Welkom

SAP Security – Ervaringen uit de praktijk

Marcel Antons, Directeur Strategie en Innovatie - myBrand

myBrand® | CONCLUSION

SAP Security

Ervaringen uit de praktijk

Marcel Antons myBrand

9 november 2021

myBrand | CONCLUSION

myBrand organisatie

Medewerkers

400+

Kennisbedrijf

3+ vestigingen in NL

Geen off-/nearshore

Verloop <5%

myBrand diensten

Agenda

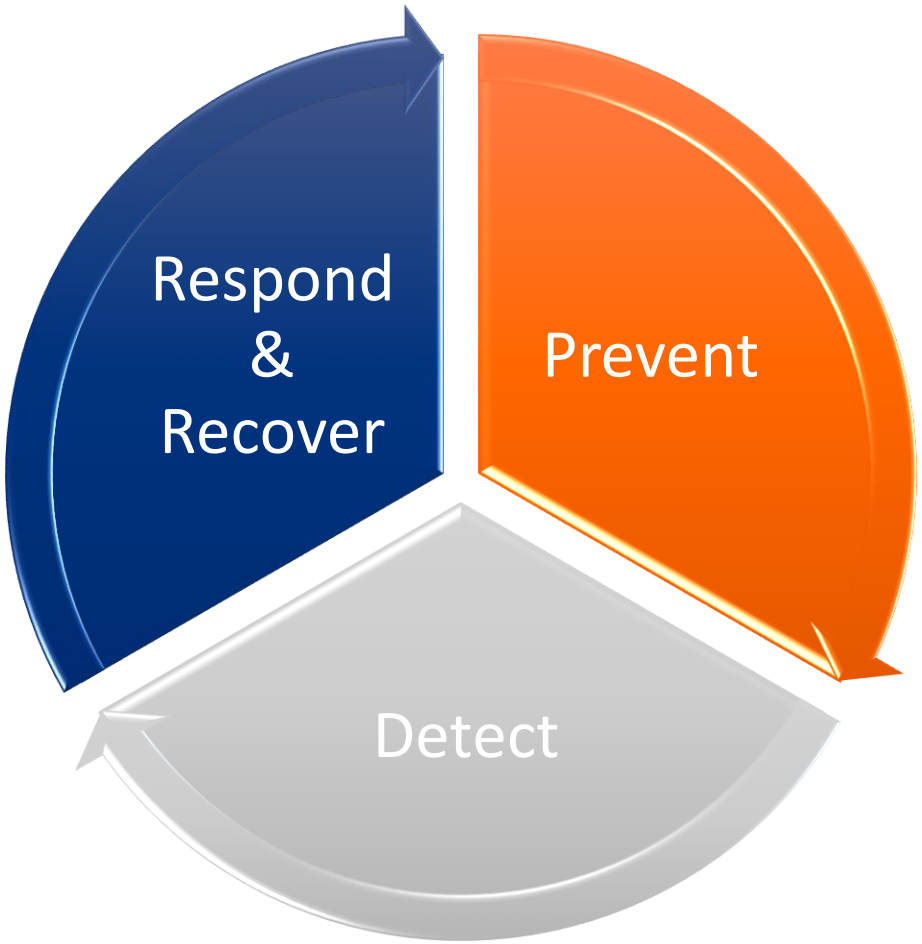
Security is meer dan alleen toegangsbeveiliging

Security Framework
Waar te beginnen?

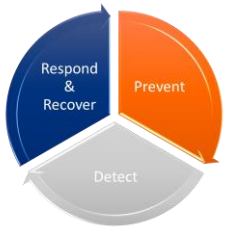
Door toenemende digitalisering, compliance en dreigingen van kwaadwillende is informatiebeveiliging voor elke organisatie steeds belangrijker. **SAP applicaties behoren vaak tot de kroonjuwelen van het bedrijf**, omdat deze vaak enorme waardevolle data bevat. Beschikbaarheid, vertrouwelijkheid en integriteit van deze data en applicatie is van essentieel belang.

In de praktijk blijkt er met name aandacht voor SAP autorisaties. Gelukkig zien we steeds vaker dat dit aan het veranderen is en zijn klanten zich steeds meer bewust van de overige beveiligingsrisico's van SAP systemen.

myBrand heeft deze behoefte van klanten onderkent en biedt, naast haar standaard dienstverlening, een aantal additionele security diensten die klanten kunnen helpen om deze risico's tot een acceptabel niveau te krijgen.



Diensten in 3 categorieën



Prevent

Maatregelen in deze categorie richt zich op het voorkomen van security incidenten. Je kunt hierbij aan maatregelen zoals bijvoorbeeld een firewall en virusscanner denken.

Vulnerability Management & Hardening

Encryptie voor SAP

Detect

Maatregelen in deze categorie richt zich op het detecteren van security incidenten. Klanten gaan er steeds vaker vanuit dat er security incidenten zullen optreden en dat het daarom belangrijk is om deze tijdig te kunnen constateren en onderzoek te kunnen verrichten.

SAP Security Monitoring

Respond & Recover

Maatregelen in deze categorie richten zich op het reageren op en herstellen van security incidenten. Je kunt hierbij denken een security incidentmanagement proces en restore en recovery activiteiten.

Vulnerability Management & Hardening

Hardening (computing)

Het beveiligen van een SAP systeem is een complexe en zeer tijdrovende klus. Daarnaast zijn de informatiebronnen over SAP Security verspreid, uitgebreid, complex en zelfs voor een SAP consultant soms moeilijk te begrijpen.

myBrand heeft deze uitdaging bij klanten herkend en een dienst ontwikkeld (**Vulnerability Management**) waarbij er structureel invulling wordt gegeven aan het preventief beveiligen van het SAP platform, inclusief besturingssysteem en database. Dit biedt de mogelijkheid om altijd een actueel en historisch overzicht te overhandigen aan bijvoorbeeld je stakeholders of auditors. Door dit continue proces, heb je altijd inzicht in de risico's en ben je in staat om hier constant op de sturen.

Doelen vaststellen

Scope bepalen

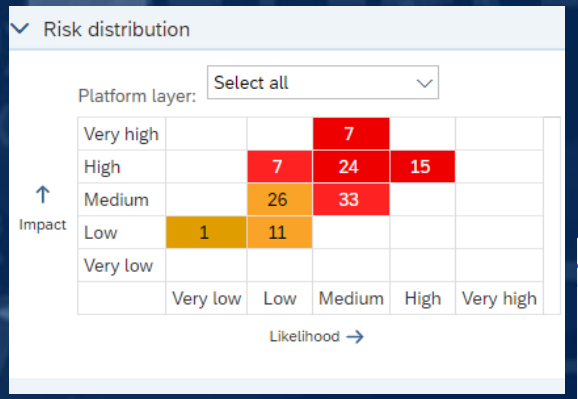
Configuratie scans

Analyse & advies

Operationaliseren

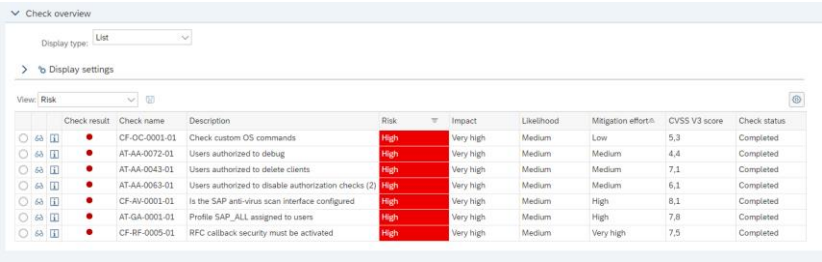
Vulnerability Management

- Meer dan 1750 vulnerability checks
- Alle checks op vulnerabilities op 1 plek
- Beschikbaar door eenmalig een rapport te draaien
- Risico's worden gerangschikt naar prioriteit
- Checks kunnen dagelijks/wekelijks/maandelijks herhaald worden.
- Voortgang in het aanpakken/verwerken van deze risico's kan zo eenvoudig worden gemonitord
- Verschillende runs van rapporten kunnen met elkaar vergeleken worden
- Vulnerabilities worden geregeld bijgewerkt
- Helder en duidelijk dashboard

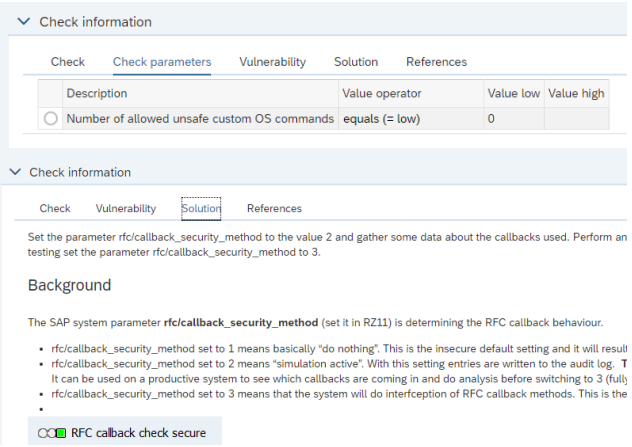


In 1 oogopslag inzicht in je grootste risico’s

- Met een heatmap krijg je in 1 oogopslag te zien waar je risico’s liggen
- Eenvoudig door te klikken op alle risico’s



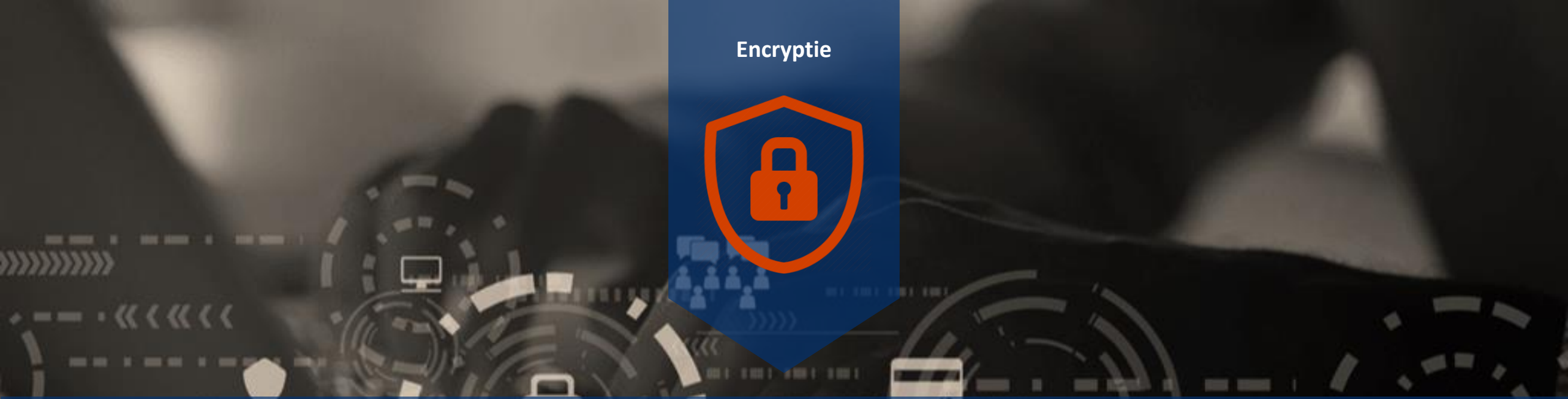
- Inclusief uitleg en oplossing!



Voorbeelden van vulnerabilities

Check name	Description	Risk	Likelihood	Impact	Mitigation effort	Platform layer	Vulnerability type
CF-MC-0002-01	Is message server ACL file restricted (#10KBlaze)	Very high	Very high	Very high	Medium	Application layer	Infrastructure design flaw (SAP)
AU-GL-0002-01	User master SAP* exists in every client and is locked	High	High	High	Very low	Application layer	SAP misconfiguration (Customer)
IN-SC-0006-01	SCC4: Client copier and comparison tool	High	Medium	Very high	Very low	Application layer	SAP misconfiguration (Customer)
IN-SC-0005-01	SCC4: Cross-client object changes	High	High	High	Very low	Application layer	SAP misconfiguration (Customer)
IN-SC-0004-01	SCC4: Changes and transports for client-specific objects	High	High	High	Very low	Application layer	SAP misconfiguration (Customer)
IN-SC-0002-01	SE06: System modifiability	High	High	High	Very low	Application layer	SAP misconfiguration (Customer)
CF-OS-0002-04	Is login as ROOT prohibited	High	High	High	Low	Operating system	Operating system misconfiguration (Customer)
CF-RF-0006-01	Check if RFC accepts expired password	High	High	High	Low	Application layer	SAP configuration not changed on install (Customer)
CO-PP-0012-01	Are SAP password rules enforced	High	High	High	Low	Application layer	SAP configuration not changed on install (Customer)
AT-AA-0024-01	Users authorized to execute all external OS commands	High	High	High	Medium	Application layer	SAP misconfiguration (Customer)
AT-AA-0063-01	Users authorized to disable authorization checks (2)	High	Medium	Very high	Medium	Application layer	SAP misconfiguration (Customer)
AT-AA-0068-01	Users authorized to maintain tables	High	High	High	Medium	Application layer	SAP misconfiguration (Customer)
AT-AA-0043-01	Users authorized to delete clients	High	Medium	Very high	Medium	Application layer	SAP misconfiguration (Customer)
AT-AA-0075-01	Users authorized to display password hashes (S_TABU_NAM)	High	High	High	Medium	Application layer	SAP misconfiguration (Customer)
AT-AA-0074-01	Users authorized to display password hashes (S_TABU_DIS)	High	High	High	Medium	Application layer	SAP misconfiguration (Customer)
AT-AA-0072-01	Users authorized to debug	High	Medium	Very high	Medium	Application layer	SAP misconfiguration (Customer)
AT-AA-0053-01	Users authorized to start imports to production	High	High	High	Medium	Application layer	SAP misconfiguration (Customer)
AT-AA-0040-01	Users authorized to change the system change option	High	High	High	High	Application layer	SAP misconfiguration (Customer)
CF-AV-0001-01	Is the SAP anti-virus scan interface configured	High	Medium	Very high	High	Application layer	SAP misconfiguration (Customer)
AT-AA-0030-01	Users authorized to display table content via RFC	High	High	High	High	Application layer	SAP misconfiguration (Customer)
AT-AA-0029-01	Users authorized to run any (remote) RFC function	High	High	High	High	Application layer	SAP misconfiguration (Customer)
CF-RF-0001-01	ABAP RFC's with stored login credentials	High	High	High	High	Application layer	SAP misconfiguration (Customer)

Encryptie voor SAP



Encryptie

- Netwerkverkeer (“data-in-transit”)
  - SNC
  - SSL
  - https
- Opgeslagen data (“data-in-rest”)
  - Database
  - Files
  - Filesystem
  - Back-up

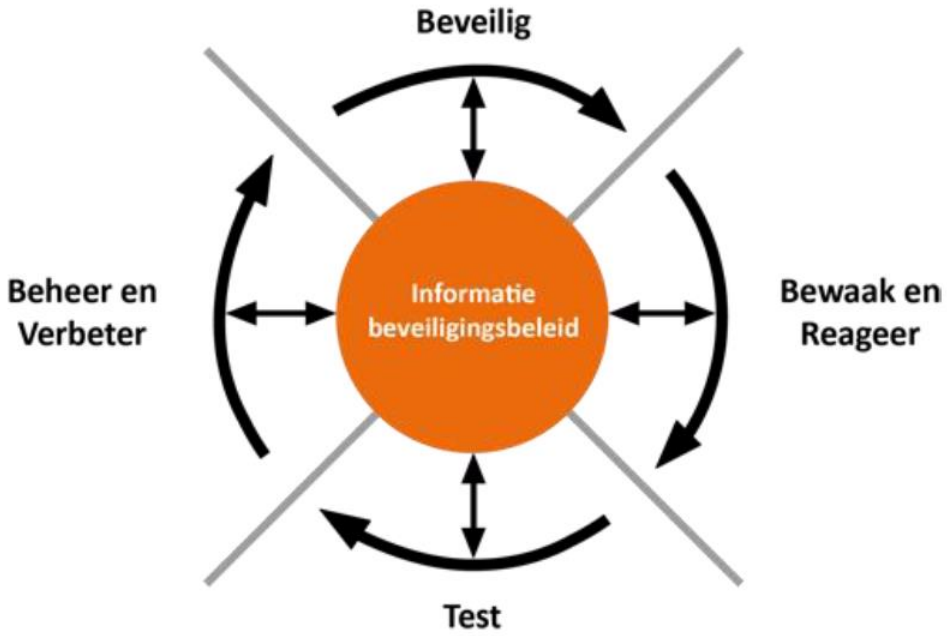
SAP Security Monitoring

SAP Security Monitoring

Informatiebeveiliging is een doorlopend proces waarin de fases: “beveilig, bewaak en reageer, test & verbeter” elkaar constant opvolgen. Het informatiebeveiligingsbeleid vormt hierbij de spil van dit proces. Binnen dit beleid worden de risico’s benoemd en de ingerichte processen en procedures zijn beschreven. Dit beleid wordt naar aanleiding van nieuwe ontwikkelingen continue geactualiseerd en bijgesteld.

Met **SAP Security Monitoring** biedt myBrand een additionele dienst waarmee zij het functioneren van de aanwezige beveiligingscomponenten controleert en bewaakt. myBrand levert de SAP (Security) expertise en kent haar klanten goed. Deze additionele dienst sluit volledig aan op de reguliere dienstverlening die myBrand levert aan haar klanten.

Daarnaast vindt er een constante registratie plaats van de activiteiten die plaatsvinden in de applicatie en op de infrastructuur. Hiermee wordt invulling gegeven aan de “bewaak en reageer” fase van het beveiligingsproces. De SAP applicatie logextractie wordt verzorgd door SAP gecertificeerde third-party software en vereist een installatie via het reguliere SAP transport mechanisme.



Use cases & governance vaststellen

Scope (systemen) bepalen

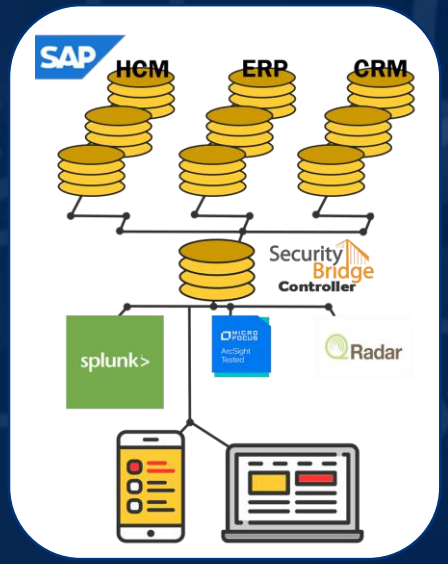
Configuratie Security Monitoring

Testen use cases

Operationaliseren

SecurityBridge

- Meer dan 70 listeners voor honderden situaties
- Real-time signalering op basis van eigen specifieke parameters
- Rapportage over alle listeners met toegang tot tijdslijn van de gesignaleerde events
- Uitgebreide filters om whitelists toe te voegen
- Afhandeling via myBrand supportprocessen
- Maandelijkse rapportage in SLR, inclusief trendrapportage
- Gebruik makend van diensten en systemen van securityspecialist Promax



Voorbeelden van use cases

Listener	Usecase	Beschrijving	Actief/Inactief	Opvolging door:	Actie na Offense
1011	CSX.C002.U011	SAP* Usage	Actief	Technisch Coordinator	TC moet kijken of dit een legitieme actie geweest is (user hoort gelocked te zijn).
1011	CSX.C002.U012	Password Check Failed on Privileged account	Actief	Business/TC	Afhankelijk van het soort user (technisch/functioneel) moet de business of de Tcer valideren of het een legitieme actie was.
1005	CSX.C002.U013	User Unlocked multiple times	Actief	Business	Contact zoeken met persoon die offense getriggerd heeft en redenen valideren.
1005	CSX.C002.U014	Multiple user unlocks by one admin	Actief	Business	Contact zoeken met persoon die offense getriggerd heeft en redenen valideren.
1017	CSX.C002.U016	Login attempt on locked privileged useraccount	Actief	Business	Contact zoeken met persoon die offense getriggerd heeft en redenen valideren.
1011	CSX.C002.U019	Password Change on Priviliged useraccount	Actief	Business	Contact zoeken met persoon die offense getriggerd heeft en redenen valideren.
1005	CSX.C002.U020	User Account Added Outside Business Hours	Actief	Business	Contact zoeken met persoon die offense getriggerd heeft en redenen valideren.
1005	CSX.C002.U021	User created outside IAM/CUA	Actief	Business	Contact zoeken met persoon die offense getriggerd heeft en redenen valideren.
1006	CSX.C003.U020	Assignment of critical authorizations and cover-up identification	Actief	Business	Contact zoeken met persoon die offense getriggerd heeft en redenen valideren.
1009	CSX.C003.U021	Program Debug overwrite	Actief	Functioneel/ABAP	Verantwoordelijke functioneel beheerder moet kijken of er iets veranderd is.
1009	CSX.C003.U022	Program Flow Change	Actief	Functioneel/ABAP	Verantwoordelijke functioneel beheerder moet kijken of er iets veranderd is.
1009	CSX.C003.U023	Forced DB commit/rollback	Actief	Functioneel/ABAP	Verantwoordelijke functioneel beheerder moet kijken of er iets veranderd is.
1009	CSX.C003.U024	Non-exclusive debugging	Actief	Functioneel/ABAP	Verantwoordelijke functioneel beheerder moet kijken of er iets veranderd is.
1009	CSX.C003.U025	Debugger Stopped A Process	Actief	Functioneel/ABAP	Verantwoordelijke functioneel beheerder moet kijken of er iets veranderd is.
1075	CSX.C003.U026	File Mutation Detected	Actief	Technisch Coordinator	TCer moet kijken of dit een legitieme actie was, zo niet, kijken of er iets veranderd is en wie dit gedaan heeft.
1056	CSX.C003.U027	Disabling of Logging of Data for Critical Tables	Actief	Technisch Coordinator	TCer moet kijken of dit een legitieme actie was, zo niet, kijken of er iets veranderd is en wie dit gedaan heeft.
1007	CSX.C003.U028	System Profile Change	Actief	Technisch Coordinator	TCer moet kijken of dit een legitieme actie was, zo niet, kijken of er iets veranderd is en wie dit gedaan heeft.
1064	CSX.C008.U002	Access to Password Hash Values	Actief	Functioneel/ABAP	Verantwoordelijke functioneel beheerder moet kijken of er iets veranderd is.
1063	CSX.C500.U018	SecureBridge Interrupted Collection from SAP (niet voor klant)	Actief	Security team	Kijken op host van de server waarom de log niet meer gevuld wordt.
1019	CSX.C500.U019	SecureBridge IDS Job Status Check (niet voor klant)	Actief	Security team	Kijken in security bridge of de IDS job nog loopt, zo niet dan starten.

Voorbeelden van uitgebreide beschrijving use cases

C002 - Detectie mogelijk misbruik privileged accounts

CSX.C002.U011 - Titel: **Failed Logon using emergency user SAP***

Beschrijving van de Use Case:

De SAP* user is een user die standaard in elk SAP systeem bestaat. Deze user heeft alle rechten.

Risico:

Een mislukte aanmeldpoging op deze user-account is verdacht.

C003 - Detectie configuratie en autorisatie wijzigingen

CSX.C003.U020 - Titel: **User Master Record Changed of Priviliged account**

Beschrijving van de Use Case:

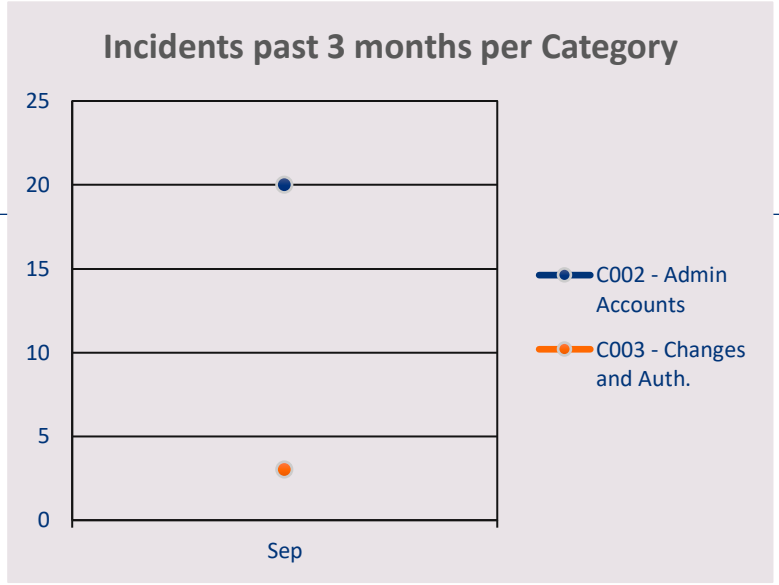
Wijzigingen aan Priviliged Accounts kunnen risicovol zijn. Deze worden met deze use-case gelogd en gemeld.

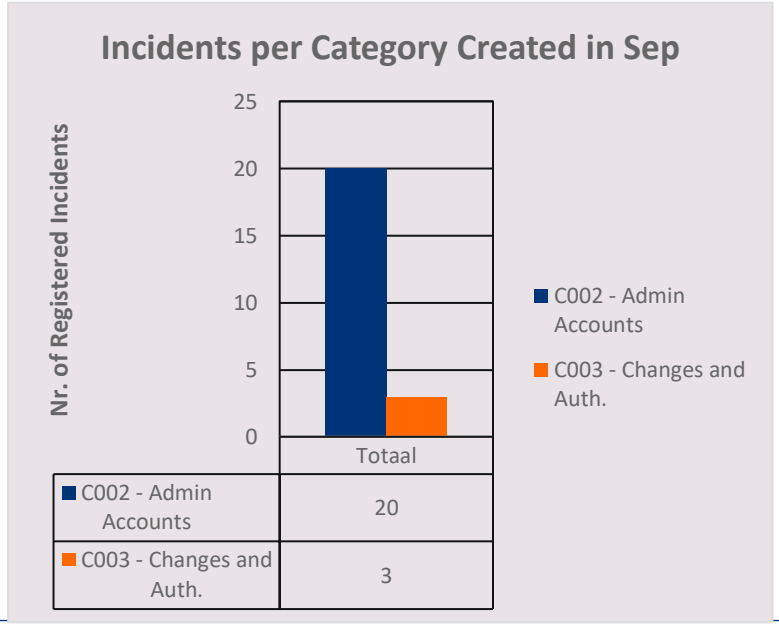
Risico:

Vanuit deze melding kan myBrand informatie verzamelen om de daadwerkelijke wijziging te bepalen en hier eventueel actie op te ondernemen.

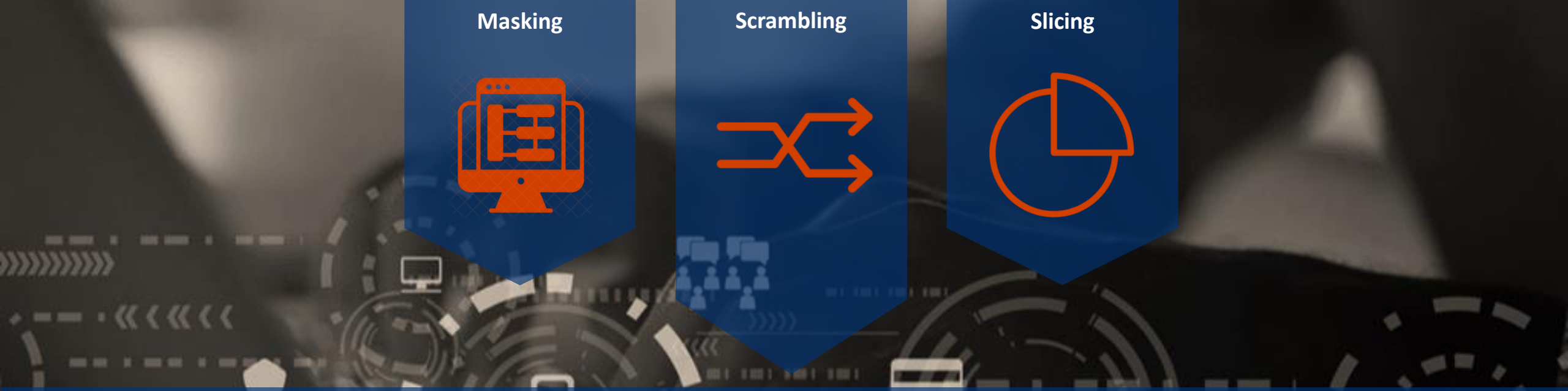
Voorbeeld rapportage

Listener	Usecase	Beschrijving	Aantal geregistreerde events (listener)*	Aantal offenses*
1005	CSX.C002.U013	User Unlocked multiple times	1125	13
1005	CSX.C002.U014	Multiple user unlocks by one admin	1125	1
1005	CSX.C002.U020	User Account Added Outside Business Hours	1125	7
1005	CSX.C002.U021	User created outside IAM/CUA	1125	1
1006	CSX.C003.U020	Assignment of critical authorizations and cover-up identification	12	1
1007	CSX.C003.U028	System Profile Change	6	0
1009	CSX.C003.U021	Program Debug overwrite	0	0
1009	CSX.C003.U022	Program Flow Change	0	0
1009	CSX.C003.U023	Forced DB commit/rollback	0	0
1009	CSX.C003.U024	Non-exclusive debugging	0	0
1009	CSX.C003.U025	Debugger Stopped A Process	0	0
1011	CSX.C002.U011	SAP* Usage	57	1
1011	CSX.C002.U012	Password Check Failed on Privileged account	57	0
1011	CSX.C002.U019	Password Change on Priviliged useraccount	57	0
1017	CSX.C002.U016	Login attempt on locked privileged useraccount	10	1
1056	CSX.C003.U027	Disabling of Logging of Data for Critical Tables	0	0
1064	CSX.C008.U002	Access to Password Hash Values	0	0
1075	CSX.C003.U026	File Mutation Detected	1	0





Masking & Scrambling
(Data Provisioning & Masking)



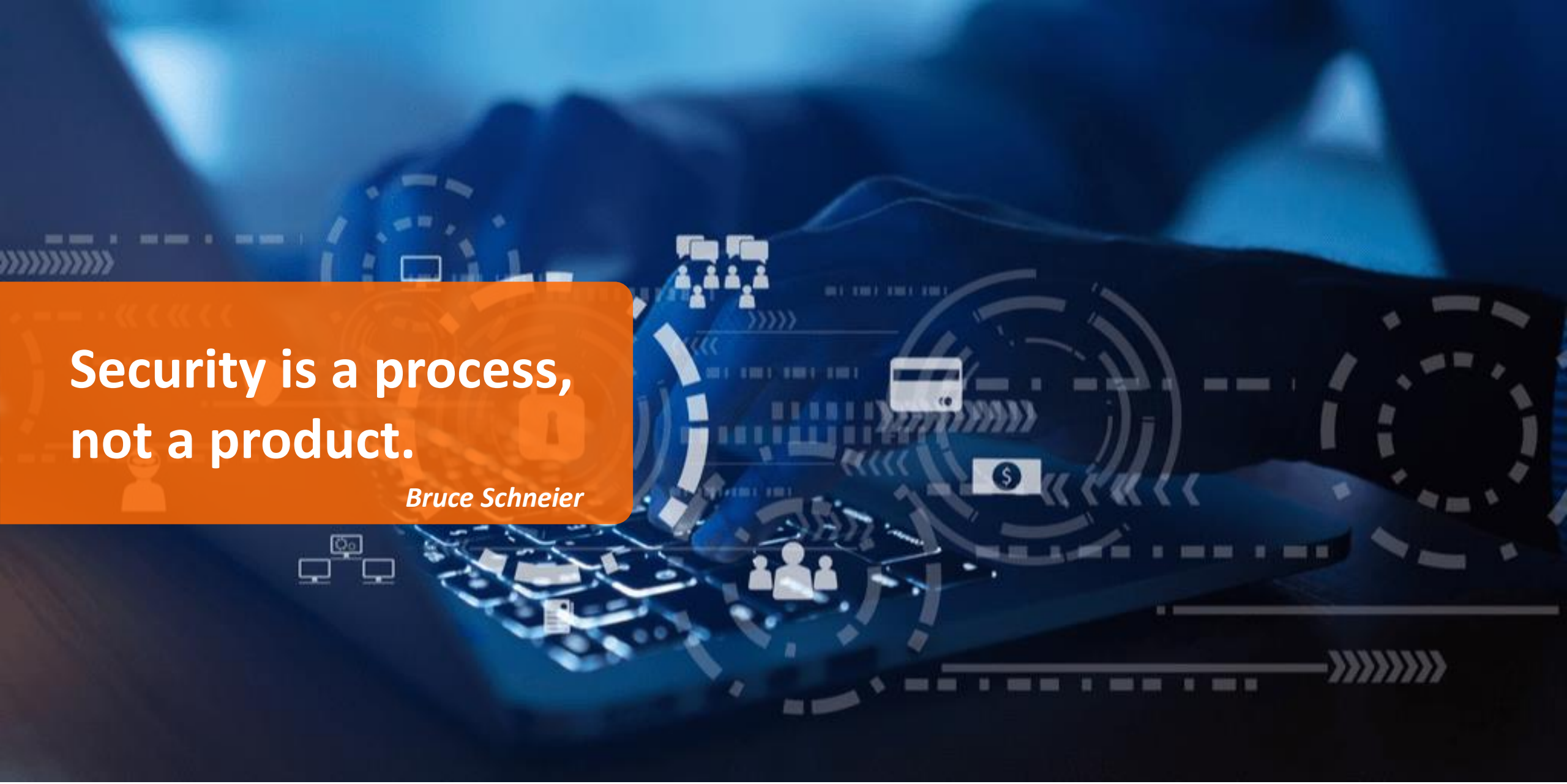
Veel organisaties maken voor het verversen van hun niet productieve omgevingen gebruik van database kopieën of client kopieën. Nadeel van deze manier van werken is dat hiermee:

- de volledige productieve data wordt gekopieerd wat leidt tot een onevenredig grote acceptatie-of ontwikkelomgeving;
- de data onveranderd wordt doorgezet van productie naar een andere omgeving waardoor wellicht personen of instanties bij de data kunnen die hiervoor conform AVG niet gerechtigd zijn;
- er relatief veel nabewerking van de omgeving nodig is, waardoor deze activiteit zowel arbeidsintensief is als relatief veel (doorloop)tijd kost.

Door gebruik te maken van een Data Provisioning and Masking (DPM) tool, zorg je ervoor dat een efficiënte manier voor het maken van een data refresh (transactie en masterdata) wordt gecreëerd.

Op hoofdlijnen doet DPM het volgende:

- Het snel maken van een extract van de productie omgeving die als basis dient voor de kopie naar de doelomgeving. Tijdens de extractiefase (Export) wordt de privacygevoelige data gemaskeerd en gescrambeld. Daardoor is de data niet meer te herleiden naar een persoon.
- Indien gewenst wordt een beperkte dataset gebruikt (company code of time slice op basis van een vanaf datum) waardoor de kopie die gemaakt wordt significant kleiner is dan de bestaande productieomgeving. Dit wordt ook wel slicing genoemd.



Security is a process, not a product.

Bruce Schneier

Bedankt voor je deelname

Bekijk op www.VNSGFocusOnline.nl welke sessies er nog meer zijn!

myBrand® | CONCLUSION