Tijd 10:30

#	Thema	Context	Datum/tijd	Prioriteit	Status	Actiehouder	Blockers/dependanci	Comments
70	Beeldvorming - Omliggend	Asset lijst vlans via RedTeam volledig	22-7-2025 00:00	ASAP	Started			
17	Data acquisitie - Netscaler	Aanleveren Netscaler image van Schade	21-7-2025 00:00	High	Started			geeft aan dat het best wat werk is maar dat aanleveren uiterlijk morgen moet lukken.
35	Onderzoek - DWO/AD-tracl	Monitoring dekkingsgraad verbeteren. U	21-7-2025 00:00	ASAP	Started	JIO		Agent selectie obv Bepalen van de scope van uitrol. Bespreken met
11	Onderzoek - Netscaler-trac	Controle op logging kwaliteit van de firev	21-7-2025 00:00	High	Not starte	onderzoeksteam		We hebben de ontvangen logs bekeken. Lijkt op intern naar intern.
16	Onderzoek - Omliggend ne	Onderzoeken van de crashdumps van n	21-7-2025 00:00	ASAP	Started	onderzoeksteam		1 x 8 mei en 2x 26 mei. 8 mei was nog niet aangeleverd. Alle 16 dumps van 26 mei is niet nodig. Eerste en laatste zijn voldoende.
33	Onderzoek - Omliggend ne	Onderzoeken welke service accounts ac	21-7-2025 00:00	Medium	Not starte	onderzoeksteam		
34	Onderzoek - DWO/AD-tracl	Onderzoeken van logs en vulner	21-7-2025 00:00	Medium	Not starte	onderzoeksteam		
38	Onderzoek - Netscaler-trac	Onderzoeken op interne zone fw logs en	21-7-2025 00:00	High	Not starte	onderzoeksteam		
49	Onderzoek - Omliggend ne	Bedenken van JIO RT scenarios om te te	21-7-2025 00:00	High	Started	onderzoeksteam		Momenteel RT gevraagd om binnen te scannen naar assets binnen deze vlans. Follow-up is verschillen in kaart brengen met CMDB Solvinity (Mai en CMDB JIO . Daarna data acquisitie opstarten van de relevante te onderzoeken systemen
50	Onderzoek - DWO/AD-tracl	Onderzoeken output (AD D.	21-7-2025 00:00	High	Not starte	onderzoeksteam		
55	Onderzoek - Netscaler-trac	Doorzoeken van logging op het IP-adres	21-7-2025 00:00	ASAP	Not starte	onderzoeksteam		IP adressen zie Mattermost screenshot in Neva Teams kanaal
59	Onderzoek - Omliggend ne	Firewall logs van internet en zone firewa	21-7-2025 00:00	High	Not starte	onderzoeksteam		
66	Onderzoek - Netscaler-trac	Het scannen met op netscaler du	22-7-2025 00:00	ASAP	Started	onderzoeksteam		
67	Data acquisitie - DWO/AD-	Het scannen met op Acquires	22-7-2025 00:00	ASAP	Started	onderzoeksteam		
64	Mitigatie & Containment	Realisatie handelingsperspectieven - zie	21-7-2025 00:00	High	Not started	JIO		
57	Organisatie	Aangifte doen bij de Politie namens JIO	21-7-2025 00:00	High	Not starte			Bewust nog even afwachtend hierin vanwege vrees voor verstorend handelen van Politie op dagelijkse operatie.
52	Onderzoek - Netscaler-trac	Onderzoek doen naar de rc-file op de ba	21-7-2025 00:00	ASAP	Blocked	onderzoeksteam		Wacht op aanleveren van netscaler backups
53	Onderzoek - Netscaler-trac	Onderzoeken naar lat move tussen nets	21-7-2025 00:00	ASAP	Blocked	onderzoeksteam		Wacht op aanleveren AP en Schadefonds netscaler kopie.
15	Data acquisitie - Omliggen	Aanleveren van duidelijke timeline van c	21-7-2025 00:00	ASAP	Not started			Vandaag verwacht.
61	Onderzoek - Netscaler-trac	Controleren van alle andere netscalers	21-7-2025 00:00	High	Not started			
60	Onderzoek - Netscaler-trac	DIVD emails opnemen in tijdlijn	21-7-2025 00:00	Medium	Started			Datum/tijdstip van DIVD notificaties opnemen in tijdlijn / rapportage
19	Data acquisitie - Omliggen	Aanleveren externe firewall logging vanu	21-7-2025 00:00	High	Not started			
21	Data acquisitie - Omliggen	Aanleveren firewall logging van de maan	21-7-2025 00:00	High	Not started			via mattermost benaderd.
37	Onderzoek - Omliggend ne	Retentie check SOC JenV inzake firewall	21-7-2025 00:00	High	Not starte			SOC JenV kan verder terug dan CLMP van Solvinity. Hoeveel verder is niet duidelijk, ca. een jaar was laatste schatting van JenV. CLMP is alleen deze en voorgaande maand.
72	Beeldvorming	Aanleveren van het pentest rapport / pin	22-7-2025 00:00	High	Started			
32	Onderzoek - Netscaler-trac	Onderzoek wat netscaler binnen het net	21-7-2025 00:00	High	Started			Vlans aangeleverd 21e einde van de dag.
65	Onderzoek - DWO/AD-tracl	Controle op alerts vanuit	21-7-2025 00:00	ASAP	Blocked	onderzoeksteam		Wacht op toegang op en Bedoeling is om verdachte DWO sessies te identificeren.
39	Organisatie	Integriteit van backups verifieren. Is er o	21-7-2025 00:00	High	Started			Realisatie extra monitoring in ransomware actor scenario
41	Organisatie	Accounts aanmaken voor toegan	21-7-2025 00:00	High	Started			heeft formulier ingevuld, heeft ook het formulier ingevuld, actie ligt nu bij DJI om het proces te tracker
51	Data acquisitie - Netscaler	Aanleveren van de config backups van d	21-7-2025 00:00	ASAP	Started			Bellen met om te checken of er backups zijn er hoe het werkt
62	Onderzoek - Omliggend ne	SOC JIO actie urt commando's ch	21-7-2025 00:00	High	Started			SOC JIO neemt contact over op met SOC JenV
63	Onderzoek - Omliggend ne	SOC JIO actie anleveren overige l	21-7-2025 00:00	High	Started			SOC JIO neemt contact over op met SOC JenV

Datum 24-7-2025
Tijd 10:30

#	Thema	Context	Datum/tijd	Prioriteit	Status	Actiehouder	Blockers/dependanci	Comments
70	Beeldvorming - Omliggend	Asset lijst vlans via RedTeam volledig	22-7-2025 00:00	ASAP	Started			
17	Data acquisitie - Netscaler	Aanleveren Netscaler image van Schade	21-7-2025 00:00	High	Started			geeft aan dat het best wat werk is maar dat aanleveren uiterlijk morgen moet lukken.
35	Onderzoek - DWO/AD-tracl	Monitoring dekkingsgraad verbeteren. U	21-7-2025 00:00	ASAP	Started	JIO		Agent selectie obv Bepalen van de scope van uitrol. Bespreken met
11	Onderzoek - Netscaler-trac	Controle op logging kwaliteit van de firev	21-7-2025 00:00	High	Not starte	onderzoeksteam		We hebben de ontvangen logs bekeken. Lijkt op intern naar intern.
16	Onderzoek - Omliggend ne	Onderzoeken van de crashdumps van n	21-7-2025 00:00	ASAP	Started	onderzoeksteam		1 x 8 mei en 2x 26 mei. 8 mei was nog niet aangeleverd. Alle 16 dumps van 26 mei is niet nodig. Eerste en laatste zijn voldoende.
33	Onderzoek - Omliggend ne	Onderzoeken welke service accounts ac	21-7-2025 00:00	Medium	Not starte	onderzoeksteam		
34	Onderzoek - DWO/AD-tracl	Onderzoeken van logs en vulner	21-7-2025 00:00	Medium	Not starte	onderzoeksteam		
38	Onderzoek - Netscaler-trac	Onderzoeken op interne zone fw logs en	21-7-2025 00:00	High	Not starte	onderzoeksteam		
49	Onderzoek - Omliggend ne	Bedenken van JIO RT scenarios om te te	21-7-2025 00:00	High	Started	onderzoeksteam		Momenteel RT gevraagd om binnen te scannen naar assets binnen deze vlans. Follow-up is verschillen in kaart brengen met CMDB Solvinity (Mai en CMDB JIO . Daarna data acquisitie opstarten van de relevante te onderzoeken systemen
50	Onderzoek - DWO/AD-tracl	Onderzoeken bloodhound output (AD D.	21-7-2025 00:00	High	Not starte	onderzoeksteam		
55	Onderzoek - Netscaler-trac	Doorzoeken van logging op het IP-adres	21-7-2025 00:00	ASAP	Not starte	onderzoeksteam		IP adressen zie Mattermost screenshot in Neva Teams kanaal
59	Onderzoek - Omliggend ne	Firewall logs van internet en zone firewa	21-7-2025 00:00	High	Not starte	onderzoeksteam		
66	Onderzoek - Netscaler-trac	Het scannen met op netscaler du	22-7-2025 00:00	ASAP	Started	onderzoeksteam		
67	Data acquisitie - DWO/AD-	Het scannen met op Acquires	22-7-2025 00:00	ASAP	Started	onderzoeksteam		
64	Mitigatie & Containment	Realisatie handelingsperspectieven - zie	21-7-2025 00:00	High	Not started	JIO		
57	Organisatie	Aangifte doen bij de Politie namens JIO	21-7-2025 00:00	High	Not starte			Bewust nog even afwachtend hierin vanwege vrees voor verstorend handelen van Politie op dagelijkse operatie.
52	Onderzoek - Netscaler-trac	Onderzoek doen naar de rc-file op de ba	21-7-2025 00:00	ASAP	Blocked	onderzoeksteam		Wacht op aanleveren van netscaler backups
53	Onderzoek - Netscaler-trac	Onderzoeken naar lat move tussen nets	21-7-2025 00:00	ASAP	Blocked	onderzoeksteam		Wacht op aanleveren AP en Schadefonds netscaler kopie.
15	Data acquisitie - Omliggen	Aanleveren van duidelijke timeline van c	21-7-2025 00:00	ASAP	Not started			Vandaag verwacht.
61	Onderzoek - Netscaler-trac	Controleren van alle andere netscalers	21-7-2025 00:00	High	Not started			
60	Onderzoek - Netscaler-trac	DIVD emails opnemen in tijdlijn	21-7-2025 00:00	Medium	Started			Datum/tijdstip van DIVD notificaties opnemen in tijdlijn / rapportage
19	Data acquisitie - Omliggen	Aanleveren externe firewall logging vanu	21-7-2025 00:00	High	Not started			
21	Data acquisitie - Omliggen	Aanleveren firewall logging van de maan	21-7-2025 00:00	High	Not started			via mattermost benaderd.
37	Onderzoek - Omliggend ne	Retentie check SOC JenV inzake firewall	21-7-2025 00:00	High	Not starte			SOC JenV kan verder terug dan van Solvinity. Hoeveel verder is niet duidelijk, ca. een jaar was laatste schatting van JenV. s alleen deze en voorgaande maand.
72	Beeldvorming	Aanleveren van het pentest rapport / pin	22-7-2025 00:00	High	Started			
32	Onderzoek - Netscaler-trac	Onderzoek wat netscaler binnen het net	21-7-2025 00:00	High	Started			Vlans aangeleverd 21e einde van de dag.
65	Onderzoek - DWO/AD-tracl	Controle op alerts vanuit	21-7-2025 00:00	ASAP	Blocked	onderzoeksteam		Wacht op toegang op en Bedoeling is om verdachte DWO sessies te identificeren.
39	Organisatie	Integriteit van backups verifieren. Is er o	21-7-2025 00:00	High	Started			Realisatie extra monitoring in ransomware actor scenario
41	Organisatie	Accounts aanmaken voor toegan	21-7-2025 00:00	High	Started			heeft formulier ingevuld, heeft ook het formulier ingevuld, actie ligt nu bij DJI om het proces te tracker
51	Data acquisitie - Netscaler	Aanleveren van de config backups van d	21-7-2025 00:00	ASAP	Started			Bellen met om te checken of er backups zijn er hoe het werkt
62	Onderzoek - Omliggend ne	SOC JIO actie urt commando's ch	21-7-2025 00:00	High	Started			SOC JIO neemt contact over op met SOC JenV
63	Onderzoek - Omliggend ne	SOC JIO actie anleveren overige l	21-7-2025 00:00	High	Started			SOC JIO neemt contact over op met SOC JenV

Datum 25-7-2025
Tijd 10:30

#	Thema	Context	Datum/tijd	Prioriteit	Status	Actiehouder	Blockers/dependanci	Comments
122	Data acquisitie - DWO/AD-	We ontvangen graag een Dissect Acquire van systeem	24-7-2025 00:00	ASAP	Not starte			en Solvinity wellicht aan elkaar koppelen.
121	Beeldvorming - Netscaler	Uitlopen nieuwe IOCs op de Netscaler	24-7-2025 00:00	ASAP	Started			
39	Organisatie	Integriteit van backups monitoren. Ove	21-7-2025 00:00	High	Started	JIO Management		Realisatie extra monitoring in ransomware actor scenario
64	Mitigatie & Containment	Realisatie handelingsperspectieven - zi	21-7-2025 00:00	High	Started	JIO Management		Afgesproken dit niet hier te tracken maar in CMT meetings.
32	Onderzoek - Netscaler-tra	Onderzoek wat netscaler binnen het n	21-7-2025 00:00	High	Started			Vlans aangeleverd 21e einde van de dag. Wachten op VMs in vlans voor toegang.
111	Beeldvorming - Netscaler	Zijn er Citrix Storefront server die	24-7-2025 00:00	High	Not starte			We willen deze mogelijk onderzoek omdat er MO bekend is bij andere slachtoffers.
	Beeldvorming - DWO / AD	Aanleveren Citrix Storefront IIS server	24-7-2025 00:00	High	Not starte			
80	Beeldvorming - DWO / AD	Achterhalen werking (is h	22-7-2025 00:00	High	Started			uitnodigen voor meeting scoping. uitnodige

Datum 28-7-2025
Tijd 10:30

#	Thema	Context	Datum/tijd	Prioriteit	Status	Actiehouder	Blockers/dependanci	Comments
122	Data acquisitie - DWO/AD-	We ontvangen graag de gemaakte snapshot van systeem	24-7-2025 00:00	ASAP	Not starte			Snapshot is gemaakt wacht op aanlevering. zorgt voor de upload.
141	Beeldvorming	Solvinity informeren over de scan resul	28-7-2025 00:00	ASAP	Started	JIO		
142	Beeldvorming	Nagaan welke assets die naar voren kwamen in de pentest scan in het scope van onderzoek Neva vallen of onder verantwoordelijkheide vallen van andere instanties (solvinity, CJIB etc)	28-7-2025 00:00	ASAP	Started	/ Solvinity		Valt samen met actie #140

Datum 29-7-2025
Tijd 10:30

#	Thema	Context	Datum/tijd	Prioriteit	Status	Actiehouder	Blockers/dependanci	Comments
67	Data acquisitie - DWO/AD-	Het scannen me p Acquires	22-7-2025 00:00	High	Started			
110	Onderzoek	IOC lijst bijwerken	24-7-2025 00:00	High	Started			Bijgewerkt: 24 juli 17:11
131	Onderzoek	Timeline opschonen	24-7-2025 00:00	High	Started			
34	Onderzoek - DWO/AD-tracl	Onderzoeken van logs en vulner	21-7-2025 00:00	High	Not starte			Bronnen ontbreken? Uitzoeken.
50	Onderzoek - DWO/AD-tracl	Onderzoeken output (AD D.	21-7-2025 00:00	High	Not starte			In de organisatie verschillijsten bschikbaar met mutaties op rechten.
148	Onderzoek - DWO/AD-tracl	Onderzoek	24-7-2025 00:00	High	Not starte			Acquire moet nog worden aageleverd
38	Onderzoek - Netscaler-trac	Onderzoeken op interne zone fw logs en	21-7-2025 00:00	ASAP	Started			naar vanaf 19 mei tot 2 juni werkte collector niet goed waardoor (bijna) alle data ontbreekt voor die periode. Geescaleerd op 28-7. 29-7 word er geprobeerd het bovenlangs te regelen dat het onderzoeksteam integraal mee kan kijken met JenV.
55	Onderzoek - Netscaler-trac	Doorzoeken van logging op het IP-adres	21-7-2025 00:00	High	Started			IP adressen zie screenshot in Neva Teams kanaal. IP-adressen moeten nog in IOC tab Excel
59	Onderzoek - Omliggend ne	Firewall logs van internet en zone firewa	21-7-2025 00:00	High	Started			
122	Data acquisitie - DWO/AD-	We ontvangen graag de gemaakte snapshot van systeem	24-7-2025 00:00	High	Finished			Snapshot is gemaakt wacht op aanlevering. orgt voor de upload. En
141	Beeldvorming	Solvinity informeren over de scan resul	28-7-2025 00:00	High	Started	JIO		
142	Beeldvorming- Omliggend	Nagaan welke assets die naar voren kwamen in de pentest scan in het scope van onderzoek Neva vallen of onder verantwoordelijkheide vallen van andere instanties (solvinity, CJIB etc)	28-7-2025 00:00	ASAP	Started	/ Solvinity		Valt samen met actie #140/141. Geescaleerd op 28-7. 29-7 word er geprobeerd het bovenlangs te regelen dat het onderzoeksteam integraal mee kan kijken met JenV.
150	Beeldvorming	Aanleveren naamconventie lijst AD DJI e	28-7-2025 00:00	High	Started			Vraag van SOC JIO en
155	Onderzoek - Netscaler-trac	(herhaling) IOC-check op de interne net	30-7-2025 00:00	High	Finished			Alle checks op de edge zijn ook intern toegepast.
156	Mitigatie & Containment		30-7-2025 00:00	High	Not started	JIO Management		Deze actie moet onderdeel worden van track 3 - onder het onderdeel handelingsperspectief / pentest bevindingen
160	Data acquisitie - DWO/AD-	Ontvangen netscalers tussen AD DJI en	30-7-2025 00:00	High	Not started	?		
161	Beeldvorming	Beheer domein beeldvorming - hoe werk	30-7-2025 00:00	High	Not starte			Opgang JIO: niet interne netscaler, obv ad groeplidmaatschap. (Niet DJI!)
149	Data acquisitie - Netscaler	Configuratie backups van netscalers jur	28-7-2025 00:00	High	Finished			Actie staat uit bij in cc

Datum 30-7-2025
Tijd 10:30

#	Thema	Context	Datum/tijd	Prioriteit	Status	Actiehouder	Blockers/dependanci	Comments
67	Data acquisitie - DWO/AD-	Het scannen me p Acquires	22-7-2025 00:00	High	Started			
110	Onderzoek	IOC lijst bijwerken	24-7-2025 00:00	High	Started			Bijgewerkt: 24 juli 17:11
131	Onderzoek	Timeline opschonen	24-7-2025 00:00	High	Started			
34	Onderzoek - DWO/AD-tracl	Onderzoeken van logs en vulner	21-7-2025 00:00	High	Not starte			Bronnen ontbreken? Uitzoeken. Track 3 meenemen?
50	Onderzoek - DWO/AD-tracl	Onderzoeker output (AD D.	21-7-2025 00:00	High	Started			In de organisatie verschillijsten bschikbaar met mutaties op rechten.
148	Onderzoek - DWO/AD-tracl	Onderzoek	24-7-2025 00:00	High	Not starte			Acquire moet nog worden aageleverd
38	Onderzoek - Netscaler-trac	Onderzoeken op interne zone fw logs en	21-7-2025 00:00	ASAP	Started			naar vanaf 19 mei tot 2 juni werkte collector niet goed waardoor (bijna) alle data ontbreekt voor die periode. Geescaleerd op 28-7. 29-7 word er geprobeerd het bovenlangs te regelen dat het onderzoeksteam integraal mee kan kijken met JenV.
55	Onderzoek - Netscaler-trac	Doorzoeken van logging op het IP-adres	21-7-2025 00:00	High	Started			IP adressen zie screenshot in Neva Teams kanaal. IP-adressen moeten nog in IOC tab Excel
59	Onderzoek - Omliggend ne	Firewall logs van internet en zone firewa	21-7-2025 00:00	High	Started			
122	Data acquisitie - DWO/AD-	We ontvangen graag de gemaakte snapshot van systeem	24-7-2025 00:00	High	Finished			Snapshot is gemaakt wacht op aanlevering. orgt voor de upload. En
141	Beeldvorming	Solvinity informeren over de scan resul	28-7-2025 00:00	High	Started	JIO		
142	Beeldvorming- Omliggend	Nagaan welke assets die naar voren kwamen in de pentest scan in het scope van onderzoek Neva vallen of onder verantwoordelijkheide vallen van andere instanties (solvinity, CJIB etc)	28-7-2025 00:00	ASAP	Started	/ Solvinity		Valt samen met actie #140/141. Geescaleerd op 28-7. 29-7 word er geprobeerd het bovenlangs te regelen dat het onderzoeksteam integraal mee kan kijken met JenV.
150	Beeldvorming	Aanleveren naamconventie lijst AD DJI e	28-7-2025 00:00	High	Started			Vraag van SOC JIO en ontvangen log niet ontvangen. Vragen
155	Onderzoek - Netscaler-trac	(herhaling) IOC-check op de interne net	30-7-2025 00:00	High	Finished			Alle checks op de edge zijn ook intern toegepast.
156	Mitigatie & Containment		30-7-2025 00:00	High	Not started	JIO Management		Deze actie moet onderdeel worden van track 3 - onder het onderdeel handelingsperspectief / pentest bevindingen
160	Data acquisitie - DWO/AD-	Ontvangen netscalers tussen AD DJI en	30-7-2025 00:00	High	Not started	?		
161	Beeldvorming	Beheer domein beeldvorming - hoe werk	30-7-2025 00:00	High	Not starte	JIO (inderz.)		Opgang JIO: niet interne netscaler, obv ad groeplidmaatschap. (Niet DJI!)
149	Data acquisitie - Netscaler	Configuratie backups van netscalers jur	28-7-2025 00:00	High	Finished			Actie staat uit bij in cc