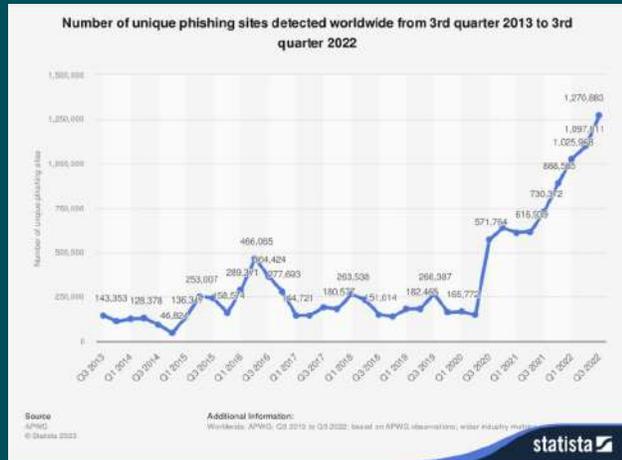




Cyber Security Operations The Frontline of Digital Protection

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!)
- Step increase in consumer fraud

7 Microsoft Digital Defense Report 2023

Executive Summary

The State of Cybercrime

Key developments

Cybercriminals are leveraging the cybercrime-as-a-service ecosystem to launch phishing, identity, and distributed denial of service (DDoS) attacks at scale. Simultaneously, they are increasingly bypassing multifactor authentication and other security measures to conduct targeted attacks.

Ransomware operators are shifting heavily toward hands-on keyboard attacks, using living-off-the-land techniques and remote encryption to conceal their tracks, and exfiltrating data to add pressure to their ransom demands. And cybercriminals are improving their ability to impersonate or compromise legitimate third parties, making it even harder for users to identify fraud until it's too late.

Find out more about The State of Cybercrime in the Microsoft Digital Defense Report 2023

- 80-90% of all successful ransomware compromises originate through unmanaged devices.
- A return on mitigation (ROM) framework is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.
- 70% of organizations encountering human-operated ransomware had fewer than 500 employees.
- Human-operated ransomware attacks are up more than 200%.
- Password based attacks spiked in 2023.
- Last year marked a significant shift in...

8 Microsoft Digital Defense Report 2023

Executive Summary

Nation State Threats

Key developments

After last year's flurry of high-profile cyberattacks, nation-state cyber actors this year pivoted away from high-volume destructive attacks and instead directed the bulk of their activity toward cyber espionage.

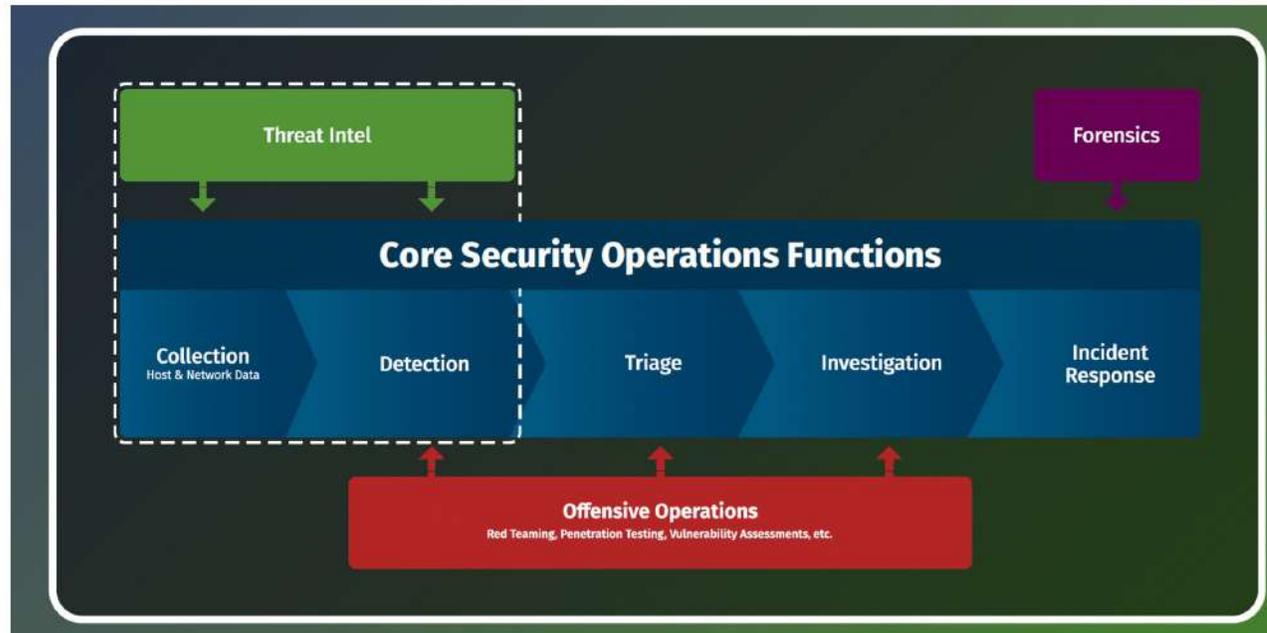
As nation-state threat actors continue to grow in sophistication, they have been increasingly used by governments to understand the plans of other nations, transnational bodies, and non-governmental organizations. Critical infrastructure also remains a popular target, with threat actors employing stealthier techniques to establish persistence and evade detection, as is the education sector. At the same time, some governments have used cyber-enabled influence campaigns to manipulate public opinion at home and abroad. Cyber operations are expanding globally, with increased activity in Latin America, sub-Saharan Africa, and the Middle East due to heightened Iranian activity.

Find out more about The State of Cybercrime in the Microsoft Digital Defense Report 2023

- Nation-state and state-affiliated threat actor activities pivoted away from high volume destructive attacks in favor of espionage campaigns.
- Russian state-sponsored threat actors used diverse means to access devices and networks in NATO member states.
- Chinese cyber threat groups carried out sophisticated worldwide intelligence collection campaigns. At the same time, China's cyber influence campaigns continue to operate at an unmatched scale.
- Iranian state actors are using increasingly sophisticated tradecraft including enhancing operations in cloud environments, regularly using custom implants, and exploiting newly released vulnerabilities faster.
- North Korean actors conducted a supply chain attack using an existing supply chain compromise.
- The unchecked expansion of the cyber mercenary marketplace threatens to destabilize the broader online environment.

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

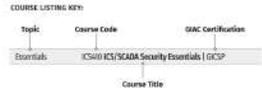
Specialty / Auxiliary Functions:

- **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.



Baseline Skills

New to Cyber Security Concepts, Terms & Skills

Cyber Security Fundamentals | SEC01 Introduction to Cyber Security | GICF

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

Core Techniques

Present, Refresh & Maintain

Every Security Professional Should Know

Security Essentials | SEC01 Security Essentials Bootcamp Style | GCSE

Hacker Techniques and Incident Handling | GCIH

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 | M2112 Security Leadership Essentials for Managers | GICM

Critical | SEC366 Implementing and Auditing the Critical Security Controls - In-Depth | GICC

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 | SEC320 Intrusion Detection In-Depth | GICIA

Monitoring & Operations | SEC321 Continuous Monitoring and Security Operations | GIMOR

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 | SEC360 Network Penetration Testing and Ethical Hacking | GPNP

Web Apps | SEC362 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

Evident Forensics | FOR500 Wireless Forensic Analysis | GCFE

Digital Forensics | FOR508 Advanced Incident Response, Threat Hunting, and Digital Forensics | GCIIR

Network Forensics | FOR527 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | GICAN

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.

CISSP Training | MGI14 SANS Training Program for CISSP Certification | GICSP

Crucial Skills, Specialized Roles

You are a candidate for advanced or specialized training

Cyber Defense Operations	Harder Specifics/Deeper
Specialized Defensive Area	
Blue Team	SEC640 Blue Team Fundamentals: Security Operations and Analysis
OSINT	SEC640 Open-Source Intelligence (OSINT) Gathering & Analysis GOSI
Advanced Generalist	SEC601 Advanced Security Essentials - Enterprise Defender GCE0
Windows/PowerShell	SEC645 Securing Windows and PowerShell Automation GCMW
Linux/Unix Defense	SEC646 Securing Linux/Unix GCLX
SER	SEC655 SIEM with Tactical Analytics GCSA
Other Advanced Defense Courses	
Security Architecture	SEC320 Defensible Security Architecture and Engineering GCSA
Adversary Emulation	SEC390 Dealing with Advanced Adversaries - Purple Team Tactics and IR Chain Defenses GDAE

Specialized Penetration Testing	Recent Techniques & Areas
In-Depth Coverage	
Vulnerability Assessment	SEC640 Enterprise and Cloud Threat and Vulnerability Assessment GCTVA
Networks	SEC640 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking GAPP
Web Apps	SEC642 Advanced Web App Testing, Ethical Hacking, and Exploitation Techniques
Mobile	SEC625 Mobile Device Security and Ethical Hacking GMDR
Cloud	SEC638 Cloud Penetration Testing and Ethical Hacking GICAN
Wireless	SEC627 Wireless Penetration Testing and Ethical Hacking GICAN
Python Coding	SEC323 Automating Information Security with Python GPCIC
Adversary Emulation	SEC390 Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection

Digital Forensics, Malware Analysis & Threat Intel	Specialized Investigative Skills
Essentials	
SFR Essentials	FOR508 Digital Forensics Essentials
Malware Analysis	FOR500 Reverse-Engineering Malware: Malware Analysis Tools and Techniques GICSP
Malware Analysis	FOR500 Reverse-Engineering Malware: Malware Analysis Tools and Techniques GICSP
Threat Intelligence	FOR528 Cyber Threat Intelligence GCTI
Cyber Threat Intelligence	FOR528 Cyber Threat Intelligence GCTI
Ransomware Forensics & Data Acquisition	FOR540 Ransomware Forensics & Data Acquisition GRRR
Smartphone Analysis	FOR525 Smartphone Forensic Analysis in Depth GSP
Memory Forensics	FOR526 Advanced Memory Forensics & Threat Detection
Mac Forensics	FOR529 Mac and iOS Forensic Analysis and Incident Response

Advanced Management	Advanced Leadership, Audit & Legal
Management Skills	
Planning, Policy, Leadership	MCI204 Security Strategy, Planning, Policy, and Leadership GCTMT
Managing Vulnerabilities	MCI206 Managing Security Vulnerabilities, Enterprise and Cloud
Project Management	MCI205 IT Project Management, Effective Communication, and PMIP® Exam Prep GCPM
Audit & Legal	
Audit & Monitor	AUD507 Auditing and Monitoring Networks, Protocols & Systems GCMN
Law & Investigations	LEG520 Law of Data Security and Investigations GILG

65+ hands-on courses

35+ certifications

To learn more about additional SANS courses, go to sans.org/courses

See in-depth course descriptions and the digital version of this roadmap at sans.org/roadmap

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

Industrial Control Systems
Every ICS Security Professional Should Know
Essentials IC540 ICS/SCADA Security Essentials GICSP
ICS Defense & Response
ICS Defense & Response IC520 ICS Active Defense and Incident Response GIDR
ICS Advanced Security
ICS Advanced Security IC502 ICS Cybersecurity In-Depth
NERC Protection
NERC Security Essentials IC540 Essentials for NERC Critical Infrastructure Protection GICP

Cloud Security
Every Cloud Security Ops Person Should Know
Essentials SEC638 Cloud Security Essentials
Secure Web Apps
Secure Web Apps SEC322 Defending Web Applications Security Essentials GAWB
Secure DevOps
Secure DevOps SEC340 Cloud Security and DevOps Automation GCSA
Cloud Security
Cloud Security SEC345 Cloud Security Architecture and Operations
Cloud Pen Test
SEC388 Cloud Penetration Testing

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 WITH SOC2000 CERTIFICATION

MAD20 MITRE ATT&CK® Adversary Emulation

Experts from MITRE produced this course to validate 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

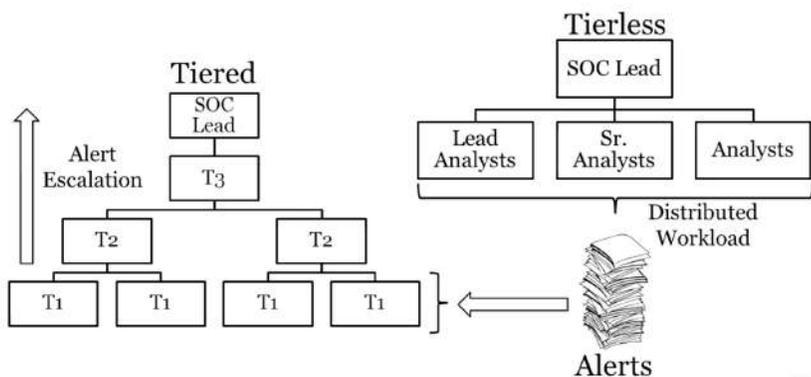
Operational models



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

The screenshot displays four assurance levels for Cyber Fundamentals, each with a thumbnail image, a description, a PDF icon, and a download button.

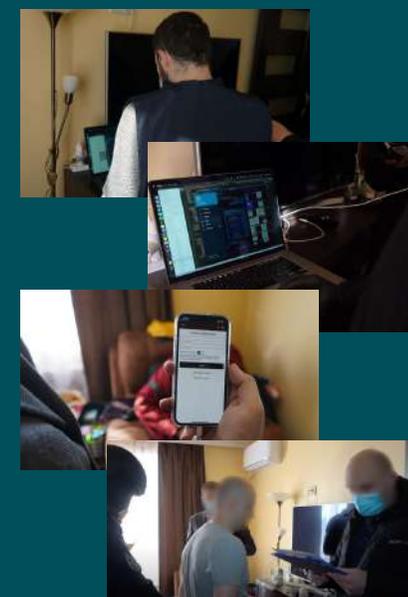
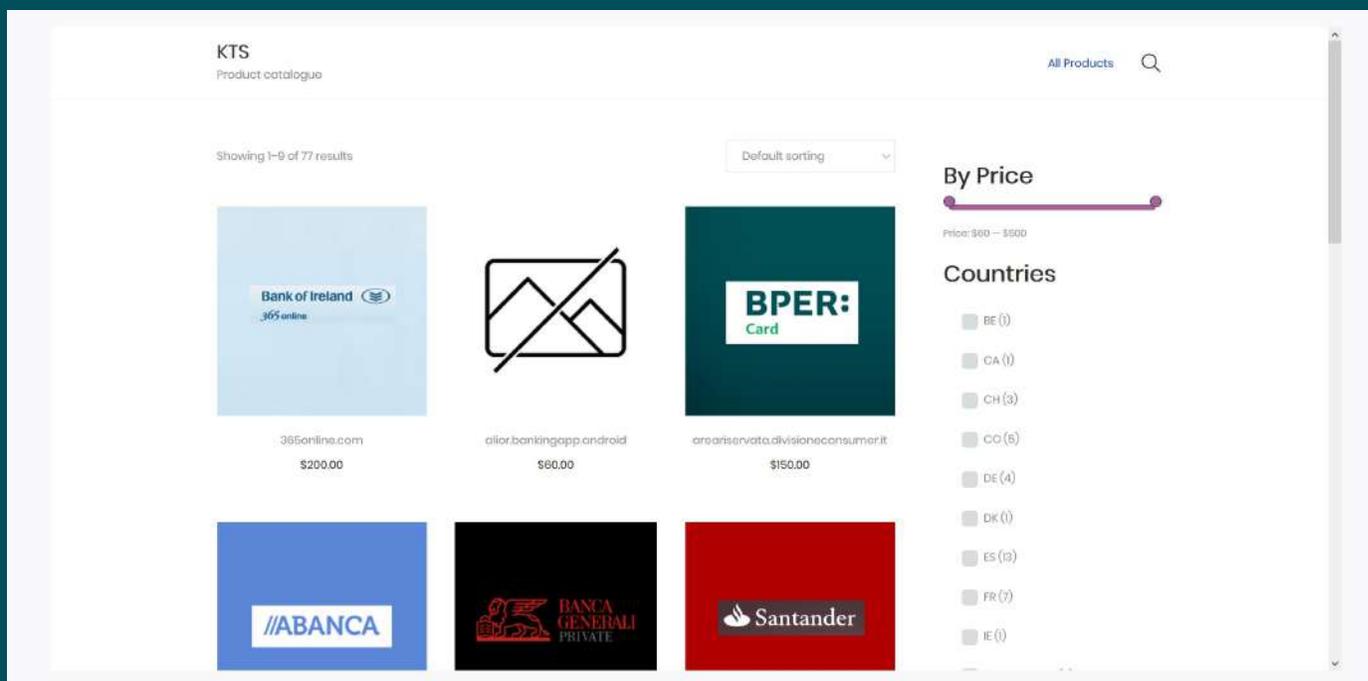
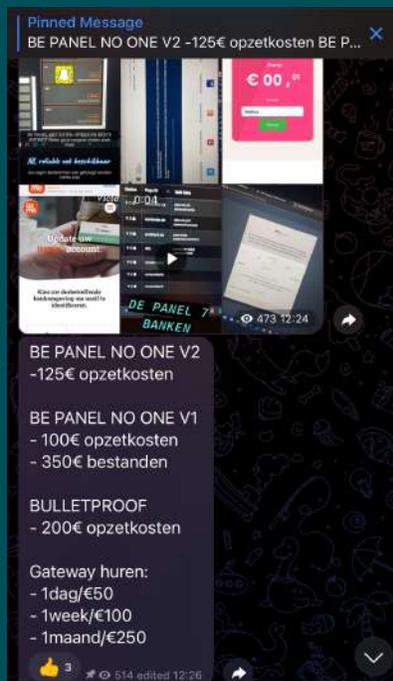
- Small**: The starting level **Small** allows an organisation to make an initial assessment. It is intended for micro-organisations or organisations with limited technical knowledge.
- Basic**: The assurance level **Basic** contains the standard information security measures for all enterprises. These provide an effective security value with technology and processes that are generally already available. Where justified, the measures are tailored and refined.
- 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.
- 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.

Some examples from itsme® collaboration

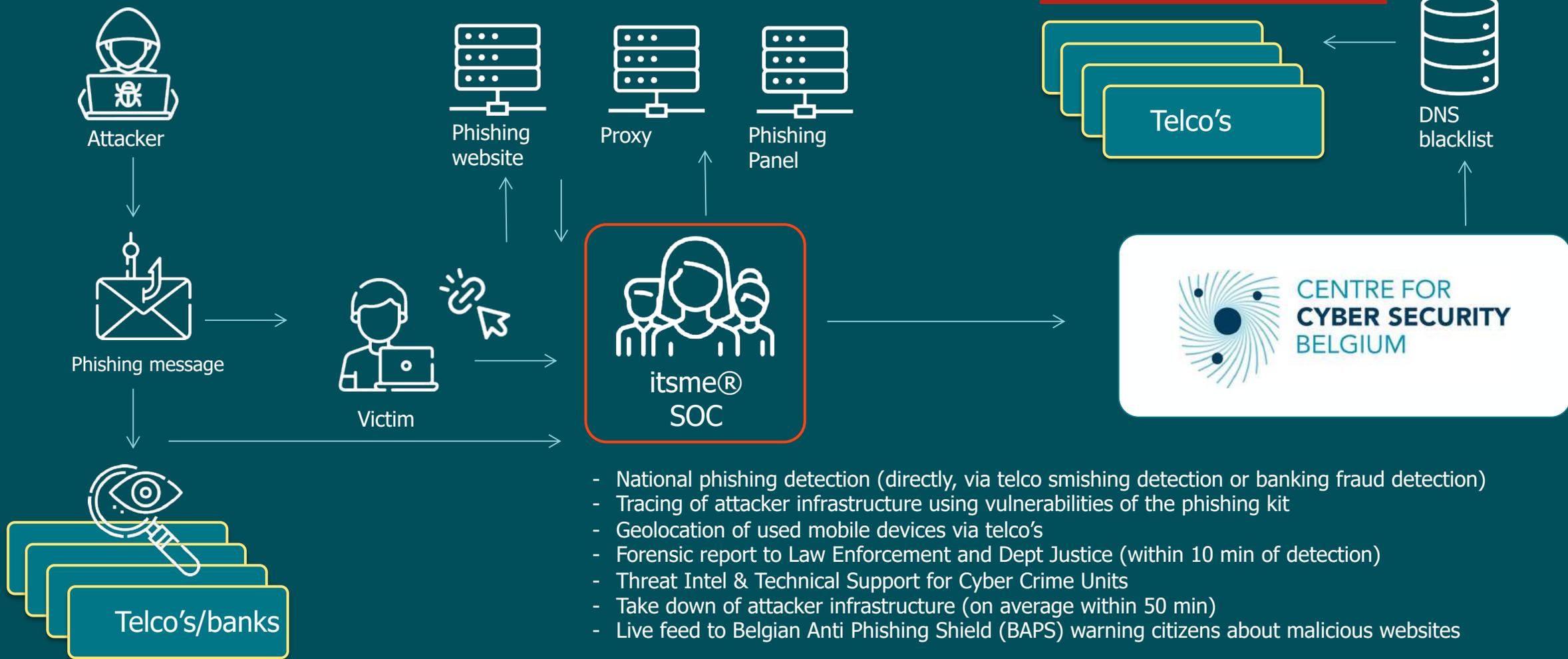
- Phishing
- Risk Warning System

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



- National phishing detection (directly, via telco smishing detection or banking fraud detection)
- Tracing of attacker infrastructure using vulnerabilities of the phishing kit
- Geolocation of used mobile devices via telco's
- Forensic report to Law Enforcement and Dept Justice (within 10 min of detection)
- Threat Intel & Technical Support for Cyber Crime Units
- Take down of attacker infrastructure (on average within 50 min)
- Live feed to Belgian Anti Phishing Shield (BAPS) warning citizens about malicious websites

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