FINAL DRAFT

CYBER CHIEF EXPERIENCE 2016

	Mon	Tue	Wed	Thu	Fri
Date	05-Sep	06-Sep	07-Sep	08-Sep	09-Sep
Topic	**Governance**	**Prevent**	**Detect**	**Respond**	**Malware analysis**
Senior lecturer	Willem van der Valk	Tom Schuurmans	Layla Alabdulkarim	Bas de Vogel	Jelle Niemantsverdriet
09:00	Introductions	Recap, form groups	Recap	Recap	Recap
09:15					
09:30	Forming groups for day 1	Introduction – secure part of the secure, detect, respond cycle	Form groups	Form groups	Form groups
09:45					
10:00	Introduction Jan/Pieter				
10:15	Introducing GSS (business case) (Joost)	Presentation network architecture GSS Case	Security monitoring theory SOCs (placement, qualifications, roles/skills - management perspective)	Composition of CERT/CIRT teams	
10:30			Quick overview: Vulnerability management, Threat intelligence, Log management		
10:45	Embracing the digital revolution with confidence			Principles of (cyber) incident response	
11:00	Theory: Three drivers that improve performance and create risk Theory: Digital dilemma	Practical work: case - network architecture	Monitoring in relation to business: SIEM + variations, assets, filters, procedures, use cases	Relation and differences Incident Response/Forensics	
11:15	Theory: Crown Jewels (Information Assets: BII, PII, liquidities)			Sample cases	Malware analysis
11:30	Break				
11:45	Get to know the attackers			IR Demonstration	
12:00	Theory: Get to know the att[H]ackers: sophistication and determination				
12:15	Exercise: Determine relevant threats for GSS	Discussion of challenges and solutions in case	Threat Intelligence exercise		
12:30	Lunch	Lunch	Lunch	Lunch	Lunch
12:45					
13:00					
13:15					
13:30		Consulting skills - translating technical to business relevant	Use case design	Crisis management vs. Incident management vs. Disaster recovery	
13:45					
14:00	Advising GSS on their cyber security strategy	Practical work: translate technical vulnerability report from technical to business		Crisis management in business: policies, plans, and practical tests	Malware analysis
14:15	Theory: Security framework: Secure, Vigilant, Resilient (NIST)		Placement of log collector		
14:30	Theory: Organizational governance cyber security (Role of the CISO, allocation of InfoSec in the organization)				
14:45					
15:00	Exercise: Develop a cyber security roadmap for GSS	Enterprise vulnerability management	Log management exercise	Exercise: design crisis management plan for GSS	Recap
15:15					
15:30		Practical work: Design a vulnerability management program for CSS			Award ceremony
15:45					
16:00	Presentation preparation	Discuss resultst and prepare presentations (practicals 2 and 3)	Presentation preparation	Presentation preparation	Borrel
16:15					
16:30					
16:45		Student presentations: - Results of security status assessment for GSS board - Management summary including advice on remediation actions (taking into account budget, current network, and results of the test)	Student presentations: - Setup of logging and monitoring at GSS, including use cases - Relation of detection capability to business value	Student presentations: - IR/CR planning/setup for GSS	
17:00	Student presentations: - Cyber security roadmap for GSS				
17:15					
17:30					
17:45					
18:00					
18:15					
18:30	Dinner/chillax time	Dinner/chillax time	Dinner/chillax time	Dinner/chillax time	
18:45					
19:00					
19:15					
19:30					
19:45					
20:00		Lock picking Social engineering OSINT (Ari Davies et al.)			
20:15	CTF (Gijs Hollestelle et al.)		(free time)	Cyber Security in Practice (TED style talks) - Roel van Rijsewijk (security as a business enabler) - Jelle Niemantsverdriet (designing unobtrusive security)	
20:30					
20:45					
21:00					
21:15					
21:30					
21:45					
22:00	(free)				
22:15					
22:30					