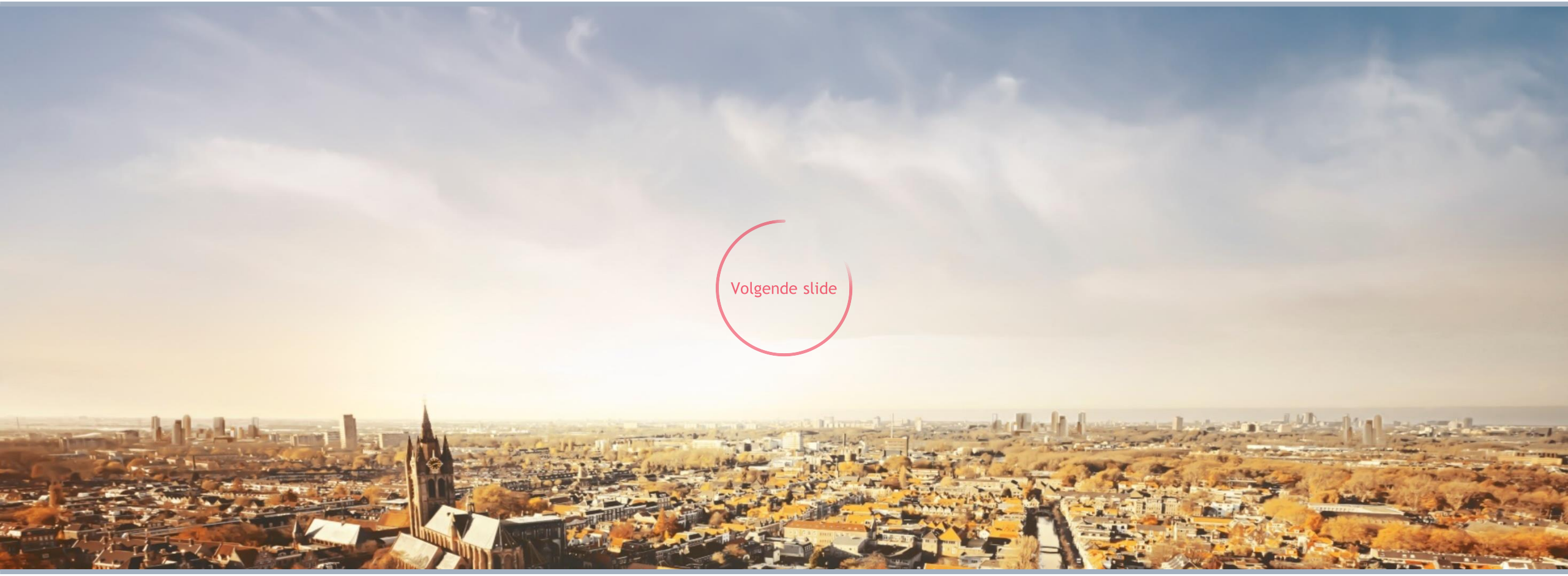
Een digitale aanval, wat nu?

Vereniging van Compliance Officers



November 2020

BDO

Introductie

Dirk de Hen

Partner, Forensic Technology

M: +31 (6) 22 420 248

E: dirk.de.hen@bdo.nl

Jelmer de Hen

Owner, General Cyber Ballistics

M: +31 (6) 19 417 787

E: jelmer@gcb.io

Incident Response

Wie is het eerste aanspreekpunt als zich tekenen van een cyber incident voordoen? Bent u voorbereid op een cyberaanval die uw infrastructuur in gevaar brengt?

Van recente incidenten leren we dat organisaties zich niet moeten afvragen óf een beveiligingsincident gaat plaatsvinden, maar wanneer. Dit komt doordat organisaties het altijd aan het juiste eind moeten hebben wat betreft het volledig beschermen van hun bezittingen en processen. Een aanvaller hoeft het namelijk maar één keer goed te hebben om aanzienlijke schade te veroorzaken bij een organisatie.

Organisaties moeten hun aandacht richten op de voorbereiding van kritieke incidenten, aangezien het garanderen van preventie nauwelijks mogelijk is, laat staan haalbaar. De manier waarop een organisatie omgaat met een aanval heeft direct gevolgen op de totale kosten van een incident. In sommige gevallen kunnen soortgelijke incidenten zelfs mogelijkheden bieden om waarde te creëren voor de stakeholders. Dit is alleen in het geval als de organisatie de incidenten snel en adequaat afhandelt. Om dit voor elkaar te krijgen, moeten organisaties een incident response plan opstellen voordat een incident zich voordoet.

Met onze proactieve incident response services bereiden wij organisaties voor op een incident. Door dit te doen, wordt het risico op imago-en financiële schade verminderend, wordt de business continuïteit verbeterd en kunnen de bedrijfsactiviteiten tegelijkertijd voldoen aan de AVG-voorschriften. Mocht het toch misgaan, dan kunt u op ons rekenen om uw organisatie door de kritieke fases na een incident te leiden.

Incident Readiness

Omgeving & stakeholders

- Risico
- Bedrijfscontinuïteit
- Reputatie
- Wet- en regelgeving
- Financieel

Cybersecurity is *niet alleen* de verantwoordelijkheid van IT.

Een incident heeft effect op de gehele organisatie. Het is daarom noodzakelijk dat het incident response team uit vertegenwoordigers bestaat die uit alle afdelingen binnen de organisatie komen.

Aanpak Incident Response

Beoordelen, verbeteren, ondersteunen en feedback

1 Kick off

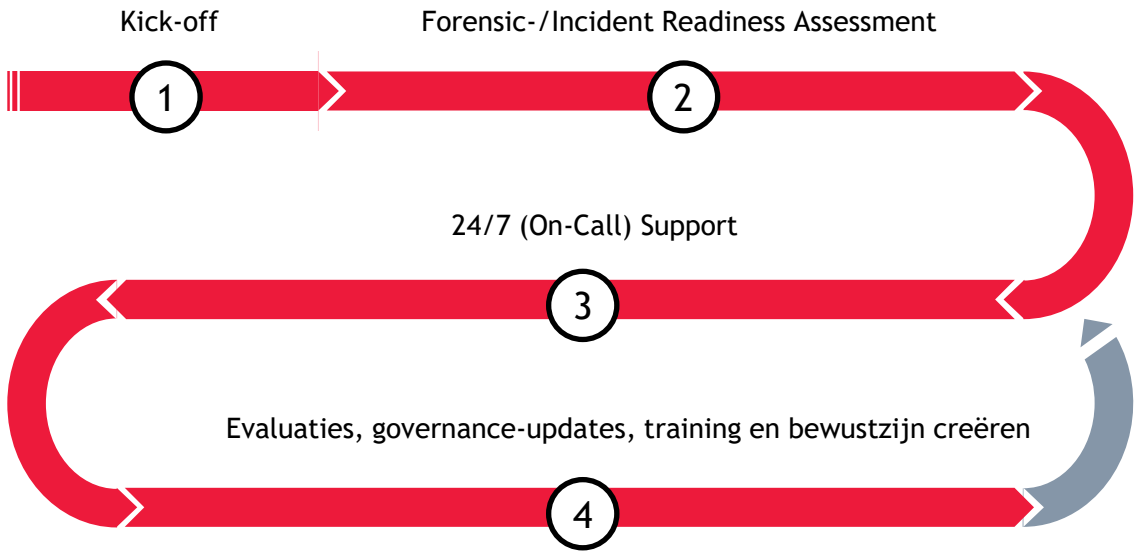
Activiteiten:
- Scope definiëren;
- Incident response maturity assessment.

Deliverable:
- Scope beschrijving;
- Projectplan for IR-implementatie.

3 24/7 On-Call Support

Activiteiten/werkzaamheden:
- Containment activities;
- Remediation activities;
- Onderzoeksondersteuning.

Deliverable:
- Advies en ondersteuning bij het beheren van incidenten;
- Rapportage van bevindingen;
- Ondersteuning bij het melden aan autoriteiten.



2 Forensic-/Incident Readiness assessment

Activiteiten:
- Interviews met key-stakeholders;
- Heatmap van infrastructuur;
- Herzien van huidig beleid en procedures;
- Externe leveranciers;
- Technische beoordeling van de aanwezigheid en inrichting van logging.

Deliverable:
- Incident Response playbook

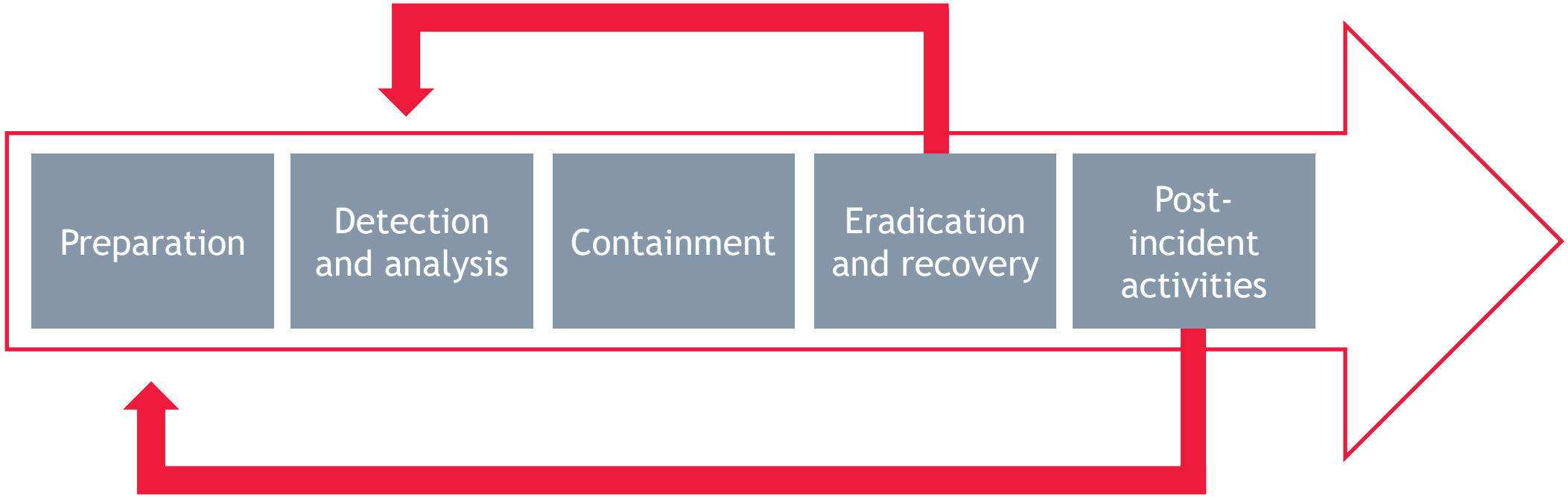
4 Evaluaties, governance-updates, training en bewustzijn creëren

Activiteiten/werkzaamheden:
- Updaten van IR-documentatie;
- First responder-training;
- Bewustwording vergroten door simulaties en ‘fire drills’;
- evaluatie van incidenten en activiteiten.

Deliverables:
- Up-to-date IR-documentatie;
- Fit for purpose IR-organisatie

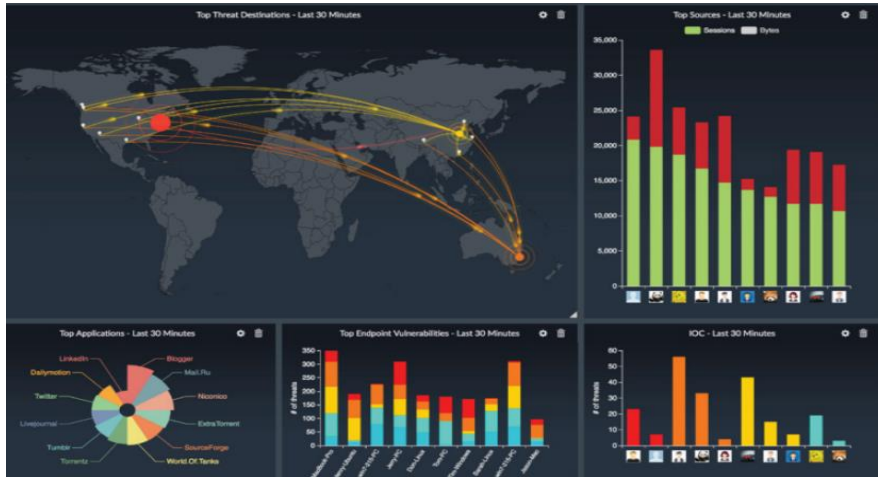
Incident Response

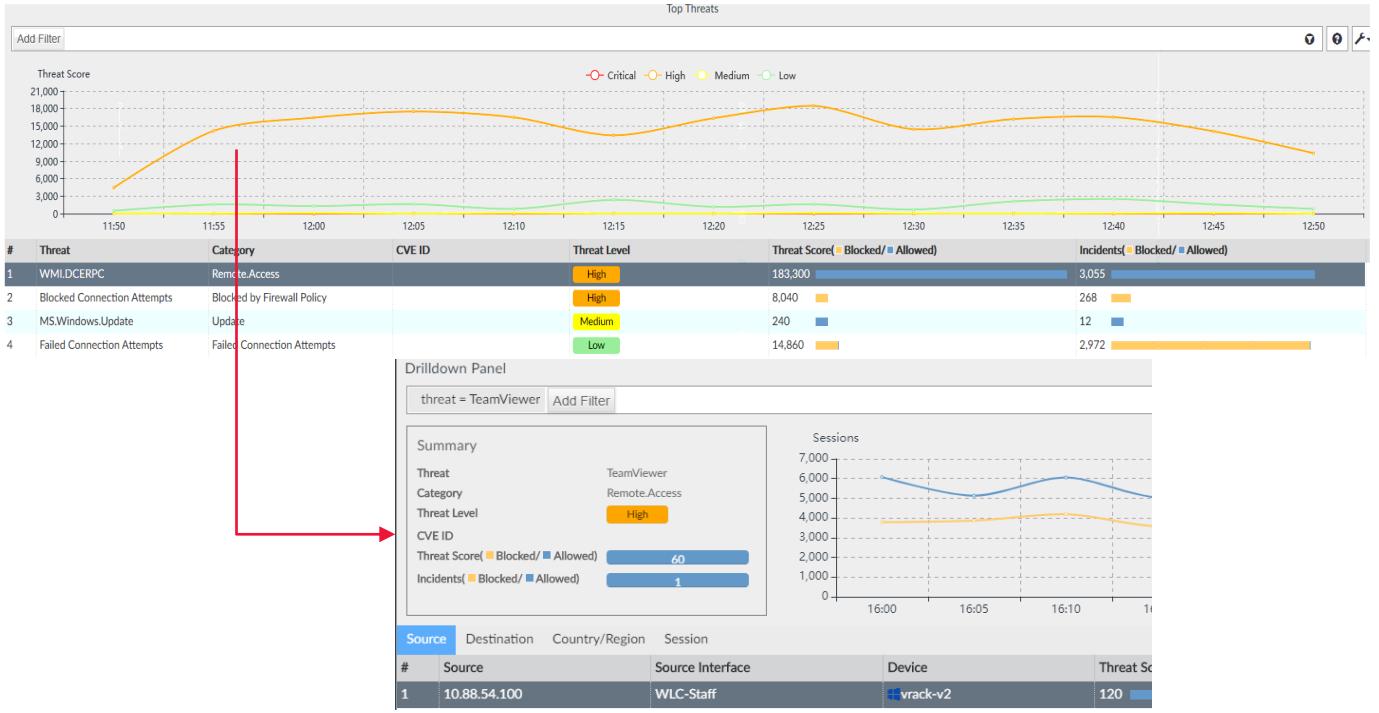
Aanpak



Detectie en analyse

- Snelheid ontwikkeling van exploits
- Samenwerking criminele organisaties
- Detectie wordt bemoeilijkt door gebruik generieke tools
- Phishing en wachtwoorden
- Ransomware
- Monitoring





Vragen?

Bedankt voor uw aandacht

Dirk de Hen E: dirk.de.hen@bdo.nl M: +31 6 22 420 248

Jelmer de Hen E: jelmer@gcb.io M: +31 6 19 417 787