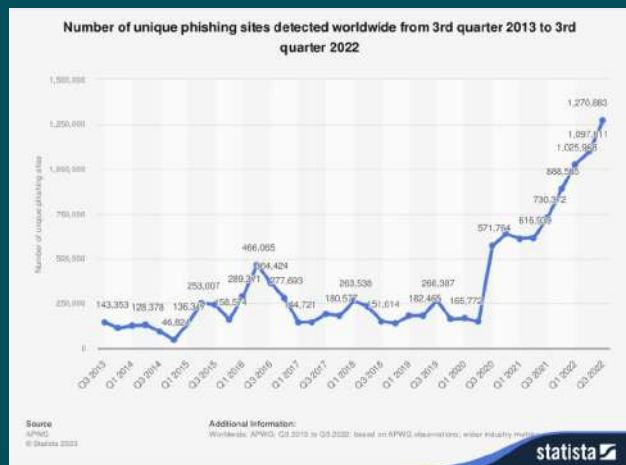




Cyber Security Operations The Frontline of Digital Protection

Evolution on Cyber Attacks and Consumer Fraud

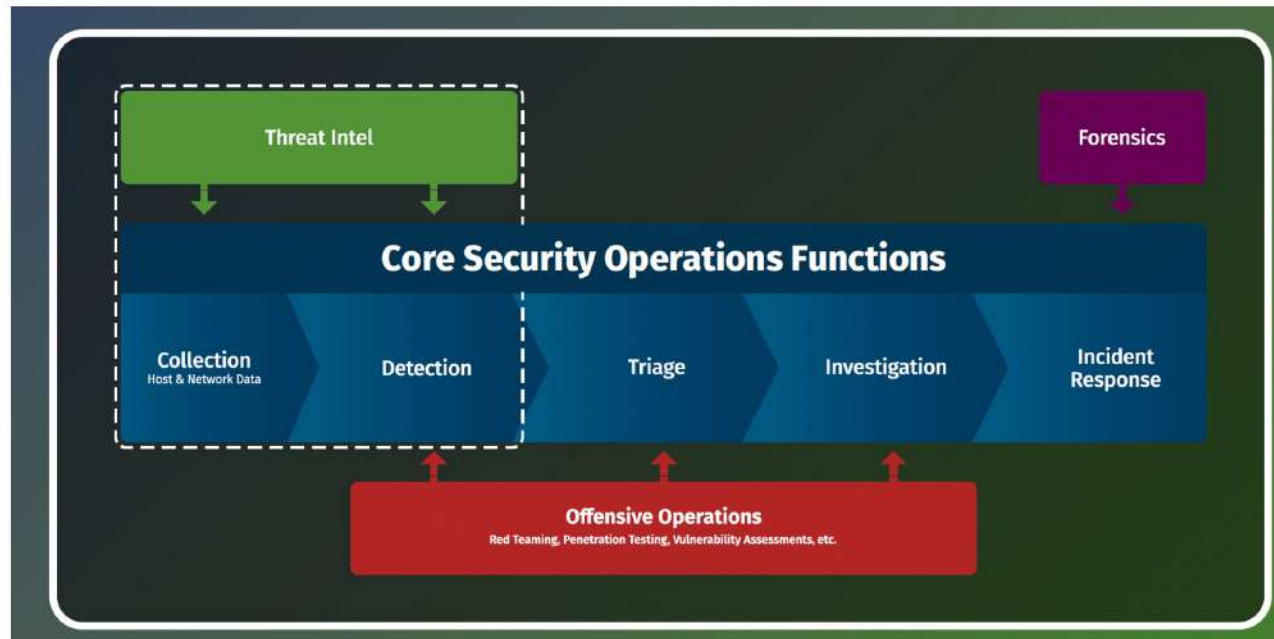


- Dwell time has remained stable ~270 days
- Cycle time has gone down from 270 days to < 10 days in 2024
- Avg time from CVE disclosure to exploit <48h (impact AI!)
- Steep increase in consumer fraud



Security Operations is not an option anymore

- APT's are scanning everybody, not just big organizations and governments
- Vulnerabilities are discovered much faster and in higher numbers
- Attacks become more sophisticated and stealthy (LOTL! – example Spider since mid 2023)
- Thousands of cyber attacks per day
- A proactive approach has become mandatory (note use of CTI in new version ISO27k!)
- MITRE, NIST CSF, CCB provide frameworks



Core SOC activities (Blue Team OPS):

- **Data collection:** What's happening on the network/devices
- **Detection:** Identify items of interest from data collected
- **Triage and investigation:** Confirming and prioritizing detected issues
- **Incident response:** Responding to and minimizing the impact of attacks

Specialty / Auxiliary Functions:

- **Threat Intelligence:** Collecting information to improve attack detection
- **Forensics:** Supporting IR with deep research and reverse engineering
- **Self-Assessment:** Vulnerability assessment, penetration testing, Red Teaming, inventory, etc...

Knowledge landscape becomes gigantic

Cybersecurity Training Roadmap

SANS' comprehensive course offerings enable professionals to deepen their skills at every stage of their cybersecurity career.

COURSE LISTING KEY:

Topic	Course Code	SANS Certification
Essentials	ICS400 ICS/SCADA Security Essentials GICSP	
	Course Title	

Baseline Skills

New to Cyber Security	Concepts, Terms & Skills
Cyber Security Fundamentals	SEC001 Introduction to Cyber Security GICF

You are experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Techniques	Present, Defend & Maintain
Every Security Professional Should Know	
Security Essentials	SEC001 Security Essentials Bootcamp Style GICE
Hacker Techniques	SEC004 Hacker Tools, Techniques, Exploits, and Incident Handling GCH
All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense in depth, understand how attacks work, and manage incidents when they occur. To be secure, you should set a high bar for the baseline set of skills in your security organization.	

Security Management	Managing Technical Security Operations
Every Security Manager Should Know	
Leadership Essentials	MGT010 Security Leadership Essentials for Managers GISC
Critical Controls	SEC046 Implementing and Auditing the Critical Security Controls - In-Depth GCEC
With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those managers will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.	

Focus Job Roles

You are experienced in security, preparing for a specialized job role or focus

Monitoring & Detection	Intrusion Detection & Monitoring Over Time
Scan Packets & Networks	
Intrusion Detection	SEC030 Intrusion Detection In-Depth GCIH
Monitoring & Operations	SEC031 Continuous Monitoring and Security Operations GCIH
The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and to interpret their output.	

Penetration Testing	Vulnerability Analysis & Ethical Hacking
Every Pen Tester Should Know	
Networks	SEC060 Network Penetration Testing and Ethical Hacking GPNP
Web Apps	SEC062 Web App Penetration Testing and Ethical Hacking GWAPT
The professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires different ways of thinking and different tools. Penetration testing skills are essential for defense specialists to improve their defenses.	

Incident Response & Threat Hunting	Host & Network Forensics
Every Forensics and IR Professional Should Know	
Incident Forensics	FOR050 Windows Forensic Analysis GCFE
Network Forensics	FOR058 Advanced Incident Response, Threat Hunting, and Digital Forensics GCIR
Network Forensics	FOR057 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response GCIN
Whether you're seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.	

CISPP Training	MGT014 SANS Training Program for CISPP Certification GISP
----------------	---

Crucial Skills, Specialized Roles

You are a candidate for advanced or specialized training

Cyber Defense Operations	Hardware Specific Defenses
Specialized Defensive Area	
Blue Team	SEC040 Blue Team Fundamentals: Security Operations and Analysis GCIH
OSINT	SEC040 Open-Source Intelligence (OSINT) Gathering & Analysis GCIH
Advanced Generalist	SEC041 Advanced Security Essentials - Enterprise Defender GCIH
Windows/PowerShell	SEC045 Securing Windows and PowerShell Automation GCIH
Linux/Unix Defense	SEC046 Securing Linux/Unix GCIH
SER	SEC045 SER with Tactical Analytics GCIH
Other Advanced Defense Courses	
Security Architecture	SEC030 Defensible Security Architecture and Engineering GCIH
Adversary Emulation	SEC041 Defeating Advanced Adversaries - Purple Team Tactics and APT Chain Defenses GCIH

Specialized Penetration Testing	Recent Techniques & Areas
In-Depth Coverage	
Vulnerability Assessment	SEC040 Enterprise and Cloud Threat and Vulnerability Assessment GCIH
Networks	SEC040 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking GCIH
Web Apps	SEC062 Advanced Web App Testing, Ethical Hacking, and Exploitation Techniques GCIH
Mobile	SEC065 Mobile Device Security and Ethical Hacking GCIH
Cloud	SEC068 Cloud Penetration Testing GCIH
Wireless	SEC067 Wireless Penetration Testing and Ethical Hacking GCIH
Python Coding	SEC063 Automating Information Security with Python GCIH
Adversary Emulation	SEC041 Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection GCIH

Digital Forensics, Malware Analysis & Threat Intel	Specialized Investigative Skills
Essentials	
SFR Essentials	FOR038 Digital Forensics Essentials GCIH
Malware Analysis	FOR039 Reverse-Engineering Malware: Malware Analysis Tools and Techniques GCIH
Threat Intelligence	FOR037 Cyber Threat Intelligence GCIH
Cyber Threat Intelligence	FOR037 Cyber Threat Intelligence GCIH
Digital Forensics & Media Exploitation	FOR040 Battlefield Forensics & Data Acquisition GCIH
Smartphone Analysis	FOR035 Smartphone Forensic Analysis In-Depth GCIH
Memory Forensics	FOR036 Advanced Memory Forensics & Threat Detection GCIH
Mac Forensics	FOR038 Mac and iOS Forensic Analysis and Incident Response GCIH

Advanced Management	Advanced Leadership, Audit & Legal
Management Skills	
Planning, Policy, Leadership	MGT014 Security Strategic Planning, Policy, and Leadership GCIH
Managing Vulnerabilities	MGT016 Managing Security Vulnerabilities, Enterprise and Cloud GCIH
Project Management	MGT015 IT Project Management, Effective Communication, and PMP® Exam Prep GCIH
Audit & Legal	
Audit & Monitor	AUD007 Auditing and Monitoring Networks, Perimeters & Systems GCIH
Law & Investigations	LEG020 Law of Data Security and Investigations GCIH



SANS The most trusted source for cybersecurity training, certifications, degrees, and research

Industrial Control Systems	
Every ICS Security Professional Should Know	
Essentials	ICS400 ICS/SCADA Security Essentials GICSP
ICS Defense & Response	ICS001 ICS Active Defense and Incident Response GRD
ICS Advanced Security	ICS002 ICS Cybersecurity In-Depth
NERC Protection	
NERC Security Essentials	ICS400 Essentials for NERC Critical Infrastructure Protection GICSP

Cloud Security	
Every Cloud Security Ops Person Should Know	
Essentials	SEC048 Cloud Security Essentials GCIH
Secure Web Apps	SEC032 Defending Web Applications Security Essentials GCIH
Secure DevOps	SEC040 Cloud Security and DevOps Automation GCIH
Cloud Security	SEC046 Cloud Security Architecture and Operations GCIH
Cloud Pen Test	SEC068 Cloud Penetration Testing GCIH

MAD20
MITRE ATT&CK®
CYBER THREAT INTELLIGENCE
CERTIFICATION

MAD20 MITRE ATT&CK®
Cyber Threat Intelligence

The MITRE ATT&CK® Cyber Threat Intelligence (CTI) Certification validates a defender's mastery in identifying, developing, analyzing, and applying ATT&CK-mapped intelligence.

Free

MAD20
MITRE ATT&CK®
SECURITY OPERATIONS CENTER ASSESSMENT
CERTIFICATION

MAD20 MITRE ATT&CK®
SOC Assessment

Experts from MITRE produced this course to validate a defender's ability to conduct Security Operations Center (SOC) assessments that are rapid, have low overhead, and are broad enough to help the SOC get on their feet with ATT&CK.

Free

MAD20
MITRE ATT&CK®
ADVERSARY EMULATION NETWORKING
CERTIFICATION

MAD20 MITRE ATT&CK®
Adversary Emulation

Experts from MITRE produced this course to develop a practitioner's ability to conduct adversary emulation activities based on real-world threats. The course takes learners through the exercise of research, planning, TTP implementation, and execution.

Free

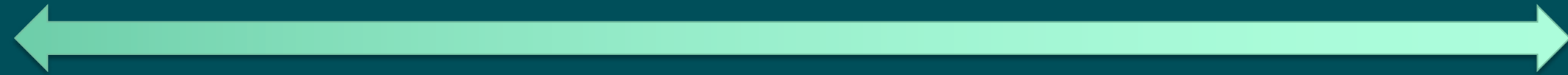
MAD20
MITRE ATT&CK®
THREAT HUNTING & DETECTION
CERTIFICATION

MAD20 MITRE ATT&CK®
Threat Hunting & Detection...

This course teaches learners how to utilize knowledge of adversary TTPs as described in the MITRE ATT&CK framework to develop, test, tune, and employ robust analytics to detect and investigate malicious cyber activity. Learners taking this course will learn how to leverage ATT&CK to develop hypotheses, determine data collection requirements, identify and mitigate collection gaps, test and tune analytics using purple-teaming, and conduct a threat-informed hunt.

Free

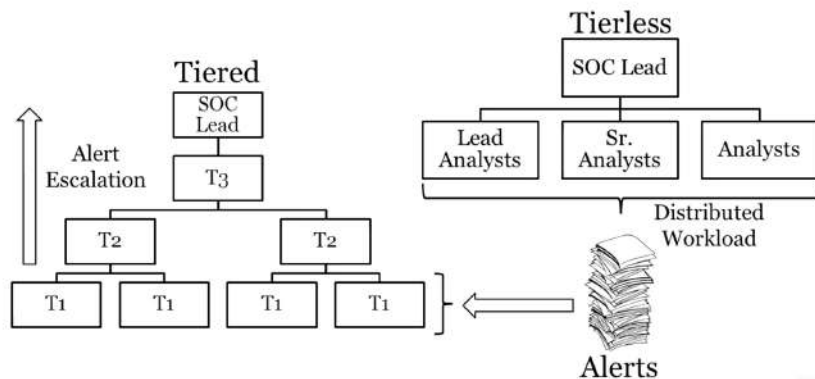
Operational models



In house

Hybrid

Outsourced



Pros

- Repeatable process
- Clear separation of work tasks
- Defined escalation path
- More optimized use of time

Cons

- Limits analysts growth
- Analysts feel more like robots
- Potential retention issues

Pros

- More varied and creative work
- Uncapped analyst talent growth
- Happier analysts

Cons


- Requires a responsible team
- Less defined process
- Can be riskier if expectations are not properly set

MSSP

Users/Endpoints	Common Solution
0 - 1.000	MSSP + non-dedicated internal security team
1.000 – 10.000	MSSP Hybrid with some functions in-house
10.000 – 100.000	Full internal SOC with possible outsourcing of specialty functions
100.000+	Full-fledged internal SOC with auxiliary/specialty services

Public Private collaboration to strengthen our cyber resilience

- Collaboration with regulators, law enforcements, national security agencies leverages on the different expertise and capabilities of each
- Examples: Cyber Security Coalition, AUSTRAC , GASA, ...
- CCB Cyber Fundamentals, BAPS, Safe On Web




Small

The starting level **Small** allows an organisation to make an initial assessment. It is intended for micro-organisations or organisations with limited technical knowledge.

pdf

[Download](#)




Basic

The assurance level **Basic** contains the standard information security measures for all enterprises. These provide an effective security value with technology and processes that are generally already available. Where justified, the measures are tailored and refined.

pdf

[Download](#)




Important

The assurance level **Important** is designed to minimise the risks of targeted cyber-attacks by actors with common skills and resources in addition to known cyber security risks.

pdf

[Download](#)



Essential

The assurance level **Essential** goes one step further and is designed to address the risk of advanced cyber-attacks by actors with extensive skills and resources.

pdf

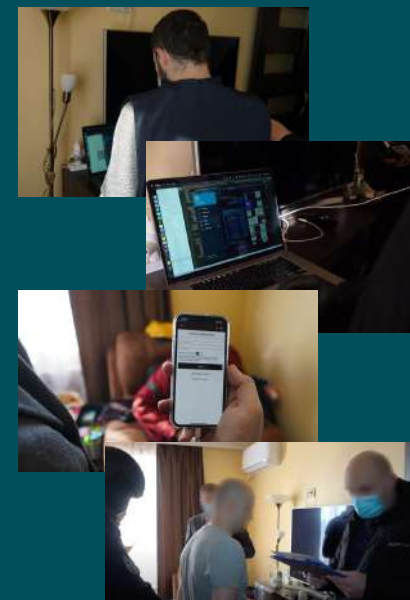
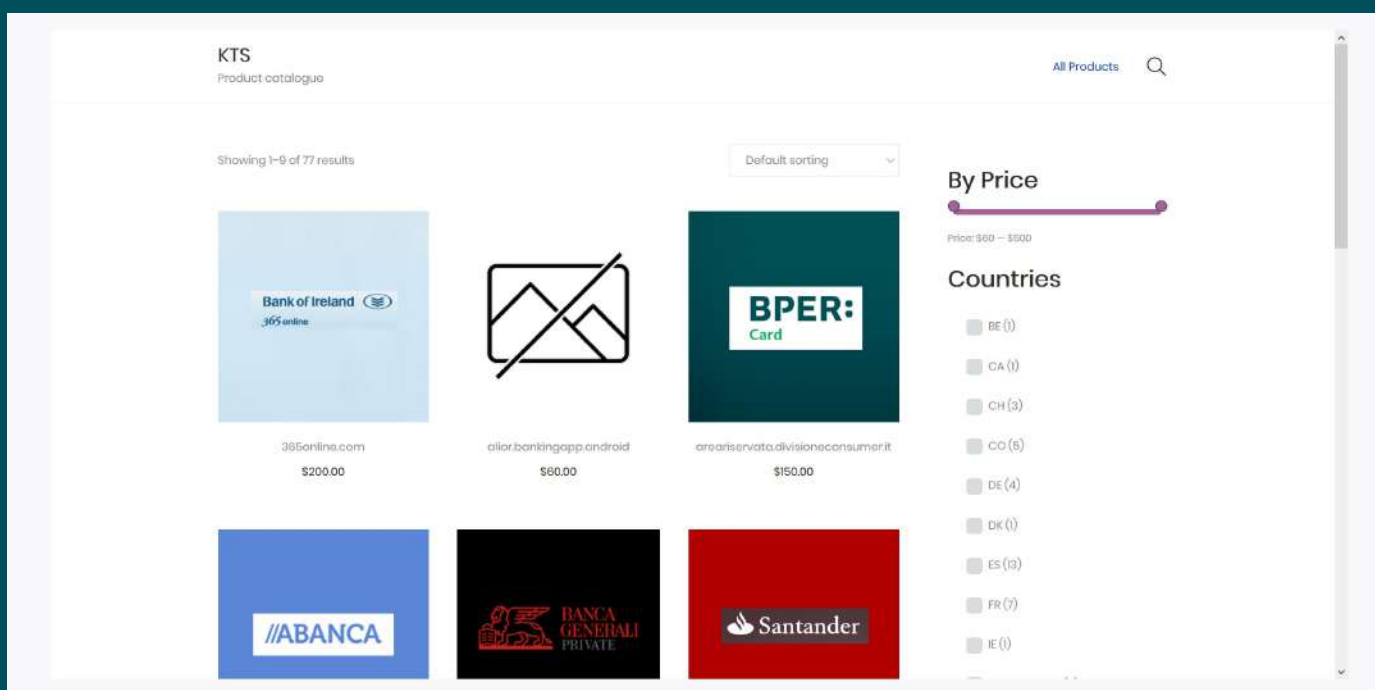
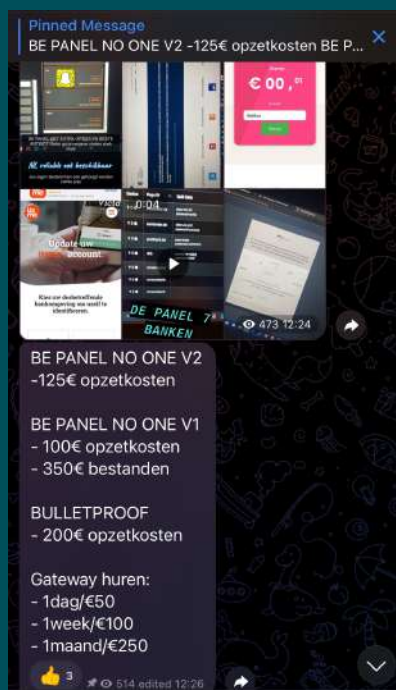
[Download](#)

Some examples from itsme® collaboration

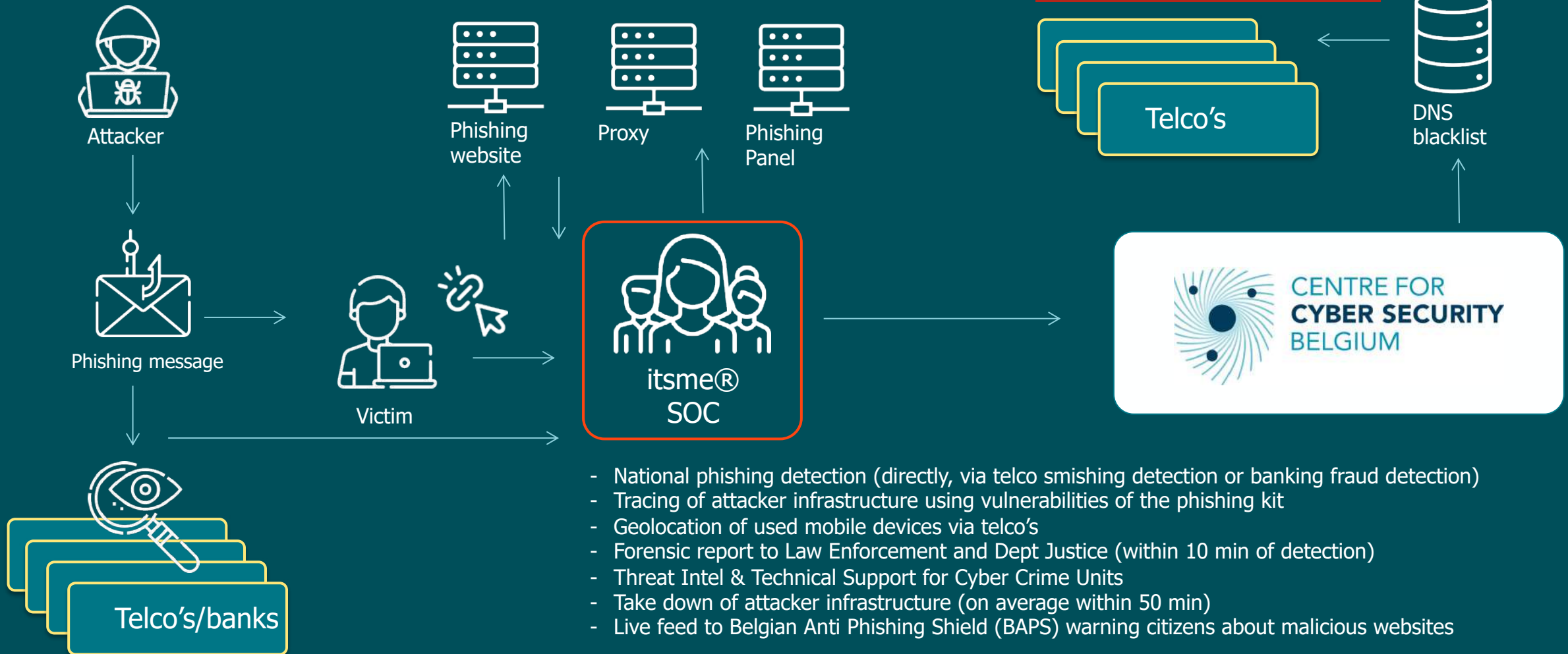
- Phishing
- Risk Warning System

Phishing as a service as one of the main drivers

- ~70% of worldwide phishing campaigns are using the UAdmin phishing kit
- The creator sold his kit via TOR and added bank templates and automated features in 2019 making it very easy to use for non-technical criminals
- Criminals are now renting phishing kit and SMS gateways via Telegram as a service, per day/week/month making it even more easy



Support in Phishing Scenario



New initiative: Risk Warning System

- Objective:
 - National Threat Intel system with indicators for consumer fraud (e.g. MSISDN's/IMEI's used for Smishing, IBAN's of mule accounts)
 - Fast(er) notification and blocking of consumer fraud
- Key stakeholders:
 - National Centre for Cybersecurity (CCB)
 - Belgian Police
 - Banks
 - Telco's
 - Digital ID infrastructure (itsme®)
 - Telco regulator (BIPT)
 - Bank regulator (FSMA)
 - FOD Economie
 - DNS Belgium

Collaboration is key

“It takes a network to fight a network”



Thank you

Remy Knecht
Chief Security Officer
remy.knecht@itsme-id.com



Curriculum lead Security Operations
Solvay Executive Master in Cybersecurity



EU CyberNet
Expert Cyber Defense & Intelligence



Financial Action Task Force
Industry Expert AML/CTF
Co-author Guidance on Digital Identity



Advisor



Founder
Consulting for EU Commission
- Digital Identity
- Cybersecurity



Advisor on Digital Identity Eco-Systems
Co-creator toolkit for governments



CSIRT Focus Group