de crisis
Proactieve diensten	IR-readiness, tabletop exercises, plan review	Geen
Vaste kosten	EUR 7.500--75.000+/jaar	Geen, betaal alleen bij incident

CSIRT-NETWERK NEDERLAND

Nederland heeft een landelijk dekkend stelsel van sectorale CSIRTs die samenwerken onder coordinatie van het NCSC [17]:

CSIRT	SECTOR	DOELGROEP
NCSC	Rijksoverheid + vitale sectoren	Ministeries, vitale infrastructuur
Z-CERT	Zorg	Ziekenhuizen, zorginstellingen
SURF-CERT	Onderwijs & Onderzoek	Universiteiten, hogescholen
IBD	Gemeenten	Alle 342 Nederlandse gemeenten
CERT-WM	Waterschappen	Alle 21 waterschappen
CSIRT-DSP	Digitale Service Providers	Cloud, marktplaatsen, zoekmachines

TIP

Het Digital Trust Center (onderdeel van het Ministerie van EZ) biedt gratis advies en tools voor niet-vitale bedrijven en MKB. Sinds 17 oktober 2024 kunnen NIS2-organisaties al NCSC CSIRT-diensten gebruiken.

4. Wat kost het?

De kosten van incident response hangen af van je model (retainer vs ad-hoc), de ernst van het incident en de omvang van je organisatie.

RETAINER-PRIJZEN NEDERLANDSE MARKT

SEGMENT	INDICATIE RETAINER/ JAAR	WAT ZIT ERIN
MKB (< 100 medewerkers)	EUR 7.500--15.000	IR-readiness assessment, IR-plan template, gegarandeerde responstijd, X uur forensics [6]
Middelgroot (100--500)	EUR 15.000--40.000	Bovenstaande + tabletop exercises, dedicated account team, snellere SLA
Enterprise (500+)	EUR 40.000--100.000+	Full DFIR retainer, 24/7 on-call, onbeperkte initiele triage, proactieve threat hunting

UURTARIEVEN SPECIALISTEN

ROL	UURTARIEF	TOELICHTING
IR-specialist	EUR 110--175	Triage, containment, coordinatie
Forensisch analist	EUR 145--250	Disk/memory forensics, malware-analyse
CISO/crisis-manager	EUR 150--250	Strategische aansturing, stakeholder management
Emergency rate (ad-hoc)	EUR 250--350+	50--70% toeslag op regulier tarief, buiten kantooruren [18]

KOSTENVOORBEELD: RANSOMWARE BIJ 200 MEDEWERKERS

POST	MET RETAINER	ZONDER RETAINER
Eerste 8 uur triage	EUR 0--2.000	EUR 2.800--4.800
Forensisch (2 weken)	EUR 15.000--25.000	EUR 25.000--45.000
Crisismanagement	EUR 5.000--10.000	EUR 10.000--20.000

POST	MET RETAINER	ZONDER RETAINER
Subtotaal IR	**EUR 25.000--52.000**	**EUR 52.800--99.800**

Met een retainer van EUR 15.000--40.000/jaar bespaar je bij een incident tot 50% op IR-kosten. Bovendien win je 2--4 uur in de eerste cruciale uren doordat het team je omgeving al kent [6].

> **Gemiddelde herstelkosten 2024**
>
> De gemiddelde herstelkosten bij ransomware bedroegen USD 2,73 miljoen in 2024 -- een stijging van 50% ten opzichte van 2023 [7]. Een retainer is een fractie van die kosten.

5. Waar moet je op letten?

Niet elke IR-dienstverlener is gelijk. Deze selectiecriteria en vragen helpen je de juiste partij te kiezen.

SELECTIECRITERIA

CRITERIUM	WAAROM HET ERTOE DOET
24/7 beschikbaarheid	Cyberincidenten houden zich niet aan kantooruren. Een retainer zonder 24/7 bereikbaarheid is onvoldoende
CERT-status / CCV Keurmerk IR	Het CCV publiceerde per 4 augustus 2025 een keurmerk voor IR-dienstverlening, certificering via Kiwa en DigiTrust [19]
Forensische capaciteit	Kan het team forensische images maken, malware analyseren en een tijdlijn reconstrueren?
Juridische expertise	IR raakt AVG-meldplicht, NIS2-meldplicht, arbeidsrecht en mogelijk strafrecht. Is er een jurist in het team?
Ervaring in jouw sector	Een IR-team dat je sector kent, begrijpt de specifieke systemen, regelgeving en risico's
SLA met concrete responstijden	Niet "zo snel mogelijk" maar "on-site binnen 4 uur" of "remote triage binnen 1 uur"
Proactieve diensten	Tabletop exercises, IR-plan review, readiness assessments -- niet alleen reactief
Deelname aan publiek-privaat	Deelname aan Project Melissa of vergelijkbare samenwerkingen toont marktpositie [20]

10 VRAGEN AAN EEN IR-DIENSTVERLENER

1. Wat is de gegarandeerde responstijd bij een actief incident?
2. Hoeveel IR-incidenten heeft het team het afgelopen jaar afgehandeld?
3. Beschikt het team over forensische capaciteit (disk, memory, malware)?
4. Wie wordt er ingeschakeld bij juridische vraagstukken (AVG, NIS2)?
5. Hoe verloopt de onboarding -- leren jullie onze omgeving vooraf kennen?
6. Wat zit er in de retainer naast reactieve IR (readiness, oefeningen)?
7. Hebben jullie het CCV Keurmerk IR of een vergelijkbare certificering?

8. Hoe communiceren jullie tijdens een incident (out-of-band)?
9. Wat gebeurt er als het incident buiten kantooruren plaatsvindt?
10. Kunnen jullie ondersteunen bij de NIS2-meldplicht (24/72 uur/1 maand)?

> **LET OP: NIET ALLE IR IS GELIJK**
>
> Sommige aanbieders noemen zich IR-dienstverlener maar bieden alleen advies of monitoring. Echte IR betekent dat het team daadwerkelijk ingrijpt: systemen isoleren, forensische images maken, malware verwijderen en systemen herstellen. Vraag concreet wat "response" inhoudt.

6. Veelgemaakte fouten

De eerste 30 minuten na een incident zijn cruciaal. Deze fouten vergroten de schade en vernietigen bewijs.

1. Systemen uitzetten in plaats van isoleren

De natuurlijke reactie is: uitzetten. Maar het vluchtige geheugen (RAM) bevat cruciale forensische informatie -- actieve processen, encryptiesleutels, command & control-verbindingen. Uitzetten vernietigt dit bewijs permanent. Isoleer het systeem van het netwerk, maar laat het draaien zodat het IR-team een forensische image kan maken [21].

2. Communiceren via gecompromitteerde kanalen

Bij een serieuze inbraak heeft de aanvaller vaak toegang tot je e-mail en interne chatplatformen. Als je via die kanalen over het incident communiceert, leest de aanvaller mee. Gebruik out-of-band communicatie: persoonlijke telefoons, een aparte tenant of beveiligde berichtenapps [21].

3. Te snel herstellen zonder scope-bepaling

Gedeeltelijk herstel kan de aanvaller tippen dat je bezig bent -- waardoor ze versnellen of backdoors activeren. Backups kunnen zelf backdoors bevatten. Bepaal eerst de volledige scope en root cause, herstel daarna [22].

4. Te laat extern inschakelen

De eerste uren zijn cruciaal voor bewijs. Wacht niet tot je "zeker weet" wat er aan de hand is. Bel je IR-partij binnen 1 uur. Ad-hoc inschakeling is 50--70% duurder dan via een retainer en de onboarding kost kostbare uren [6].

5. Geen logbestanden beschikbaar

Zonder logs is forensisch onderzoek onmogelijk. Je kunt de root cause niet achterhalen, de scope niet bepalen en het NIS2-eindverslag niet schrijven. Richt logging vooraf in met minimaal 90 dagen retentie [23].

6. Geen offline backups

Aanvallers zoeken actief naar backups en versleutelen die mee. De 3-2-1 regel: 3 kopieen van je data, op 2 verschillende media, waarvan 1 off-site of offline. Test je backups regelmatig -- een backup die je niet kunt herstellen is geen backup [21].

7. Losgeld betalen zonder strategie

29% van de slachtoffers in Nederland betaalde losgeld in 2024, een stijging van 18% in 2023 [1]. Maar er is geen garantie op een werkende decryptiesleutel. Betrek altijd je IR-team, een jurist en de politie (Team High Tech Crime) voordat je een besluit neemt.

DE EERSTE 24 UUR: TIJDLIJN

- **T+0 min** -- Incident gedetecteerd. Niet uitzetten. Netwerk isoleren
- **T+5 min** -- Out-of-band communicatie opstarten (telefoon, Signal)
- **T+15 min** -- IR-retainer bellen / ad-hoc IR-partij inschakelen
- **T+30 min** -- Eerste documentatie: screenshots, ransom note, tijdstippen
- **T+1--2 uur** -- IR-team start remote triage. Scope bepalen
- **T+2--4 uur** -- IR-team on-site (bij retainer). Forensische images starten
- **T+4--8 uur** -- Containment compleet. Eerste beeld van aanvalsvector
- **T+8--12 uur** -- Backup-integriteit checken. Communicatieplan activeren
- **T+24 uur** -- NIS2 vroegtijdige waarschuwing versturen (NCSC) [24]

7. NIS2 en de meldplicht

De Cyberbeveiligingswet (Cbw) -- de Nederlandse implementatie van NIS2 -- treedt naar verwachting in Q2 2026 in werking. De 24-uurs meldplicht maakt professionele IR onmisbaar.

MELDPLICHT IN 3 STAPPEN

STAP	TERMIJN	WAT MOET ER GEMELD WORDEN
1. Vroegtijdige waarschuwing	Binnen 24 uur	Eerste indicatie: aard incident, mogelijk grensoverschrijdend? [5]
2. Vervolgmelding	Binnen 72 uur	Ernst, impact, indicators of compromise, aanvalsvector
3. Eindverslag	Binnen 1 maand	Root cause, genomen maatregelen, grensoverschrijdende impact, lessons learned

Meldingen gaan via **mijn.ncsc.nl** -- een centraal meldpunt dat de melding doorstuurt naar zowel het sectorale CSIRT als de bevoegde toezichthouder [5].

SANCTIES

ENTITEIT-TYPE	MAXIMALE BOETE	TOEZICHT
Essentiele entiteit	EUR 10 miljoen of 2% wereldwijde jaaromzet	Proactief toezicht
Belangrijke entiteit	EUR 7 miljoen of 2% wereldwijde jaaromzet	Reactief toezicht

Daarnaast geldt **persoonlijke bestuurdersaansprakelijkheid** -- directieleden kunnen strafrechtelijk aansprakelijk worden gesteld bij het niet nakomen van NIS2-verplichtingen [25].

SAMENLOOP MET AVG

Bij ransomware met datadiefstal meld je bij twee instanties: de Autoriteit Persoonsgegevens (72 uur, AVG) en het CSIRT (24 uur, NIS2). Zonder professionele IR is het onhaalbaar om binnen 24 uur een kwalitatieve melding te doen -- de onboarding bij ad-hoc inschakeling kost alleen al uren [26].

ZONDER IR-RETAINER HAAL JE DE DEADLINE NIET

De 24-uurs meldplicht vereist dat je binnen een dag kunt beoordelen wat er aan de hand is. Forensisch bewijs moet vanaf het eerste moment veiliggesteld worden voor de eindrapportage na 1 maand. Een retainer garandeert dat je team er op tijd is.

8. IR vs MDR vs SOC vs CERT

De afkortingen vliegen je om de oren. Dit is het verschil -- en waarom je ze niet moet verwarren.

DIENST	TYPE	WANNEER ACTIEF	WAT KRIJG JE
Incident Response (IR)	Reactieve dienst	Na een incident	Crisisrespons, containment, forensics, herstel, rapportage
MDR	Preventieve managed service	24/7 continu	Monitoring, detectie, threat hunting, actieve respons op alerts
SOC	Team/functie	24/7 continu	Monitoring, alerting, first-line respons. Kan intern of extern zijn
CERT/CSIRT	Respons-team	Bij incidenten	Gecoordineerde incidentafhandeling, vaak sectoraal of nationaal [17]
DFIR	Specialisatie	Na een incident	IR + forensisch bewijs voor rechtszaken en compliance-rapportages

Hoe verhouden ze zich?

MDR is je eerste verdedigingslinie: 24/7 monitoring en detectie om incidenten te voorkomen of vroeg te detecteren. IR is je laatste verdedigingslinie: als het toch misgaat, beperkt IR de schade en herstelt je systemen. Een SOC is het team dat dit uitvoert (intern of extern). Een CERT/CSIRT coordineert op sectorniveau. De meest complete aanpak: MDR voor preventie, IR-retainer als vangnet [9].

TIP

Steeds meer aanbieders bieden MDR + IR als gecombineerd pakket. Dat scheelt in kosten, voorkomt dubbel werk bij onboarding en zorgt voor naadloze escalatie van detectie naar response.

9. Trends 2025--2026

Vier ontwikkelingen die incident response de komende jaren veranderen.

1. AI-assisted incident response

AI versnelt de triage-fase: automatische correlatie van alerts, snellere malware-analyse en geautomatiseerde rapportage. Maar AI versnelt ook de aanval: AI-gestuurde phishing is nauwelijks te onderscheiden van echte communicatie en deepfake-fraude neemt toe [27]. Het gevolg: IR-teams moeten sneller en slimmer werken dan ooit.

2. Cloud incident response

Met de verschuiving naar cloud-omgevingen verandert IR fundamenteel. Cloud-forensics vereist andere tools en technieken dan on-premise. Logbestanden zitten bij de cloudprovider, containment werkt anders en de jurisdictie is complexer. IR-dienstverleners investeren in cloud-specifieke expertise en tooling.

3. OT/ICS incident response

Operational Technology (OT) en Industrial Control Systems (ICS) zijn steeds vaker doelwit. IR bij OT-systemen vereist domeinspecifieke kennis -- een productielijn kun je niet zomaar isoleren. NIS2 brengt veel OT-organisaties voor het eerst onder de meldplicht.

4. Project Melissa: publiek-privaat

Project Melissa is een Nederlands publiek-privaat samenwerkingsverband tegen ransomware. Deelnemers: het OM, Politie THTC, NCSC, Cyberveilig Nederland en diverse gespecialiseerde IR-partijen en advocatenkantoren. Succesvolle operaties: Deadbolt, Genesis Market, Qakbot, LockBit en Cactus [20]. Deze samenwerking toont dat IR niet alleen een commerciele dienst is, maar ook een publiek belang.

CCV KEURMERK INCIDENT RESPONSE

Per 4 augustus 2025 is er een keurmerk voor IR-dienstverlening, gepubliceerd door het CCV en gecertificeerd via Kiwa en DigiTrust. Het keurmerk is beschikbaar voor IR-dienstverleners vanaf 3 november 2025 [19]. Dit helpt je als MKB-bedrijf om kwaliteit te objectiveren bij je selectie.

10. Aan de slag

Incident response begint niet bij het incident. Het begint bij voorbereiding. Drie stappen die je vandaag kunt zetten.

1. Stel een basis IR-plan op

Het NCSC en Digital Trust Center bieden gratis templates. Leg minimaal vast: wie is verantwoordelijk, wie bel je als eerste, hoe communiceer je intern en extern, en waar staan je backups. Test het plan minimaal jaarlijks met een tabletop-oefening [23].

2. Overweeg een retainer

Vanaf EUR 7.500/jaar heb je een basisretainer met gegarandeerde responstijd. Voor een MKB-bedrijf dat afhankelijk is van digitale systemen is dit een van de meest impactvolle investeringen in cyberweerbaarheid. Je bespaart niet alleen geld bij een incident, maar ook tijd -- en die eerste uren zijn allesbepalend [6].

3. Bereid je voor op NIS2

De Cyberbeveiligingswet treedt naar verwachting in Q2 2026 in werking. Als je onder NIS2 valt, is een IR-plan en meldprocedure verplicht. Begin nu met de voorbereiding, niet als de wet al van kracht is.

Bronnenlijst

[1] **NCSC** -- Jaarbeeld Ransomware 2024: 121 incidenten, ICT 24%, handel 20%, 29% betaalde losgeld. https://ncsc.nl/jaarbeeld-ransomware-2024

[2] **NCSC** -- Jaarbeeld Ransomware 2025: EUR 11,5M schade, 65 aangiften, 39 ransomware-families. https://ncsc.nl/nieuwsbericht/jaarbeeld-ransomware-2025

[3] **Mandiant / Google Cloud** -- M-Trends 2025: dwell time 11 dagen globaal, 22 dagen EMEA, 5 dagen ransomware. https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025

[4] **ESET / Hallo** -- Cybercriminaliteit kost MKB EUR 270.000 per incident. https://hallo.eu/kennis/blogs/cybercriminaliteit-kost-mkb-euro-270-000-per-incident/

[5] **NCSC** -- Meldplicht Cyberbeveiligingswet: 24u/72u/1mnd. https://ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor/meldplicht

[6] **Exabeam / Arctic Wolf / IPV Network** -- IR-retainer: 50--70% goedkoper, sneller herstel. https://exabeam.com/explainers/incident-response/incident-response-retainer-options-whats-included-and-8-key-considerations/

[7] **ANP / ChannelConnect** -- Losgeld 24% van totale kosten, totale kosten 7x hoger dan losgeld. https://channelconnect.nl/security-en-privacy/kosten-ransomware-aanval-7x-hoger-dan-het-betaalde-losgeld/

[8] **Sygnia** -- What is Incident Response? Process, Plan, and Complete Guide. https://sygnia.co/blog/what-is-incident-response-process-plan-and-complete-guide/

[9] **Palo Alto Networks** -- What is DFIR? https://paloaltonetworks.com/cyberpedia/digital-forensics-and-incident-response

[10] **SURF** -- What Maastricht University learned from the ransomware attack. https://surf.nl/en/case-study/what-maastricht-university-learned-from-the-ransomware-attack-part-1

[11] **Security.nl** -- Hof van Twente: EUR 4,2M herstelkosten, RDP-poort open met zwak wachtwoord. https://security.nl/posting/682578/

[12] **KNVB** -- Informatie cyberinbraak KNVB, LockBit, 300 GB data gestolen. https://knvb.nl/info/68084/informatie-cyberinbraak-knvb

[13] **Security.nl** -- VDL Groep: 105 dochterondernemingen geraakt, productie maand stil. https://security.nl/posting/736215/

[14] **IBM** -- Cost of a Data Breach Report 2025: USD 5,29M zonder IR-plan. https://ibm.com/reports/data-breach

[15] **Vodafone Business** -- 77% MKB cybercrime in afgelopen 2 jaar. https://vodafone.nl/zakelijk/inspiratie/mkb-doelwit-cybercrime-onderzoeken

[16] **Cynet** -- Incident Response SANS: The 6 Steps in Depth. https://cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/

[17] **NCSC / NCTV** -- Landelijk dekkend stelsel, sectorale CSIRTs. https://nctv.nl/onderwerpen/landelijk-dekkend-stelsel

[18] **Mijnzzp.nl** -- Salaris en tarief Security Specialist. https://mijnzzp.nl/Beroep/756-Security-Specialist-(ICT)/Salaris-en-tarief

[19] **CCV** -- Keurmerk Incident Response, certificering via Kiwa en DigiTrust. https://hetccv.nl/keurmerken/cybersecurity/incident-response/

[20] **Cyberveilig Nederland** -- Project Melissa: publiek-privaat tegen ransomware. https://cyberveilignederland.nl/project-melissa

[21] **NCSC** -- Incidentresponsplan Ransomware (PDF). https://ncsc.nl/documenten/publicaties/2022/juni/3/incidentresponsplan-ransomware/

[22] **Microsoft** -- Ransomware IR Playbook: DART ransomware approach. https://learn.microsoft.com/nl-nl/security/ransomware/incident-response-playbook-dart-ransomware-approach

[23] **Digital Trust Center** -- Incident Response Plan. https://digitaltrustcenter.nl/informatie-advies/incident-response-plan

[24] **NCSC** -- NIS2 Incident melden. https://ncsc.nl/contact/contactformulieren/incident-melden

[25] **Kynexis** -- NIS2 boetes en handhaving, bestuurdersaansprakelijkheid. https://kynexis.nl/nis2-boetes-cyberbeveiligingswet-uitgelegd/

[26] **Networking4all** -- Impact meldplicht NIS2 op 24/7 monitoring en IR. https://networking4all.com/nl/nieuws/blog/post/impact-meldplicht-nis2-op-cybersecurity-de-noodzaak-van-24-7-monitoring-incident-response

[27] **Banken.nl** -- 2026 wordt het jaar van geindustrialiseerde cybercriminaliteit en AI-agents. https://banken.nl/nieuws/26681/2026-wordt-het-jaar-van-geindustrialiseerde-cybercriminaliteit-en-ai-agents/