Bron		Vraag	
CISO DT&V (email d.d. 10 oktober 17:19)	1	In paragraaf 2.8 worden 13 bullets genoemd die het onderzoek hebben beperkt. (pagina 20 van 56) Hoeveel van die 13 bewust / besloten / beschreven beleid is geweest? Hoeveel van die 13 punten zijn ondertussen verholpen?	1. De netscaler logdata was niet aanwezig in het SIEM, dit is inmiddels wel aanwezig. 5.1.2h 3. Deze kwetsbaarheid is door onze pentesters zichtbaar gemaakt. Vervolgens heeft Solvinity dit aangepast. 4. Er zijn betere werkafspraken gemaakt tussen SOC JIO en SOC JenV. Het ontbreken van deze werkafspraken heeft niet gezorgd voor 5.1.2ebelemering. 5. Hiervoor geldt hetzelfde als bij punt 1 alleen hier gaat het om de interne netscalers. 6. De IIS logdata is nog onderdeel van onderzoek om toe te voegen aan het SIEM. Wat hier in meespeelt is de omvang van de dataset. 5.1.2h 8. Zie hetzelfde antwoord voor punt 1. 9. Het opnieuw inspoelen is 1 van de maatregelen zodat een aanvaller geen persistentie kan creeren op het systeem en draagt bij aan een veilig systeem. Het nadeel is dat hiermee ook de sporen van de aanvallers verwijderd worden. Het opnieuw inspoelen van de systemen, wordt gezien als goede maatregel ondanks de onderzoeksbeperking. 10. Om het nadeel van 9 te ondervangen kan je de DWO aansluiten op het SIEM. De installatie van de storage is eind december afgerond in het datacenter, de uitrol van 5.1.2h op de DWO omgeving starten we begin januari 11. Zie het antwoord voor punt 10. 12. Inmiddels is dit punt beter geworden door de verdere uitrol van 5.1.2h op alle OS'en 13. Zie het antwoord voor punt 7.
	2	Wat is de JIO tijdlijn van activiteiten en beslissingen tussen 7 juli (de firma Citrix meldt compromittatie) en 19 juli (telefoontje naar 5.1.2f Dit is namelijk na de beknopte uitleg van 5.1.2e 5.1.2e nog niet helemaal helder. (pagina 24 van 56)	Op 7 juli krijgen wij het advies van Citrix. Vanaf diezelfde dag is ons SOC benaderd en betrokken bij het probleem. In de dagen na 7 juli zijn in overleg met citrix diverse aanvullende maatregelen genomen zoals in pagina 18/19 van het rapport is verwoord.
	3	5.1.2f concludeert dat het 5.1.2h kwetsbaar is. Zoals te lezen is op pagina 37, wordt het aangeraden om gebruikers op de hoogte te stellen dat er mogelijk informatie zoals wachtwoorden is gelekt? (pagina 37 van 56)	Wij hebben na aanleiding van de adviezen, de gebruikers van de organisatie afgedwongen de wachtwoorden te wijzigen. Voor DJI zijn de wachtwoorden na 25 juli gefaseerd gereset, voor DTenV zijn de wachtwoorden op 31 juli gefasseerd gereset, voor JIO zijn de wachtwoorden op 31 juli 2025 om 13.00 uur gereset.
	4	5.1.2f heeft op 21 juli een advies afgegeven om de kroonjuwelensysteem tijdelijk uit te zetten. Er is nog niet helemaal duidelijk waarom dit advies door JIO niet als zodanig is ingebracht bij het dagelijks crisisoverleg CISO's van opdrachtgevers. (pagina 20 van 56)	Het uitschakelen/afschakelen van kroonjuweelsystemen heeft een grote impact op de continuiteit van de bedrijfsvoering van onze opdrachtgevers. Vanwege de koppeling met andere systemen zou deze impact vele malen groter zijn voor de hele JenV keten. Een besluit of een systeem uit te schakelen moet in het bredere perspectief op JenV niveau genomen moeten worden. Wij waren hier over in gesprek met 5.1.2e 5.1.2e
	5	In het rapport wordt een verband gelegd tussen diverse incidenten die (mogelijk) het gevolg waren van compromittatie activiteiten. Onlangs zijn er problemen geweest met 5.1.2h 5.1.2h en wellicht nog andere. Worden deze incidenten ook meegenomen in de uitwisseling met 5.1.2f 5.1.2(pagina 24 van 56)	Bij ons is niet bekend (geen aanwijsbare signalen) dat er een verband ligt tussen diverse incidenten en gevolg van compromitatie. Wij hebben geen verband kunnen aantonen.
	6	Hoezo is de Exchange omgeving nog toegankelijk en als 5.1.2h aangemerkt vanuit de Citrix Netscaler, terwijl de webmail functionaliteit is al geruime tijd niet meer mogelijk is via de dienst Connect? (pagina 34 van 56)	De webmail functionaliteit staat inderdaad al geruime tijd dicht via Connect, voor de genoemde exchange omgeving lopen er een aantal security maatregelen die eerder met de OG's zijn gecommuniceerd, de korte termijn oplossing zal eind december worden geïmplementeerd en de lange termijn oplossing eind april
	7	Er wordt meermaals in de aanbeveling gedaan om 5.1.2h in te stellen. Dit staat ook in het door JIO vastgestelde wachtwoordbeleid d.d. 28-04-2025 (paragraaf 4.4 op pagina 12 uit het bijgesloten JIO wachtwoordbeleid). Waarom wordt dit beleid niet nageleefd en is hiervoor dan een exceptie opgesteld? Dit zou middels een pilot nu getest worden (dit is door 5.1.2e 5.1.2e verteld), wat is hier de doorlooptijd van?	De pilot loopt nog tot en met December. De evaluatie neemt kort na de jaarswisseling plaats. Aan de hand van deze uitkomst zal er een keuze worden gemaakt. 5.1.2h
	8	Hoe kan het dat wijzigingen in augustus 2023 goedgekeurd worden (5.1.2h 5.1.2h) nog steeds niet is uitgevoerd? 5.1.2h 5.1.2h 5.1.2e	De domain controllers zijn eerst versneld onder monitoring gebrackt tijdens de crisis. De domain controllers zijn voor het einde van het jaar op versie 2022. Hierna volgt ook nog een aanvullend hardeningstraject.
	9	Waarom hebben zelfs nu nog niet alle beheerteams van JIO de opdracht gekregen om te controleren op sporen zoals voorgesteld in paragraaf 5.1 van het rapport? (pagina 42 van 56)	Dit is actie project LoMe. De analyse van LoMe loopt. Daarnaast hebben wij onze eigen medewerkers extra alert gemaakt op verdachte acties.
	10	Is er melding gemaakt bij de Autoriteit Persoonsgegevens (AP) over een datalek en / of is er aangifte gedaan zoals voorgesteld door 5.1.2f in tabel 4 (2025-07-21)? (pagina 20 van 56) Of verwacht JIO dat de getroffen opdrachtgevers dit doen?	Er is aangifte gedaan bij de politie en hierdoor is onze informatiepositie verbeterd omdat er informatie vanuit de politie kwam. Er is ook melding gedaan bij de AP op 25 juli en de opdrachtgevers geadviseerd dit ook te doen.
	11	Project LOME (pagina 37 van 56); Wat is de scoping- en wat zijn de projectdeliverables van project LOME? Wie zit er in de stuurgroep van project LOME?	Deze informatie is vastgelegd in projectdocumentatie en mag opgevraagd worden.
CISO DJI (email d.d. 24 oktober 12:28)	12	Ik ontvang eerdaags graag nog verslag van de meeting van de eerste bespreking van het rapport de 9e oktober, zoals toen mondeling ook is afgestemd.	Deze is verstuurd op di 14-10-2025 15:02 naar alle uitgenodigde van het overleg op 9 october.
	13	Wordt n.a.v. de bespreking nog en bijgestelde versie van het rapport opgesteld, met daarin correctie van de tijdlijn?	Ja, er is een versie 1.1 van 5.1.2f Deze versie is aangepast door 5.1.2f na aanleiding van de bespreking op 9 october. Het betrefd de aanpassing van de tijdlijn en andere kleine aanpassingen. Deze versie 1.1 zal samen met de antwoorden worden gedeeld.
	14	In onze bespreking op 9 oktober heeft 5.1.2e opgemerkt dat van JIO verwacht wordt dat zij een appreciatie bij het rapport opstellen. Dit ook n.a.v. vragen van de pSG op dit dossier. Is dit nu opgepakt en wanneer kunnen wij deze verwachten?	Er komt geen seperate management appreciatie op dit rapport. Wij hebben dit rapport inhoudelijk toegelicht en gaan in op al de gestelde vragen.
	15	Voorts onderstreep ik vanuit DJI de vragen van DT&V. Daarbij wil ik met name vragen om meer duidelijkheid m.b.t. vraag 2: Naar aanleiding van analyse van een eerder geconstateerd incident (crashes processen op een van de Netscalers)) is op 7 juli is door Citrix aan JIO gemeld dat zij hebben vastgesteld dat een compromittatie heeft plaatsgevonden met daarbij concrete adviezen. Naast opvolgen van de aanwijzingen ter directe mitigatie is hierin door Citrix, met nadruk, geadviseerd om forensisch onderzoek te starten via het eigen of een extern security team. Citaat inclusief nadruk in oorspronkelijk bericht: "we strongly advise you to follow your internal security team's protocols and take the necessary actions. Please understand that NetScaler support is unable to perform security forensic analysis to verify the integrity and security of the NetScaler in such cases. We recommend engaging your internal or external security team for expert guidance on this matter."	Dit is het advies wat wij op 7 juli gekregen hebben van Citrix. "we strongly advise you to follow your internal security team's protocols and take the necessary actions. Please understand that NetScaler support is unable to perform security forensic analysis to verify the integrity and security of the NetScaler in such cases. We recommend engaging your internal or external security team for expert guidance on this matter.". Op pagina 18 van het rapport is terug te lezen welke acties JIO vervolgens heeft genomen. Dit betreft onderandere het inschakelen van JIO SOC als interne security team.
	16	Bij bespreken van het rapport op 9 oktober heb ik gevraagd of JIO op 7 juli reeds intern bij hun eigen SOC heeft gemeld dat een Netscaler gecompromitteerd was en meer concreet of er die datum triage door het JIO SOC gestart is. Dit is bevestigend beantwoord. Dit past niet bij wat ik heb gezien in verloop van het incident in die periode en de weergave in het rapport. Daar is gemeld dat pas op 17 juli (wat feitelijk de 18e moet zijn geweest, dit is opgemerkt bij bespreking van het rapport) is besloten om forensisch onderzoek te starten. Dus nadat duidelijk werd dat situatie bij OM geëscaleerd was:	Op 7 juli krijgen wij het advies van Citrix. Vanaf diezelfde dag is ons SOC benaderd en betrokken bij het probleem. In de dagen na 7 juli zijn in overleg met citrix diverse aanvullende maatregelen genomen zoals in pagina 18/19 van het rapport is verwoord.
	17	5.1.2f wil daarom in meer detail weten wat nu precies wel en niet de response van JIO is geweest tussen 7 en 18 juli. Vanuit mijn perspectief lijkt hier een belangrijke afslag gemist te zijn en gezien dat belang vraagt dat om reflectie. Is op voor JIO SOC gebruikelijke wijze in 5.1.2h een case aangemaakt voor triage, wat zijn daarbij de eerste conclusies/advies en vervolgstappen geweest? Op basis waarvan is JIO niet eerder dan 18 juli tot overweging gekomen om forensisch onderzoek naar de op 7 juli ontdekte compromittatie te starten, ondanks direct advies daartoe van Citrix? Waarom zijn DJI en andere geraakte opdrachtgevers niet toen al geïnformeerd en geadviseerd? Is over de compromittatie reeds vóór 18 juli contact geweest tussen JIO en NCSC of SOC JenV? Etc.	Wij hebben bij het constateren van instabiliteit problemen direct contact opgenomen met de leverancier (Citrix). Dit is onze eerste reactie want die weten het meest. Later bleek dat het om een beveiligingsincident ging. Onze reflectie nu achteraf is dat wij niet de netscaler schoon hadden moeten maken, maar deze er tussenuit moeten halen met continuiteits problemen tot gevolg zodat er onderzoek gedaan kon worden. Ja er is contact geweest met SOC JenV, SOC JIO, NCSC en vooral met de leverancier voor 18 juli.
CISO DJI (email d.d. 12 november 17:43)	18	In eerste meeting is ter sprake gekomen dat 5.1.2f ook hulp kan bieden met verbeteren van verschillende concrete zaken t.a.v. adviezen in het rapport en weerbaarheid die direct relateren aan bevindingen. 5.1.2e sprak toen uit dat hij ziet dat dat ook nodig is. Ik heb hem daarop gevraagd om te kijken om op die onderdelen te zien om via bijv. 5.1.2f versterking te zoeken. Het is een behoorlijke opgave en JIO kan dit niet alleen. In vervolggesprek d.d. 06-11 heb ik gevraagd of dit nu plaatsvindt, was onduidelijk. Ik heb aan 5.1.2e verzocht om na te vragen en hier verder opvolging aan te geven.	5.1.2f biedt verschillende diensten. Wij hebben 5.1.2f verder ingezet voor project LoMe, een breed threat assessment op de omgeving van ons en opdrachtgevers die hier aan mee wilden doen.
	19	In terugkoppeling is door JIO aangegeven 'Netscalers zijn nu aangesloten op logging'. Dit is gemeld als gereed. 5.1.2f heeft geadviseerd: verifieer de detectiekwaliteit. Vraag van mij vanuit DJI: hebben jullie voor de nieuw aangesloten logging getest, o.a. op concrete indicatoren uit de aanval die we gehad hebben, dat de signalering/detectie nu werkt. Uit antwoord komt naar voren dat dit niet is vastgesteld. Ik heb JIO daarop verzocht dit alsnog te gaan doen en terug te koppelen.	Door het verzamelen van de logging hebben wij nu zicht op het verkeer en bouwen wij een history op. Logging is aangesloten. Het testen door het uitvoeren van een purple-team op de nu verzamelde logging 5.1.2h Vanuit het IPW security team, Integratie bij IT4IT, SOC en PENtesters wordt het purple team georganiseerd 5.1.2h
Verdere vragen DTenV	20	**Logging** 1. Welke beheerprocessen (instellingen zoals load balancing rules, content switching policies of authentication methodes worden gewijzigd zonder logische verklaring of zonder dat een beheerder dit heeft aangepast), beheeractiviteiten (zoals verhoogde CPU-belasting- of geheugenbelasting) en dataverkeer (communicatie via ongebruikelijke poorten) worden in de DMZ door JIO gelogd?	
	21	2. Zijn infrastructurele loggings in de logbestanden aanwezig?	
	22	3. Welke infrastructurele loggings zijn plotseling afwezig in de logbestanden / logboeken? (logbestanden zijn incompleet, missen cruciale gegevens of tonen onrealistische inlogtijdstippen) **Back-ups**	
	23	1. Vanaf welke datum kan JIO garanderen dat de back-up van ons primair processysteem ISTV en BO 100% volledig is?	
	24	2. Vanaf welke datum kan JIO garanderen dat de back-up van ons e-mail-omgeving 100% volledig is?	
	25	3. Vanaf welke datum kan JIO garanderen dat de back-up van ons DWO Productie-omgeving 100% volledig is?	
	26	4. Wanneer is de laatste back-up en restore test in relatie tot dienstverlening DTenV geweest en wat was het resultaat? **Rapportage als gevolg van forensisch onderzoek van** 5.1.2f	
	27	1. Rapportage Spoor 1: Gecompromitteerd systeem, wanneer is de verwachting dat deze met DTenV wordt gedeeld?	
	28	2. Rapportage Spoor 2: Direct omliggende sysrtemen en netwerken, wanneer is de verwachting dat deze met DTenV wordt gedeeld?	
	29	3. Rapportage Spoor 3: DWO en AD-omgevingen DTenV en DJI en JIO, wanneer is de verwachting dat deze met DTenV wordt gedeeld?	