COMunities of ExperTs CYB & SIL

Intrusion Detection

En partenariat avec :

05/06/2018

9:00	**Introduction** *CNES*
9:15	**Modern tactics, techniques and procedures for targeted malicious attacks** *Talos –Vanja Svajcer*
9:50	***Le renseignement au service des entreprises*** *Thalès – Ivan Fontarensky*
10:25	**Security Orchestration, Automation and Response** *McAfee - Boubker Elmouttahid*
10:55	Coffee Break
11:15	**Apport des plateformes de SIRP dans la gestion des incidents** *Sogeti – Vincent Mammeri et Grégory Beauverger*
11:50	**ESA-CERT lessons learned** *European Space Agency - Andrea Baldi & Sergio Pagnozzi*
12:25	Lunch
14:00	**Panel** *Hervé Schauer Sécurité - Hervé Schauer* *Sogeti – Fabien Pouget*
14:35	**Détection d'intrusion sans SIEM – Approche Elastic** *Elastic – Ronan Tallec & Baha Azarmi*
15 :10	**Coffee Break**
15:25	**Machine Learning appliqué à la detection d'anomalie** *OCTO technologies – Constant Bridon*
16:00	**Satellite Control Center Operators internal threats detection** *Thales Aliena Space - Franck Perrin*
16:35	**Conclusion** *CNES – COMET-CYB*

Biographies

Talos –Vanja Svajcer

Vanja Svajcer works as a Technical Leader for Cisco Talos. He is a security researcher with more than 15 years of experience in malware research and detection development. Prior to joining Talos, Vanja worked as a Principal researcher for SophosLabs and led a Security Research Team at Hewlett Packard Enterprise. Vanja enjoys tinkering with automated analysis systems, reversing binaries and other malware types. He thinks time spent scraping telemetry data for signs of new attacks is well worth the effort.

In his free time, he is trying to improve his acoustic guitar skills and often plays basketball, which at his age, is not a recommended activity.

Thalès – Ivan Fontarensky

Ivan Fontarensky dirige l'activité de renseignement sur la menace (Threat Intelligence) de Thales. Ivan a mené de nombreuses réponses à Incidents pour lutter contre des attaques avancées visant des organisations françaises. Précédemment, il a travaillé chez Airbus DS Cybersecurity et Cassidian CyberSecurity où il effectuait notamment des analyses « forensic » pour la justice sur différents types de plates-formes. Il a également travaillé pendant plusieurs années au sein du département français de la Sécurité intérieure en tant qu'expert informatique forensic et mise au clair.

McAfee - Boubker Elmouttahid

Boubker Elmouttahid, Enterprise Architect, at McAfee. Boubker has over 18 years' experience in the security industry. Industry leading specialist in building and proposing cyber security solutions to Enterprise organizations and partners. Able to design and scope McAfee security technology as well as partner's security products as a single integrated platform. A key member in building solution show showcase and leading security workshops.

He is currently specialised in security in the following verticals: finance, critical infrastructure, Cloud and Industrial IoT in EMEA. Boubker is a Certified Information Systems Security Professional (CISSP), a Certified Information Systems Manager (CISM), and Certified in Risk and Information Systems Control (CRISC) and SABSA. He has been a member of the Information Systems Audit and Control Association (ISACA) since 2007.

Sogeti – Alexis LE FLOCH

Sogeti – Vincent MAMMERI

European Space Agency - Andrea Baldi

European Space Agency - Sergio Pagnozzi

Hervé Schauer Sécurité – Hervé Schauer

Hervé Schauer est un expert renommé internationalement en cybersécurité (ou sécurité des systèmes d'information).
https://www.schauer.fr/biographie/

Sogeti – Fabien Pouget

Elastic – Ronan Tallec

Elastic – Baha Azarmi

OCTO technologies – Constant Bridon

Constant est consultant au sein de la tribu Big Data Analytics d'Octo Technology depuis plus 2 ans.

Diplômé de l'Ecole Normale supérieure de Cachan, il dispose d'une solide expérience de la recherche appliquée et d'une forte culture de veille technologique. Il est aussi co-auteur de 4 articles publiés en conférence spécialisées, 2 en Télécommunications et 2 en Interface Homme - Machine.

Formé en mathématiques appliquées, Constant s'est spécialisé en Data Science au NICTA (désormais Data61 de CSIRO) de Sydney, le premier institut de recherche en ICT d'Australie, au sein du Machine Learning Research Group.

Convaincu que la valorisation des données passe par l'industrialisation, Constant s'est attaché à développer une expertise en architecture de données (classique, distribuée, ad hoc...) afin de proposer des solutions de data science full stack. Il est par ailleurs certifié HDPCD, développeur Pig Hive et Spark pour la HDP.

Soucieux de partager son savoir, Constant entrecoupe son activité de consulting avec une activité soutenue de formation : Fondamentaux de la Data Science, Data Science Avancée, Développer en Pig&Hive d'hortonworks, Développer des applications spark en Python et en Scala. Son prochain engagement ? Devenir formateur AWS Big Data.

Enfin, Constant n'a pas pu se détacher de ses premières amours de chercheur, et il mène une veille conséquente sur deux sujets de data science : l'interprétation de modèles ensemblistes (gradient boosting), et l'application du Machine Leanrning à la maintenance prédictive en milieu industriel. Il a pu présenter ses résultats dans 4 conférences en 2017.

Thales Aliena Space - Franck PERRIN

Engineering degree in Computer Science and Management

- Since 2017: Thales Alenia Space cybersecurity expert in charge of strategic cybersecurity roadmap and offer definition
- 2015-2017 : Referent of the corporate program Cyber secured in Thales for Thales Alenia Space activities
- 2011-2015 : Service delivery manager for CNES IT outsourcing and Cyber-security regional referent (Thales Services)
- 2007-2010 : Enterprise Infrastructure Management Services national Practice Leader (SOGETI Regions)
- 2005-2006 : Security domain director of Unisys France
- 2001-2005 : Manager of the Managed Security Services of Thales group (first SOC creation of the group)
- 1995-2001 : Consultant / Pre sales manager on recovery services and high availability solutions for different company (IBM, Veritas Software, Open group)