VNSG Themadag Security & Controls | 16 juni 2022

09.00 - 10.00	**Ontvangst deelnemers / koffie**		
10.00 - 10.45	**Plenaire opening - Everything you always wanted to know about securing RISE with S/4HANA**		
	Arndt Lingscheid, Global Solution Owner Cybersecurity and Dataprotection, Product Management - SAP Labs & Patrick Boch, Product Management S/4HANA Security - SAP SE		
	"Business transformation as a service" is what RISE with SAP S/4HANA offers. But what are the security implications of that move? What are the areas that customers need to focus on, security wise, when moving to the cloud and which other areas will be something that SAP customer can neglect because they are now the responsibility of SAP as a cloud provider? The opening keynote session hosted by SAP Solution Management will provide an overview of the security services of RISE with SAP S/4HANA. Question like: what do customers need to consider when migrating the SAP S/4HANA cloud and how can SAP secures their new core ERP solution for them, will be answered during this session. Join this session to: • Get more details on the security implications of SAP S/4HANA • Know which areas are important to focus on when moving to the cloud • Learn about the general security of the cloud services from SAP S/4HANA		
11.00 - 11.45	**Emergency Access Management – Een gevoelig onderwerp**	**Introductie tot access management in SAP Analytics Cloud (SAC)**	**The Threat Landscape is Transforming: Understanding The Importance of Business Critical Application Protection - Engelstalig**
	Tiede-Jan de Jong, Platform Security NL lead - Accenture & Yee-Tee Ho, SAP Security & Authorizations Specialist Marel & Vincent Doux, SAP COE for GRC, Cybersecurity and Data Protection - SAP	Joost van Moerkerk, SAP COE for GRC, Cybersecurity and Data Protection - axl & trax	Pedro Pérez, Sales Engineer - Onapsis & André Ros, Director, Alliances & Channels EMEA & APAC
	Emergency Access Management (EAM) in SAP is bedoeld om gebruikers in staat te stellen op een veilige en gecontroleerde manier taken uit te voeren die buiten hun normale dagelijkse verantwoordelijkheden vallen. Verhoogde toegang zoals debugging, herconfiguratie van de applicatie, veranderen van kritische systeemparameters, hebben enorme veiligheids- en operationele implicaties. Alleen vertrouwde gebruikers zouden toestemming mogen krijgen om dergelijke activiteiten uit te voeren en deze activiteiten moeten ook worden vastgelegd en beoordeeld vanuit het oogpunt van een audit. Het lijkt er echter op dat elke organisatie worstelt met dit onderwerp en het moeilijk vindt om het goed te doen. Omdat het een moeilijk, maar interessant, onderwerp is en omdat auditors en internal control steeds meer aandacht besteden aan Emergency Access Management, heeft Accenture onderzoek gedaan onder honderden klanten om inzicht te krijgen in hun huidige situatie, vereisten en wensen bij het beheren van toegang in noodsituaties. Tijdens deze sessie bespreekt Accenture de EAM onderzoeksresultaten en good practices, terwijl SAP een korte systeemdemonstratie geeft, deelt een (klant)deskundige zijn ervaringen vanuit de praktijk.	**Krijg inzicht in de eerste ervaringen met het autoriseren van gebruikers in SAP Analytics Cloud (SAC). Tijdens de sessie worden lessons learned gedeeld die zijn opgedaan tijdens het opzetten van het rollenmodel.**	**Business-critical applications such as SAP, are the lifeblood of every organization, with 87% of the world's transaction revenue touching these systems. These applications house customers, sales, financial, product, services, employee information, and trade secrets – and hackers are starting to take notice.** Recent joint threat intelligence reporting from SAP and Onapsis shows threat actors using various multiple attack vectors to target and compromise organizations running unpatched and unprotected SAP applications. This presentation will deliver an in-depth overview of this threat activity, showcasing hackers possessing sophisticated knowledge of business-critical applications to actively target and exploit unsecured SAP applications through a varied set of techniques, tools and procedures.
11.45 - 13.00	**Lunchpauze**		
13.00 - 13.45	**All you need is……data**	**Verantwoordelijk voor beveiliging van eigen SAP- systemen, maar HOE?**	**Managing SAP User Access – IDM vs GRC Solutions - Engelstalig**
	Meta Hoetjes, SAP Security and Controls expert - CSI Tools	Patrick Mensink, Security Officer – myBrand, Joris van de Vis, SAP Security specialist - Protect4S, Marcel Antons, Directeur Strategie & Innovatie – myBrand	Emile Steyn, Business Unit Director - Soterion Benelux
	We weten allemaal dat de data in SAP van het grootste belang is en goed beschermd moet worden. In deze presentatie legt Meta Hoetjes van CSI Tools uit op welke manieren de data bereikt kan worden (via de verschillende lagen) en hoe deze data goed beschermd kan worden. Deze sessies is interessant, omdat het beschermen van data meer is dan alleen functiescheidingsconflicten controleren.	**De wereld verandert snel. Cyberdreiging en druk vanuit wet- en regelgeving (compliancy en audits) zijn enorm toegenomen. Toch zien wij in de praktijk nog te vaak dat SAP-gebruikers niet of nauwelijks investeren in SAP Cybersecurity, ondanks dat het eigenaarschap van de data bij de gebruiker ligt.** Enerzijds komt dat doordat SAP cyberrisico's vaak nog een blinde vlek zijn en anderzijds omdat er vaak onterecht vanuit wordt gegaan dat de SAP-beheerpartner dat standaard volledig regelt. De werkelijkheid is weerbarstiger en betekent in de praktijk vaak een "shared responsibility model" waar partijen over met elkaar in gesprek dienen te gaan. In een interactieve setting worden twee experts geïnterviewd en hebben deelnemers ook de gelegenheid bij te dragen aan de discussie door vragen te stellen of voorbeelden te geven.	**Assigning SAP user access via an Identity Access Management solution versus the Access Control (GRC) solution. The pros and cons of both provisioning methodologies, as well as when to consider a hybrid approach.** Identity Access Management solutions can bring about great efficiencies in the user access provisioning process but are less well equipped to identify access risk. On the other hand, access control solutions are well equipped to identify access risk but are less powerful at user provisioning. In this session we will discuss some scenarios where the benefits of provisioning SAP access using an IAM solution outweigh that of GRC solution, as well as other scenarios where provisioning access using the Business Role concept (of the access control / GRC) solution are more beneficial than that of the IAM solution. Key take aways • Pros and cons of user provisioning of the different methodologies • Understanding your organization's business objectives to help you decide on the most appropriate provisioning strategy

14.00 - 14.45	**Implementatie SAP GRC Access Control bij Vitens in een hybride SAP en non SAP (cloud)landschap**	**Achmea en haar road to security: ervaringen, geleerde lessen en toekomstplannen**	**Maak het onderhouden en testen van SAP en Fiori autorisatie rollen gebruikersvriendelijker en tot 70% sneller!**
	Ilone Roelofsen, Senior Functioneel Beheerder SAP Security - Vitens & Virgil Verloop, Independent SAP Security & GRC Consultant - Profilus	Jaap van der Meer, Sales Director - SecurityBridge & Frans Suijkerbuijk, SAP Development Application Partner - SecurityBridge & Robert Wegh, IT Security - Achmea & Eric van Berkel, SAP Security & Authorisation Specialist - Achmea	Nico Kuijper, Data governance & management / Privacy Consultant - D&IM Services BV
	Leer hoe Vitens, het grootste drinkwaterbedrijf van Nederland, SAP GRC Access Control gebruikt voor SAP en non-SAP, in combinatie met SAP IAG voor cloud systemen. Position Based Access Control heeft geïmplementeerd en SuccesFactors als bronsysteem heeft gekoppeld. Daarnaast hoor je hoe Vitens alle 4 de submodules gebruikt inclusief joiner, mover leaver, extension processen, (Azure) Active Directory provisioning, SuccesFactors als target, Manual provisioning, Java provisioning, SOD Review, User Access Review, Password Reset, Access Request Management, Firefighter, Ruleset Management en Business Role Management gebruikt. Tot slot hoe Snow Optimizer for SAP Software wordt ingezet voor een optimaal en schoon landschap als aanvulling op SAP GRC Access Control.	**Achmea werkt hard aan het beveiligen van haar SAP-omgevingen. In deze presentatie kun je leren van de ervaringen die zij hebben opgedaan bij de implementatie van Real time threat detection, Data loss prevention, Code Scanning en Compliance monitoring.** Implementatie van een platform houdt ook in dat de organisatie daarop ingericht moet worden. Van de lessen die Achmea hier geleerd heeft delen zij graag hun ervaringen. Ook wordt in deze presentatie aandacht besteed aan de dagelijkse activiteiten rondom security management, zoals het inregelen van de verschillende sensors, het whitelisten etc. Specifiek wordt daarbij ingegaan op de uitdagingen rondom gebruikersbeheer en individuele rechten. De presentatie wordt afgerond met een vooruitblik op een nieuwe module in het platform “Violation Management”.	**Ben je benieuwd hoe bedrijven als Mercedes Benz, Munich Airport, Electrolux en anderen het onderhouden en testen van hun SAP-autorisatieconcept hebben verbeterd? Neem dan deel aan deze sessie!** Het testen van SAP-autorisaties zal voor velen nooit een hobby worden. Vaak is niet volledig duidelijk wat getest moet worden (welke transacties, rapporten, functionaliteiten). Testers worden ook herhaaldelijk geconfronteerd het autorisatiefouten welke teruggekoppeld moeten worden (SU53). Deze zullen vervolgens gecorrigeerd moeten worden en opnieuw getest. Dit kost vanzelfsprekend erg veel tijd tot frustratie van sommige eindgebruikers. Niet alleen het onderhouden en testen van het autorisatieconcept is resource intensief. Er komen ook veel vernieuwingen aan als het gaat om het (her)inrichten van uw SAP-autorisatieconcept. Organisaties welke willen migreren naar S/4HANA zullen voor een belangrijk deel hun autorisatie concept en nieuwe Fiori rollen moeten gaan (her)inrichten, testen en onderhouden. Kortom: uitdagingen genoeg om een SAP autorisatieconcept te onderhouden en te vernieuwen in de komende jaren. Gelukkig bestaan er oplossingen welke jouw organisaties optimaal kunnen ondersteunen in het onderhouden en testen van jouw SAP autorisatieconcept op een wijze welke veel van de genoemde knelpunten rond het inrichten en testen van rollen wegneemt en kan bijdragen tot een efficiency verbetering tot zelfs 70%!
14.45 - 15.15	**Koffiepauze**		
15.30 - 16.15	**Plenaire afsluiting - #hackenislief!**		
	Casper Kuijper, Security & Hybrid Cloud Engineer at LinProfs BV		
	Het Dutch Institute for Vulnerability (DIVD) neemt jullie mee in een wereld van duistere figuren die zich verschuilen op zolderkamers, verpakt in capuchons, omringt door lege pizzadozen en lege bekers koffie. Hoe onderscheiden we vriend van vijand in deze vreemde tijd waarin de ene informatie-oorlog de andere opvolgt en hoe voorkom je dat je zelf slachtoffer wordt? Een blik op de toekomst van informatisering door de ogen van een groep hackers met een brede kijk op het informatielandschap.		
16.15 - 17.00	**Afsluitende borrel**		