



Tax and Customs Administration

TLP:CLEAR





Security Operations Center

2022-12-13

Security Operations Center



Traffic Light Protocol

Assignment	Description	TLP tag example
RED	Information is exchanged on a personal, confidential basis. Further dissemination is not permitted and the information will not be stored.	<div>TLP:RED</div> 
AMBER	The information may only be shared with colleagues within one's own organization on a need-to-know basis and with customers who need to receive this information so that they can protect themselves or prevent further damage with it. The sender may place a restriction on the dissemination of the information. The restriction must be included in the TLP:AMBER coding.	<div>TLP:AMBER</div>  With restriction: <div>TLP:AMBER - STRICT</div>
GREEN	The information is not public but may be freely shared within the work environment. However, the information may not be published.	<div>TLP:GREEN</div> 
CLEAR	Free distribution allowed, of course taking into account e.g. copyright.	<div>TLP:CLEAR</div> 



\$ whoami

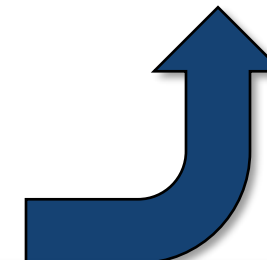
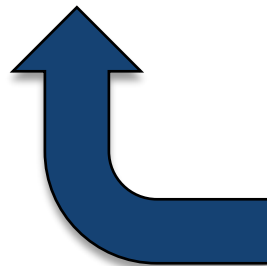


Karl Lovink
Technical Lead SOC
Dutch Tax and Customs
Administration

kw.lovink@belastingdienst.nl



- Technical Lead SOC Belastingdienst
- Mentor DEF CON Blue Team Village
- Chair anti-DDoS Coalition – WG Exercises
- Liaison NCSC
- 18 Security Analysts
- Started in June 2010



Who do we work for?



Berichtenbox

In de Berichtenbox ontvangt u berichten van de overheid.

→ Naar de Berichtenbox



- Ⓢ Citizens and companies.
- Ⓢ Customers within the service.
- Ⓢ Customers outside the service.

"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012



IV – Facts and Figures



24 Petabyte
storage



> 2.000 Physical
> 2.150 Virtual



3 locations



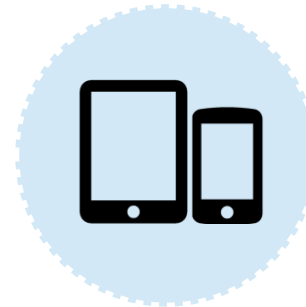
43.000
notebooks/pc



1.600
applications



30 million LoC



> 50.000 mobile
devices

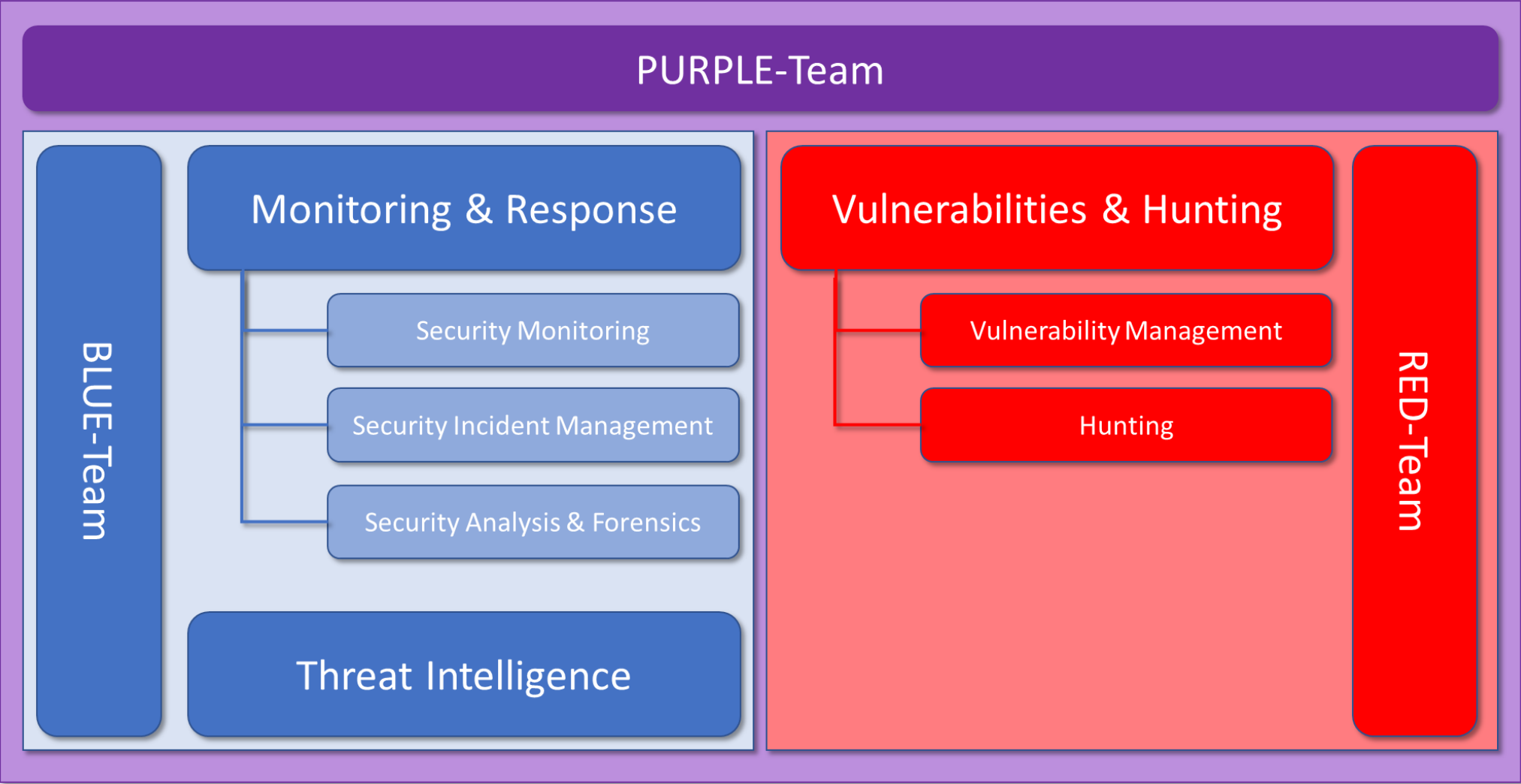


> 300 apps

Definition Security Operations Center

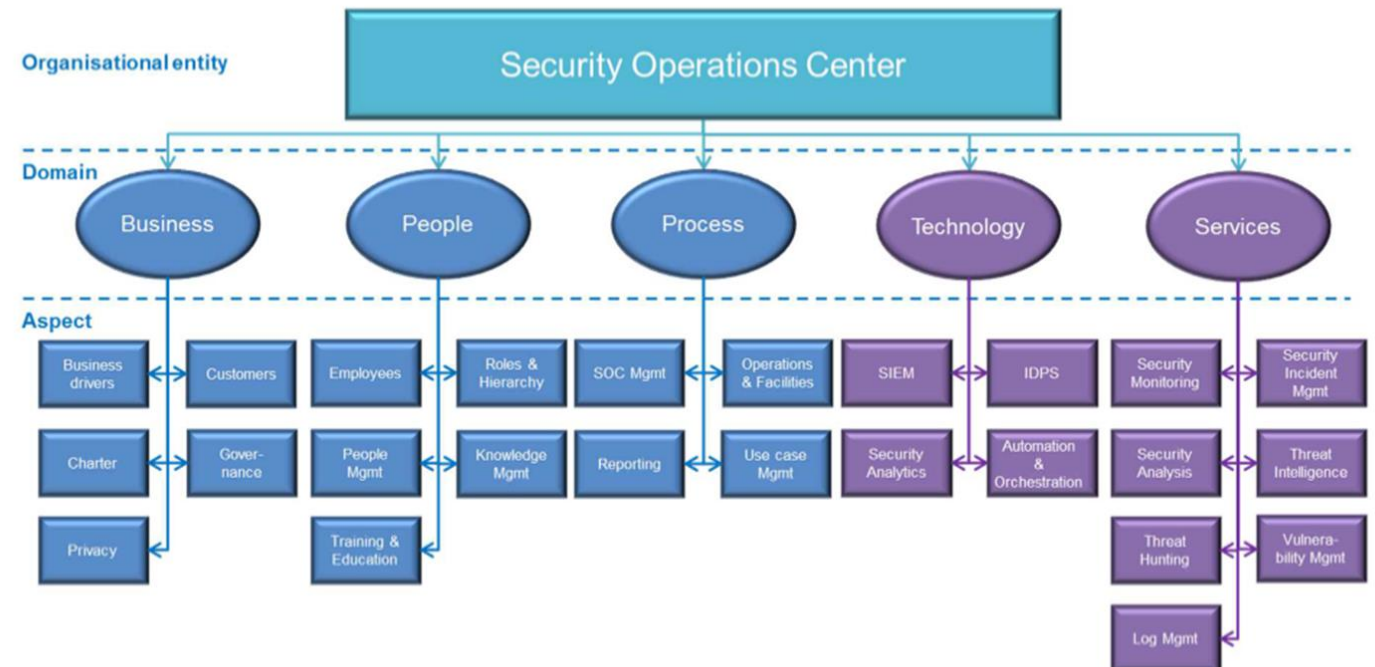
“A Security Operation Center (SOC) is a centralized function within an organization employing **people, processes, and technology** to continuously monitor and improve an organization's security posture while **preventing, detecting, analyzing, and responding** to cybersecurity incidents.”

Main processes SOC

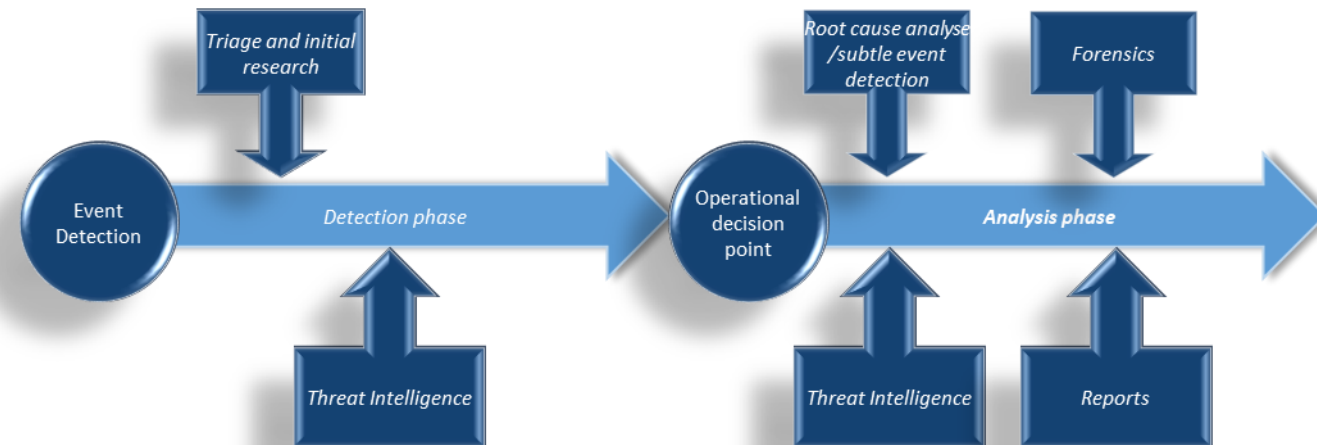
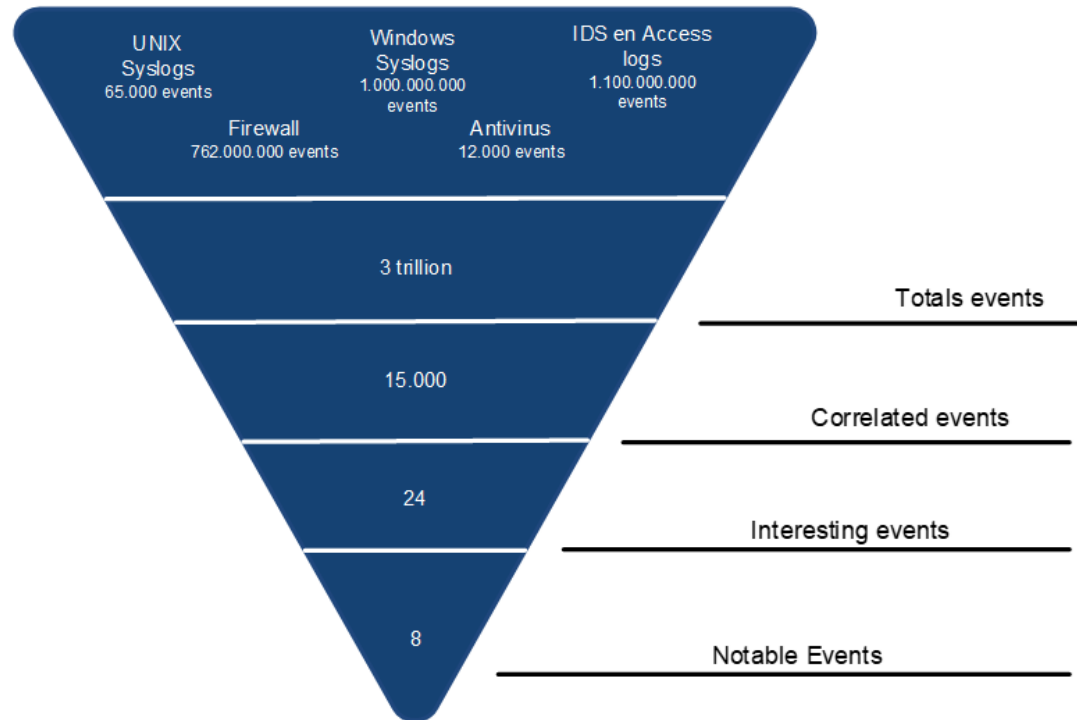


Main processes SOC

- ④ SOC-CMM services mapping to SOC processes.
- ④ Making it measurable.
- ④ Mapping to NIST Cyber Security Framework.
- ④ More on SOC-CMM at the end of this talk.



Challenge Security Monitoring: from events to incidents



Monitoring & Response - Scope

The SOC deals with Security Monitoring, examples of which are :

- ① unauthorized account creation in the domain “Belastingdienst”;
- ① use of honey token account.

Examples not covered by security monitoring:

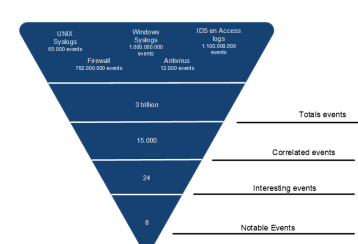
- ① an unexpected restart;
- ① unexpected restoration of a backup;
- ① availability of an application;
- ① abnormalities in behavior.

Monitoring & Response – Use-cases

What is a SOC use-case?

“Methodology used by the SOC team to identify and organize technical and organizational requirements for detection and response to specific threats”

From 4 Terabytes per day to less than 25 incidents.....



Monitoring & Response - Use-case examples

- ④ Inside to inside:
 - ④ unauthorized creation of users;
 - ④ use of "honey token accounts".
- ④ Outside to inside:
 - ④ DDoS detection;
 - ④ inbound malware;
 - ④ hacking attempts, exploiting vulnerabilities, Coordinated Vulnerability Disclosure.
- ④ Inside to outside:
 - ④ detection of network traffic to botnets, malware workstations.
- ④ Outside to outside:
 - ④ reports from citizens about Phishing/Smishing.

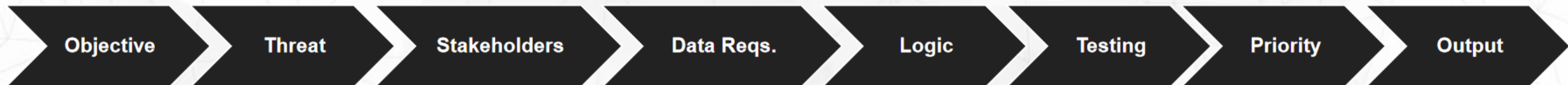
Use-case Framework

🕒 Objective:

- 🕒 why is the creation of this use case adding value to the business and what will it accomplish? Insight for managers on current detection capabilities.

🕒 Threat:

- 🕒 what threats and security risks do we want to protect ourselves against?
- 🕒 linking to the MITRE ATT@CK framework. Possibility of additional classifications, for example Digid, BIR;
- 🕒 gives a background as to why the use-case is being drawn up.



Source: SANS DFIR Summit Prague 2016 - RSA

MITRE Att@ck Matrix for Enterprises

example x +

ATT&CK™ Navigator ?

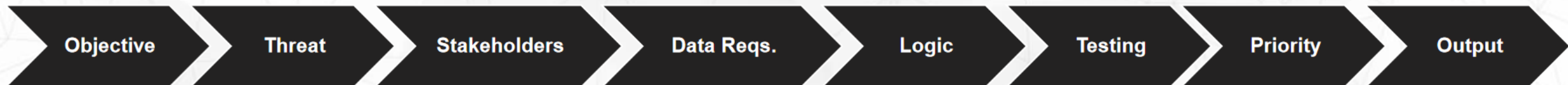
selection controls layer controls technique controls

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command And Control
51 items	27 items	49 items	18 items	17 items	17 items	25 items	13 items	9 items	19 items
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Data Compressed	Communication Through Removable Media
AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Browser Extensions	Data Encrypted	Connection Proxy
AppInit DLLs	AppInit DLLs	Clear Command History	Credential Dumping	Network Service Scanning	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Application Shimming	Application Shimming	Code Signing	Credentials in Files	Network Share Discovery	Logon Scripts	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Authentication Package	Bypass User Account Control	Component Firmware	Exploitation of Vulnerability	Peripheral Device Discovery	Pass the Hash	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Bootkit	DLL Search Order Hijacking	Component Object Model Hijacking	Forced Authentication	Hooking	Pass the Ticket	InstallUtil	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Browser Extensions	Dylib Hijacking	Deobfuscate/Decode Files or Information	Input Capture	Permission Groups Discovery	Remote Desktop Protocol	Local Job Scheduling	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Change Default File Association	Exploitation of Vulnerability	Disabling Security Tools	Input Prompt	Process Discovery	LSASS Driver	LSASS Driver	Email Collection	Scheduled Transfer	Fallback Channels
Component Firmware	Extra Window Memory Injection	DLL Search Order Hijacking	Keychain	Query Registry	Remote File Copy	Mshhta	Input Capture	Man in the Browser	Multi-hop Proxy
Component Object Model Hijacking	File System Permissions Weakness	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Remote System Discovery	Remote Services	PowerShell	Screen Capture	Scheduled Transfer	Multi-Stage Channels
Create Account	Hooking	Exploitation of Vulnerability	Network Sniffing	Security Software Discovery	Replication Through Removable Media	Regsvcs/Regasm	Video Capture		Multiband Communication
DLL Search Order Hijacking	Image File Execution Options Injection	Extra Window Memory Injection	Password Filter DLL	System Information Discovery	Shared Webroot	Regsvr32			Multilayer Encryption
Dylib Hijacking	Launch Daemon	File System Logical Offsets	Private Keys	System Network Configuration Discovery	SSH Hijacking	Rundll32			Remote File Copy
External Remote Services	New Service	Gatekeeper Bypass	Replication Through Removable Media	System Network Connections Discovery	Taint Shared Content	Scheduled Task			Standard Application Layer Protocol
File System Permissions Weakness	Path Interception	Hidden Files and Directories	Securityd Memory	System Owner/User Discovery	Third-party Software	Scripting			Standard Cryptographic Protocol
Hidden Files and Directories	Plist Modification	Hidden Users	Two-Factor Authentication Interception	System Service Discovery	Windows Admin Shares	Service Execution			Standard Non-Application Layer Protocol
Hooking	Port Monitors	HISTCONTROL			Windows Remote Management	Source			Uncommonly Used Port
Hypervisor	Process Injection	Image File Execution Options Injection				Space after Filename			Web Service
Image File Execution Options Injection	Scheduled Task	Indicator Blocking				Third-party Software			
Launch Agent	Service Registry	Indicator Removal from Tools				Trap			
Launch Daemon	Permissions Weakness	Indicator Removal on Host				Trusted Developer Utilities			
Launchctl	Setuid and Setgid	Install Root Certificate				Windows Management Instrumentation			
LC_LOAD_DYLIB Addition	SID-History Injection	InstallUtil				Windows Remote Management			
Local Job Scheduling									

Use-case Framework

- ④ Stakeholders:
 - ④ mapping stakeholders; are not necessarily the owners of the use case;
 - ④ examples are HR, security officers etc;
 - ④ format by stakeholder matrix.

- ④ Data Requirements:
 - ④ what raw log/packet/flow/endpoint data sources are required for the use case;
 - ④ requirements for high and low level data.



Source: SANS DFIR Summit Prague 2016 - RSA

Use-case Framework

- ④ Logic:
 - ④ here the source data is displayed to give an understanding of how the use case is structured;
 - ④ configure tools, screenshots to clarify aspects.
- ④ Testing:
 - ④ verification phase whether the use-case generates the right hits with reliable alerting;
 - ④ possibility to perform tests based on scenarios.



Source: SANS DFIR Summit Prague 2016 - RSA

Use-case Framework

- ④ Priority:
 - ④ prioritizing the use case to determine urgency and impact;
 - ④ collaboration with customer and SOC;
 - ④ based on policy and business requirements;
 - ④ remains an ongoing process, requires good collaboration between the SOC and customer.

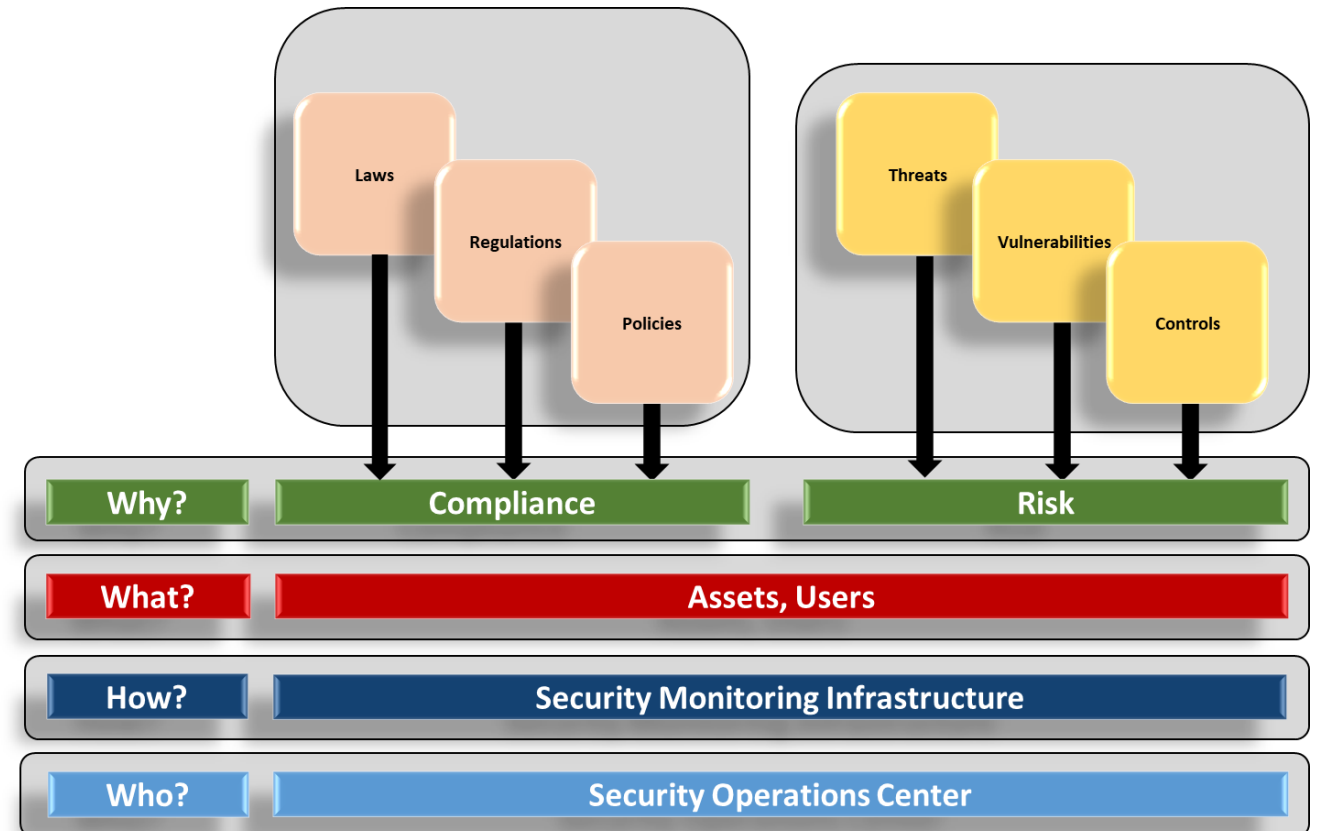
- ④ Output:
 - ④ final events generated, dashboards, workflow actions, incident review, response plans etc.



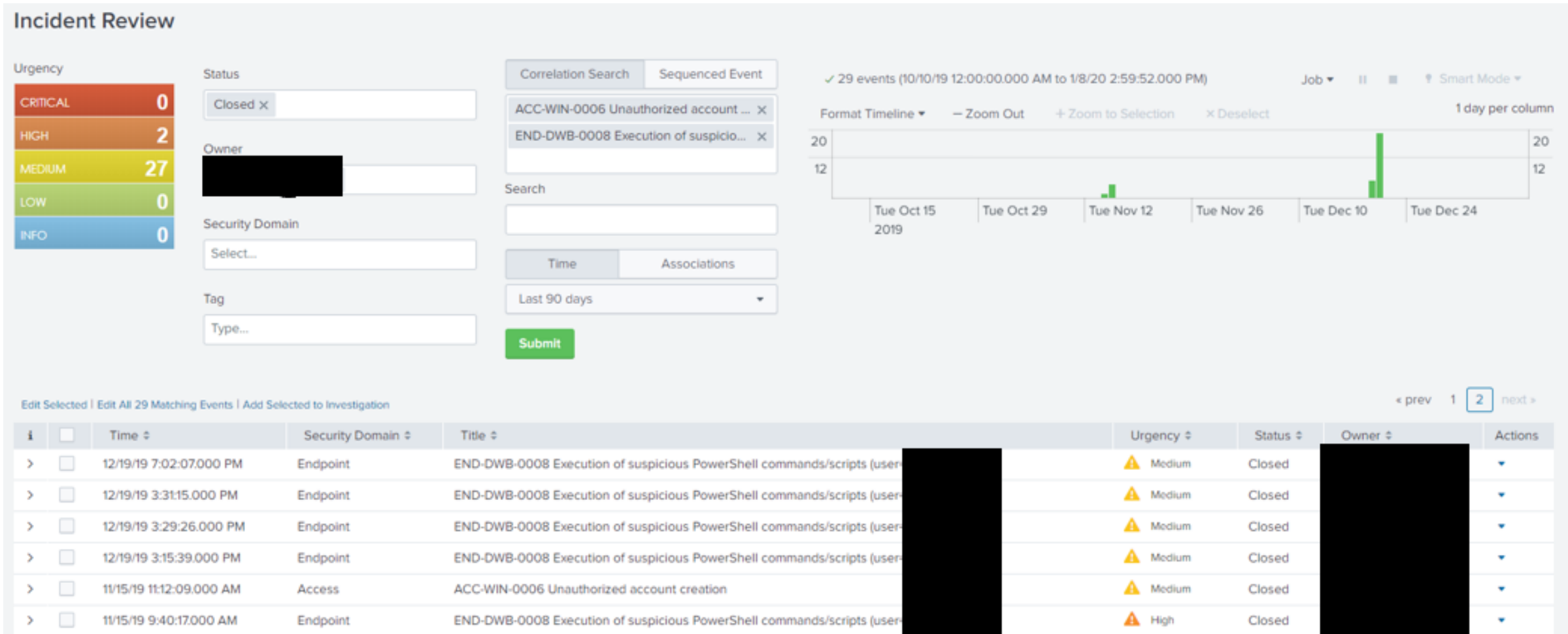
Source: SANS DFIR Summit Prague 2016 - RSA

MAGMA Use-case Framework





- ① The MaGMA Use Case Framework (UCF) is a framework and tool for use case management and administration on security monitoring
- ② Now: Use-case: bottom-up
- ③ Future: Risks/Compliance: top-down



Security Incident and Event Management system



Outside to inside: DDoS detection

Rulebase & Screening	Rulebase     1m ago	Screening	Amplification Type	Src IP session Limits	Dest IP session Limits
331609 IP's	72684 Unieke IP's	240 Unieke IP's	317831 UDP packets	0 Hits Src IP session Limits	47 Hits Dest IP session Limits
4 % IP's from NL	8 % IP's from NL	0 % IP's from NL	UDP/DNS (79%) #1 Attack UDP	— #1 IP	101.178.237.246 #1 IP
96 % IP's from other Country's	92 % IP's from other Country's	0 % IP's from other Country's	TCP/53169 (2%) #1 Attack NON UDP		
Russia(25%) #1 Non NL Country	United States(25%) #1 Non NL Country	Russia #1 Non NL Country	Russia #1 Non NL Country	— #1 Non NL Country	Australia #1 Non NL Country

Outside to Inside - RED-/BLUE-TEAM DDoS Exercise

- Twice a year:
 - volume-based DDoS test;
 - applicative DDoS test.



Belastingdienst

UNIVERSITY
OF TWENTE.



EQUINIX



Rijkswaterstaat
Ministerie van Infrastructuur en Milieu



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*



Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie



Ministerie van Defensie



Nationale Beheersorganisatie Internet Providers

de volksbank

Outside to inside - DDoS Exercise - Preparation

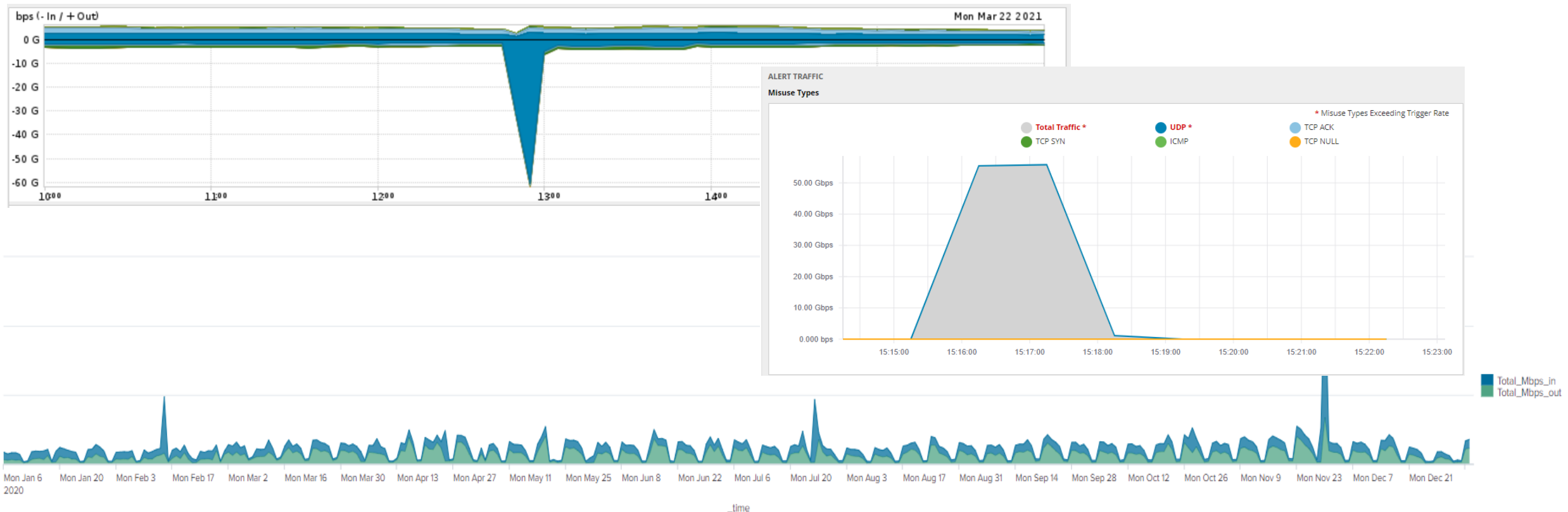
- ④ Set targets and inform customers.
- ④ RED/BLUE-team exercise.
- ④ Roles: RED-team, BLUE-team, Observers, Game Leaders
- ④ Peering mapping and configuring (routing over the
 - ④ Internet).
- ④ Prepare indemnification statements.
- ④ Arrange catering.
- ④ Communication to providers and internet nodes
 - ④ (AMS-ix and NL-ix).
- ④ Gameboard and Test Bed (PURPLE-Teaming).



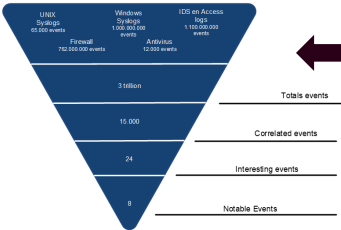
Always expect the unexpected (things can always happen that were not foreseen).

Outside to inside - DDoS attacks 2020/2021/2022

- 4 major DDoS numbers (February, July and November 2020, March 2021)
- Dependency external parties for example: DNS Providers
- Two months and continuing of PSRD DNS dictionary attacks

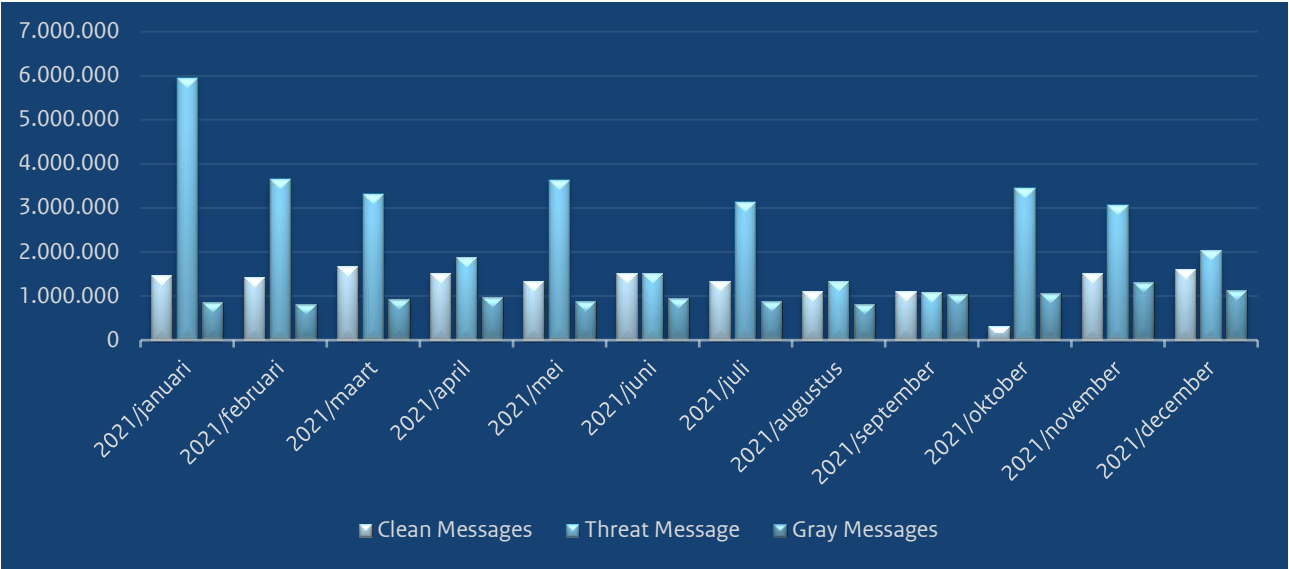


Outside to Inside - External Mail

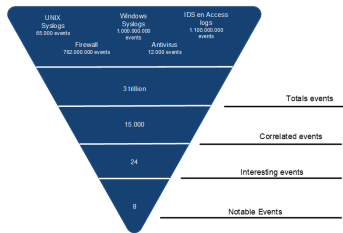


Totals 2021

Threat Messages	34.010.631	55,21%
Gray Messages	11.66.683	18,94%
Clean Messages	15.928.775	25,86%
Total	61.607.089	100.00%

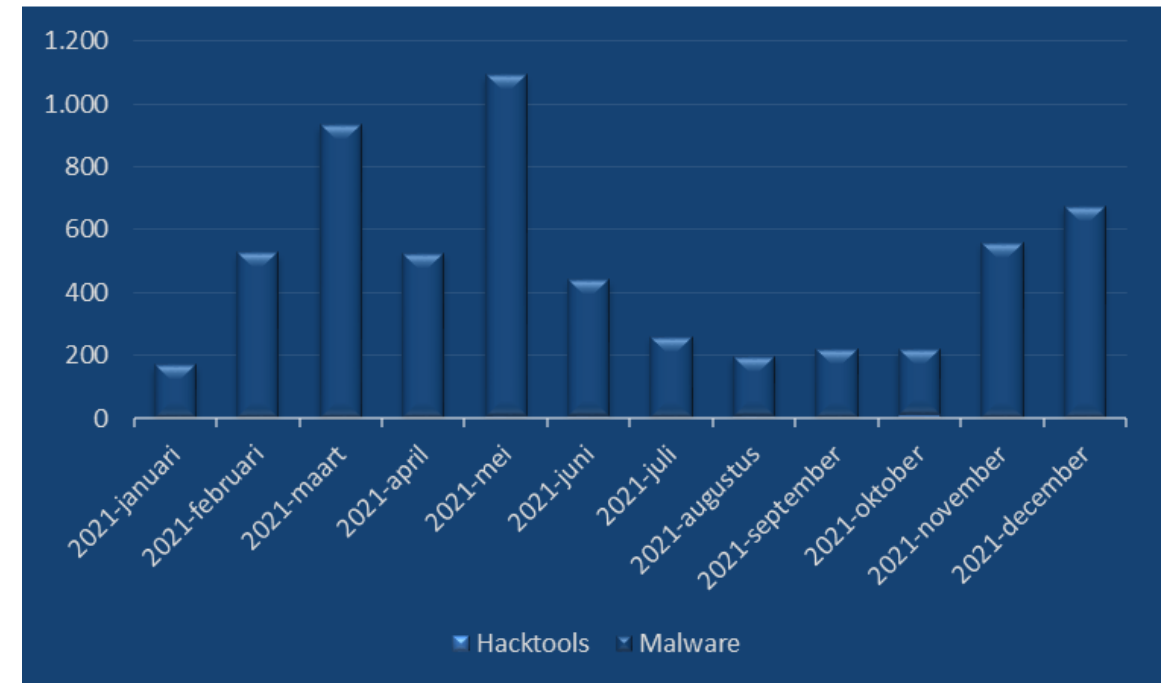


Inside to outside/inside - Malware workstations



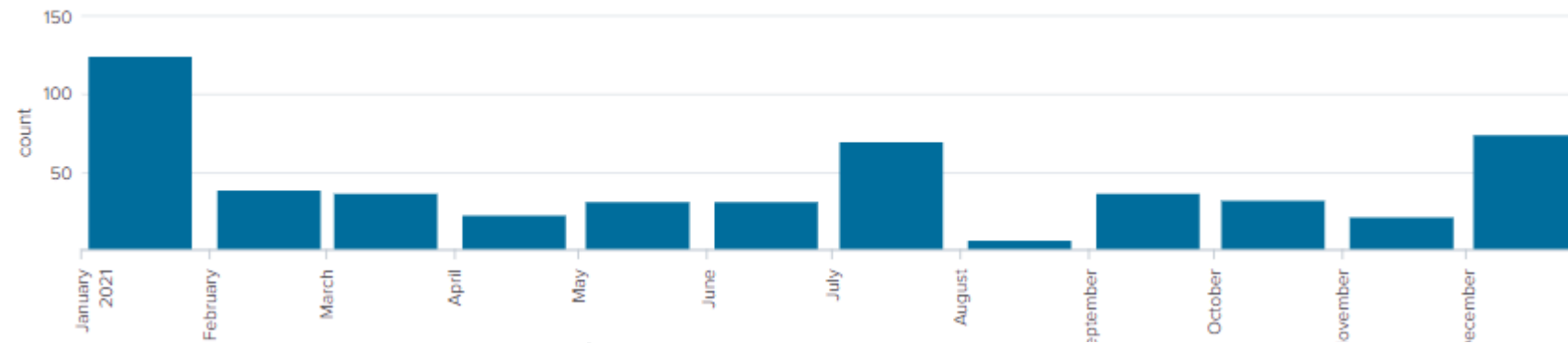
Totals 2021

- Malware 5799
- Hacktools 29

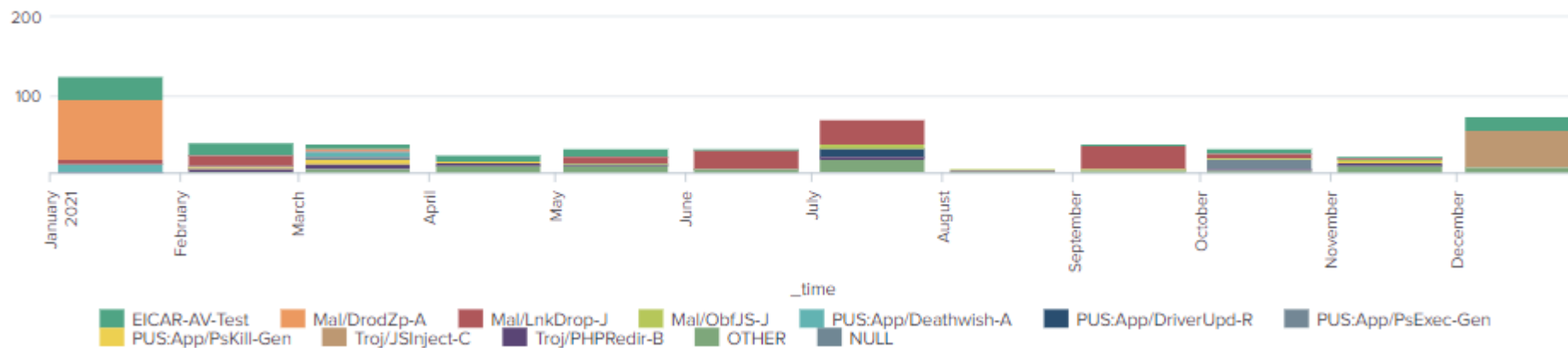


Inside to outside - Proxy servers

Viruses found - last year

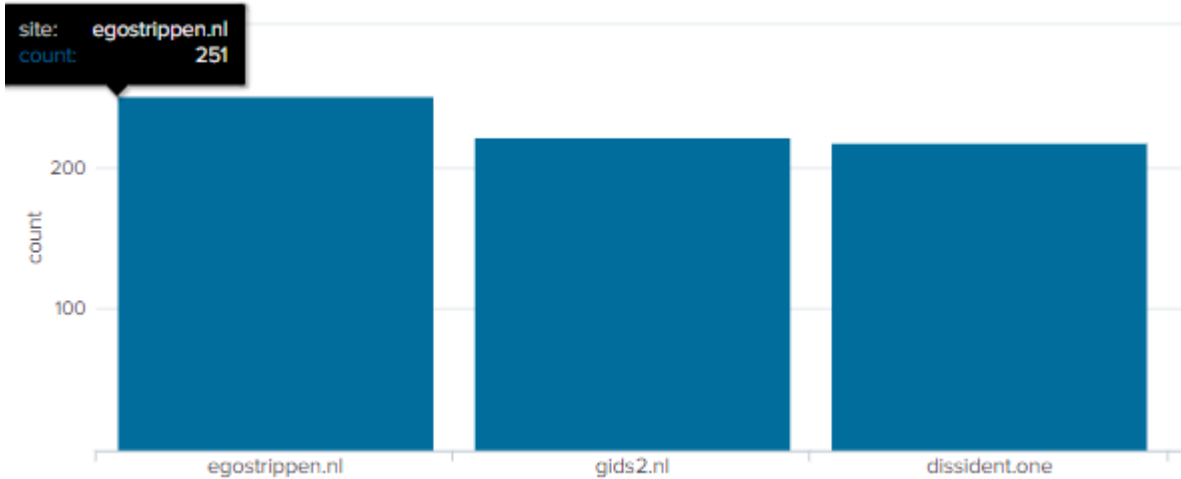



Viruses found-Last - last year



Inside to outside - Proxy servers

Category: Malicious Sources/Malnets





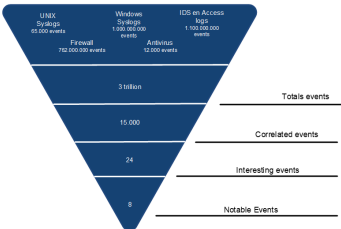
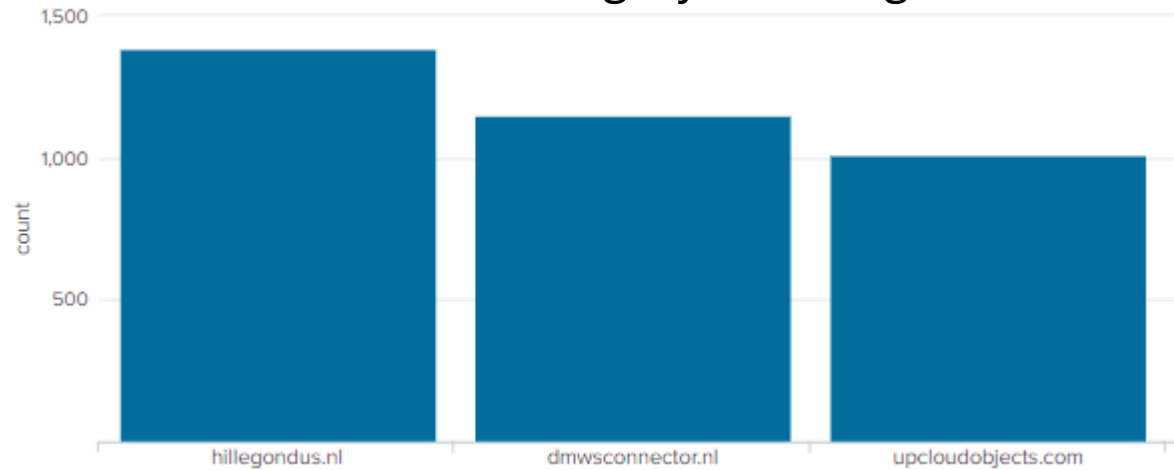
Deceptive site ahead

Attackers on **unanalytics.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers or credit cards). [Learn more](#)

☐ Automatically send some system information and page content to Google to help detect dangerous apps and sites. [Privacy Policy](#)

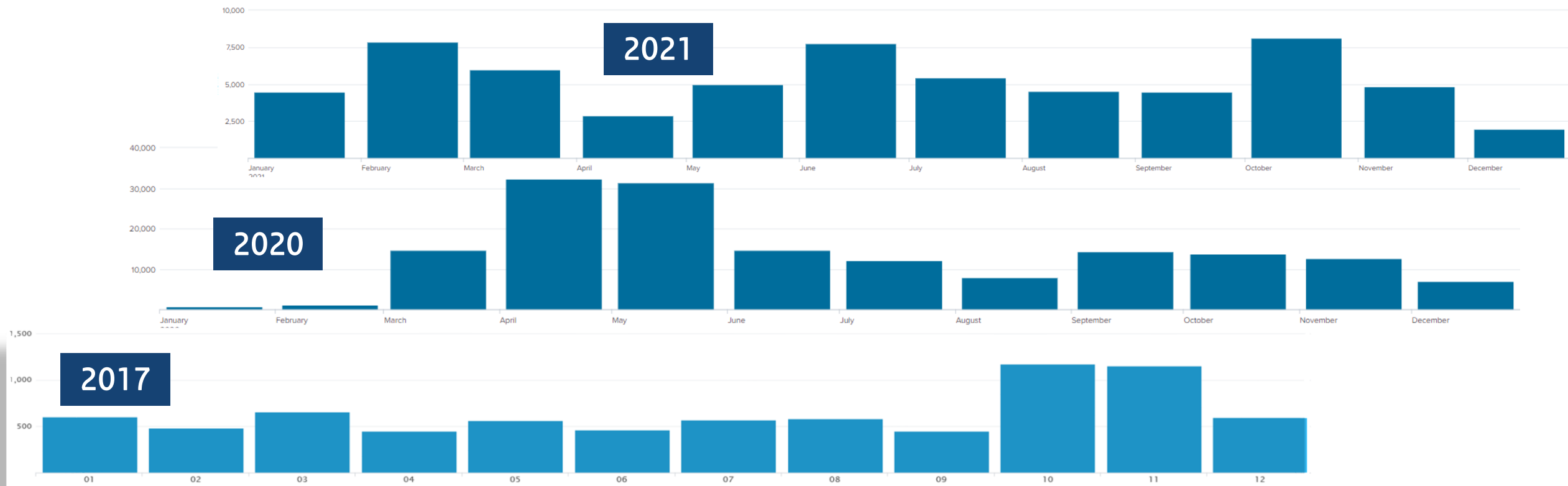
[DETAILS](#)[Back to safety](#)

Category: Phishing

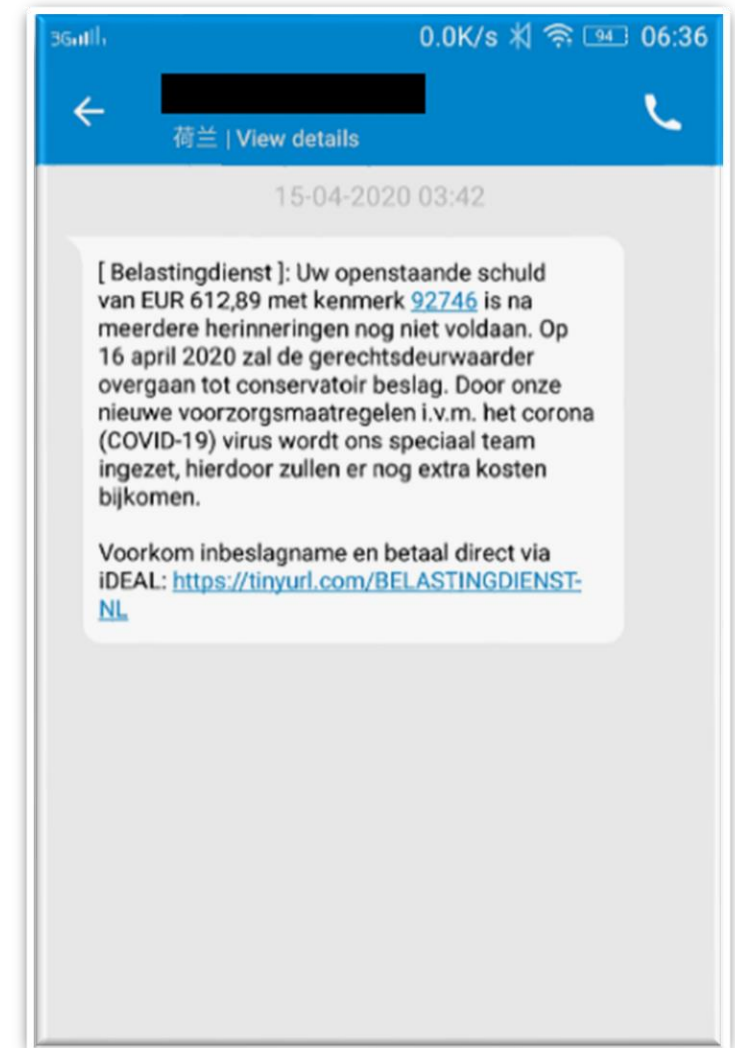
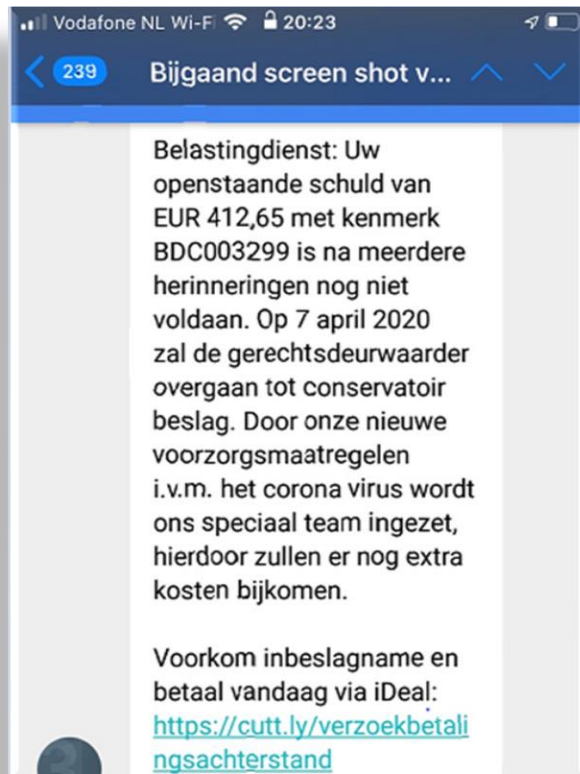


Outside to outside - Phishing, SMishing, and SPAM

# e-mails received	2017	2020	2021
valse-email@belastingdienst.nl	7.791	162.624	63.200

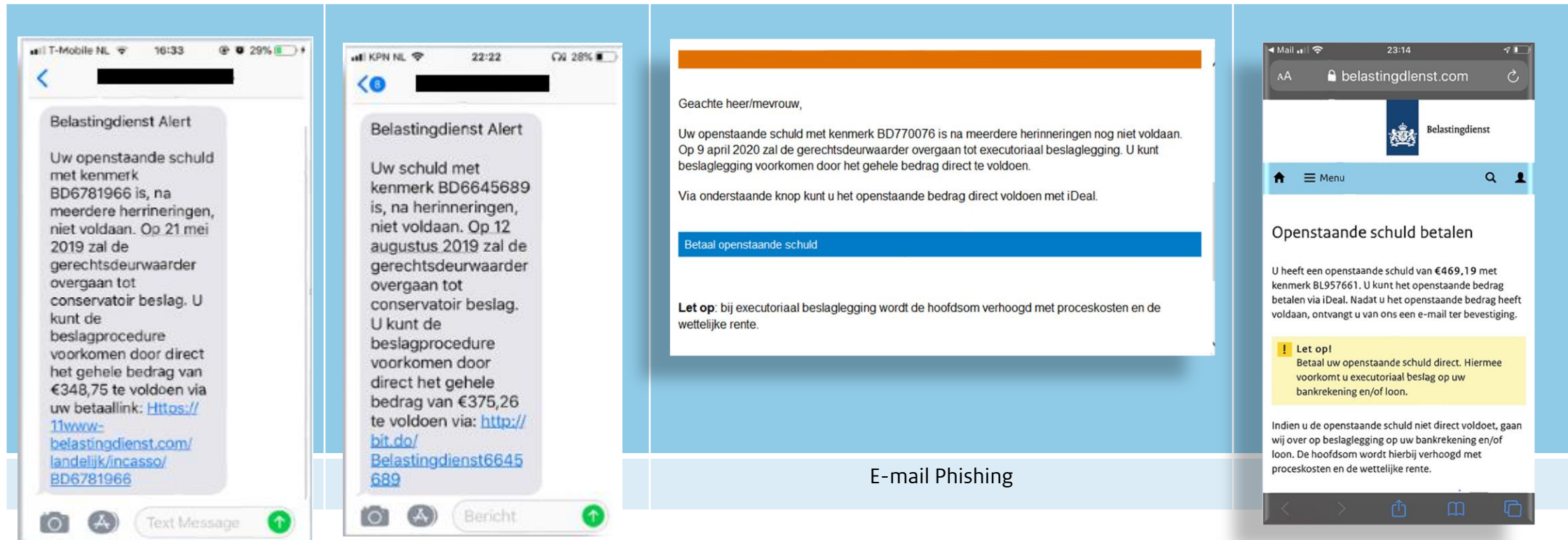


Outside to outside - Phishing, SMishing, and SPAM



Outside to outside - Phishing, SMishing, and SPAM

Evolutie van Phishing naar SMishing/Phishing

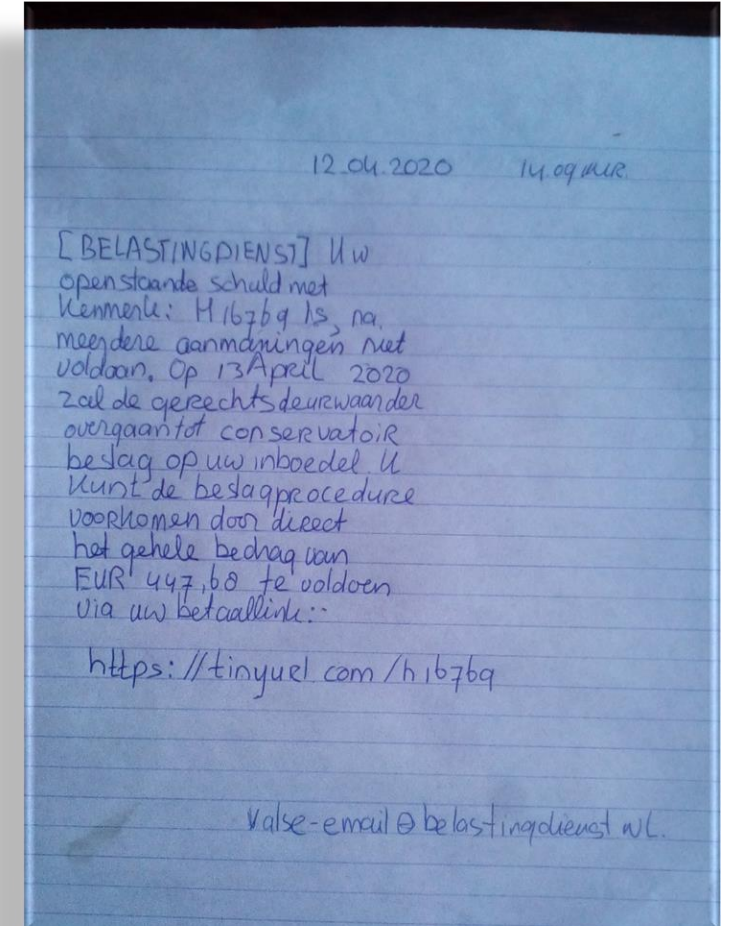


The image illustrates the evolution of phishing attacks through four stages:

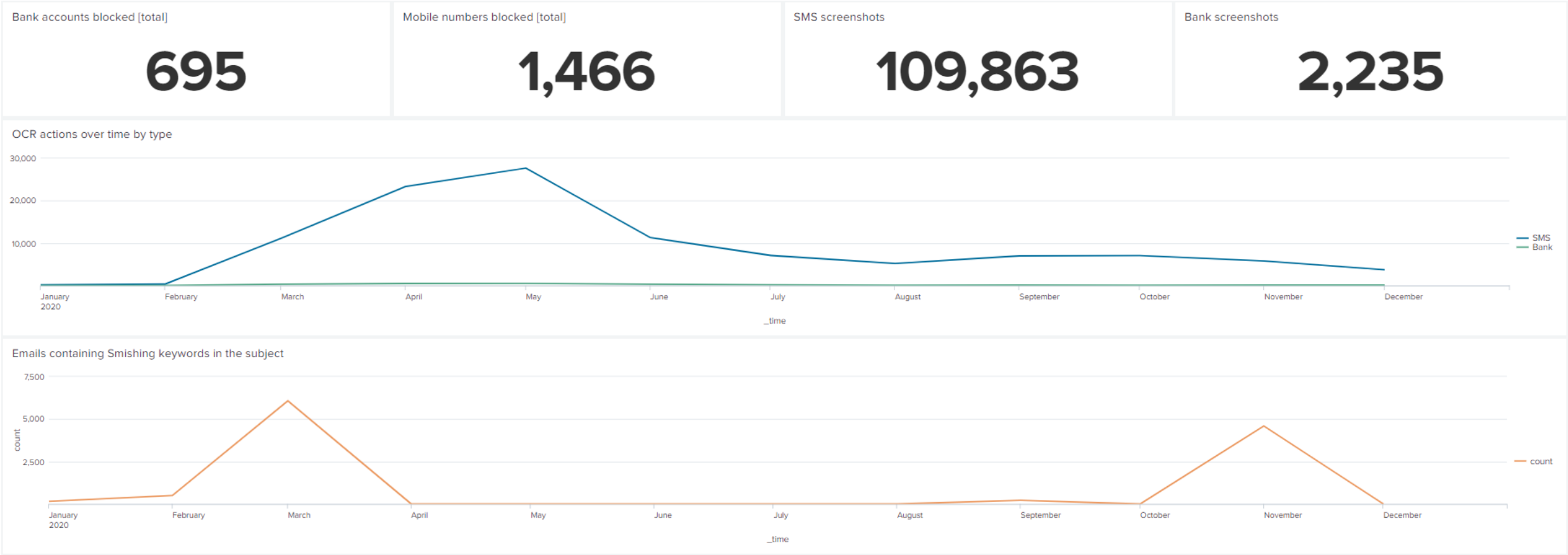
- Stage 1 (SMS):** A text message from 'Belastingdienst Alert' (Tax Service Alert) warning of a conservatorship seizure (conservatoir beslag) for a tax debt (Uw openstaande schuld met kenmerk BD6781966) and providing a link to <https://11www-belastingdienst.com/landelijk/incasso/BD6781966>.
- Stage 2 (SMS):** A text message from 'Belastingdienst Alert' warning of a conservatorship seizure for a tax debt (Uw schuld met kenmerk BD6645689) and providing a link to <http://bit.do/Belastingdienst6645689>.
- Stage 3 (Email):** An email from 'Belastingdienst' with a subject line 'Geachte heer/mevrouw,' and a body text warning of a conservatorship seizure for a tax debt (Uw openstaande schuld met kenmerk BD770076) and providing a link to <https://www.belastingdienst.com>.
- Stage 4 (Email):** An email from 'Belastingdienst' with a subject line 'Openstaande schuld betalen' (Pay outstanding debt) and a body text warning of a conservatorship seizure for a tax debt (U heeft een openstaande schuld van €469,19 met kenmerk BL957661) and providing a link to <https://www.belastingdienst.com>.

The email phishing stage is labeled 'E-mail Phishing'.

Outside to outside - Phishing, SMishing, and SPAM



Outside to outside - Phishing, SMishing, and SPAM



Outside to outside - Phishing, SMishing, and SPAM

Ik heb helaas dit bedrag overgemaakt!

Mvg M. ...

Tel:06-20000000

Verstuurd vanaf mijn iPhone

Begin doorgestuurd bericht:

Van: "Belastingdienst" <belastingaangifte@belastingdienst.nl>

Datum: 23 augustus 2015 11:05:10 CEST

Aan: info@belastingdienst.nl

Onderwerp: Belastingaangifte 2014

Antwoord aan: belastingaangifte@belastingdienst.nl

Van: Belastingdienst <belastingaangifte@belastingdienst.nl>

Antwoord-naar: belastingaangifte@belastingdienst.nl

Aan: info@belastingdienst.nl

GEBOEKT

dit worden
geboekt?

BETAALD PER OVERBOORT 05 AUG 2015


BETAALD PER OVERBOORT 05 AUG 2015

Geachte heer/mevrouw,

Bij controle van onze administratie hebben wij geconstateerd dat er een betaling is geboekt op



Outside to outside - Phishing, SMishing, and SPAM



DigiD Je eigen inlogcode voor de hele overheid

Belastingbetaling (1/3)

1 Persoonsgegevens

Burgerservicenummer *


Geboortedatum * onbekend

Postcode *

Uw e-mailadres *

Volgende

Geen antwoord op uw vraag?
[Bekijk de overige veelgestelde vragen](#) [opent in een nieuw venster] of [neem contact op](#) [opent in een nieuw venster] met de DigiD helpdesk.



DigiD Je eigen inlogcode voor de hele overheid

Belastingbetaling (2/3)


2 Betaling

Bedrag **46,00 Euro**

Kies uw bank *

Volgende

Geen antwoord op uw vraag?
[Bekijk de overige veelgestelde vragen](#) [opent in een nieuw venster] of [neem contact op](#) [opent in een nieuw venster] met de DigiD helpdesk.



Betalen met iDEAL

Ondertekenen Betalen Bevestigen Terug naar webwinkel

Begunstigde **Stichting Mollie Payments inzake Bitonic**

Omschrijving **BTC 0,09519700 aan 19Hg...**


Bedrag **€ 46,00**

Bankpas Rekeningnummer/**IBAN**

Pasnummer

Ga verder Annuleren Help

Ga alleen verder als de adresregel begint met <https://betalen.rabobank.nl/...>
> [Hoe controleert u de veiligheid van uw verbinding?](#)
> [Lees meer over veiligheid](#)



Outside to outside - Phishing, SMishing, and SPAM

[Success] BTC Address: <bitcoin wallet>

idc:<ssn>

dbd: 01

dbm: 9

dby: <geboortejaar>

zip:<zipcode>

eml: <email adres>

bid: ideal_RABONL2U

IP : 84.26.XX.XX9

USERAGENT : Mozilla/5.0 (Windows NT 6.1; WOW64)

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.153

Safari/537.36

=====

Success] BTC Address: <bitcoin wallet>

idc:<ssn>

dbd: 21

dbm: 11

dby: <geboortejaar>

zip:<zipcode>

eml: <email adres>

bid: ideal_RABONL2U

IP : 77.169.XXX.XX8

USERAGENT : Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)

=====



Outside to outside - Phishing, SMishing, and SPAM

**DigiD**

Je eigen inlogcode voor de hele overheid

Belastingteruggave

Geachte b.schrijver@xmsnet.nl ,

Na de laatste jaarlijkse berekeningen van uw fiscale activiteit, hebben wij vastgesteld dat u in aanmerking komt voor belastingteruggave. De belastingteruggave dient u aan te vragen dit wordt binnen 14 werkdagen verwerkt.

In uw situatie is geconstateerd dat u belasting ontvangt over het jaar 2016. Om uw belastingteruggave aan te vragen klikt u op de DigiD logo en doorloopt u de stappen.

Een teruggave kan worden uitgesteld voor een verscheidenheid van redenen.

Bijvoorbeeld het indienen van ongeldige records of toepassen na de deadline.

Let op!

Bewaar deze brief/e-mail bij uw andere papieren.

Zo hebt u belangrijke informatie over de Belastingdienst bij de hand.

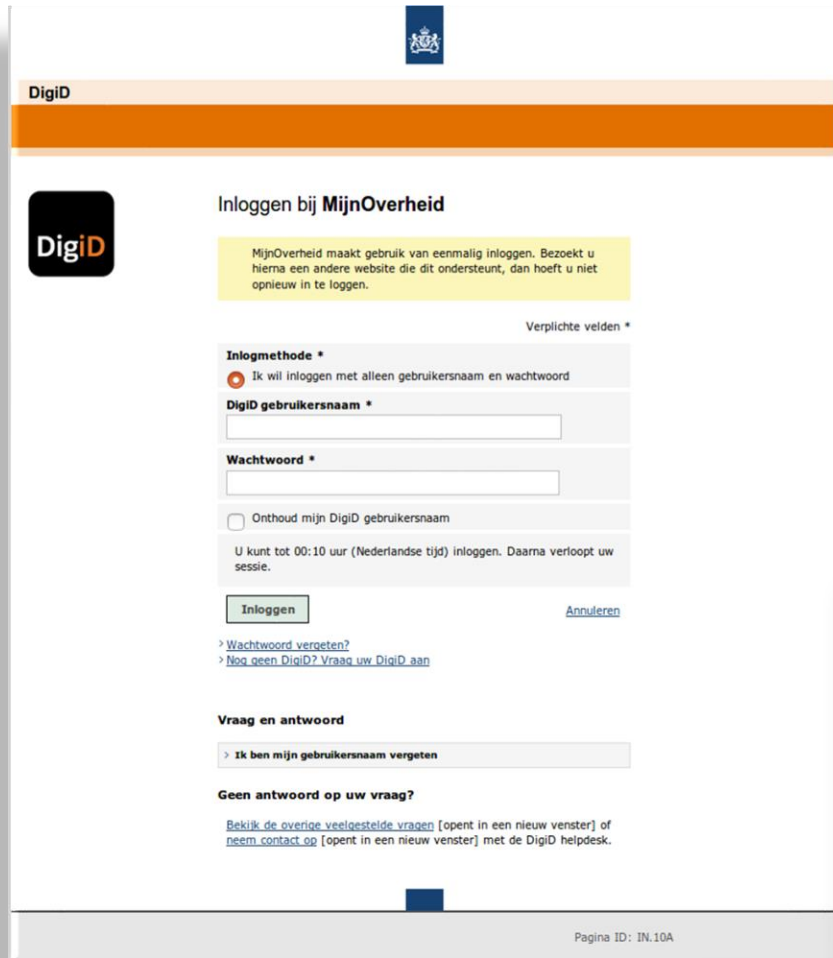
Met vriendelijke groet,

Jos Paal

Belastingdienst

Afdeling Administratie

Outside to outside - Phishing, SMishing, and SPAM



DigiD

Inloggen bij **MijnOverheid**

MijnOverheid maakt gebruik van eenmalig inloggen. Bezoekt u hierna een andere website die dit ondersteunt, dan hoeft u niet opnieuw in te loggen.

Verplichte velden *

Inlogmethode *

☒ Ik wil inloggen met alleen gebruikersnaam en wachtwoord

DigiD gebruikersnaam *

Wachtwoord *

☐ Onthoud mijn DigiD gebruikersnaam

U kunt tot 00:10 uur (Nederlandse tijd) inloggen. Daarna verloopt uw sessie.

[Annuleren](#)

[Wachtwoord vergeten?](#)
[Nog geen DigiD? Vraag uw DigiD aan](#)

Vraag en antwoord

Geen antwoord op uw vraag?

[Bekijk de overige veelgestelde vragen](#) [opent in een nieuw venster] of [neem contact op](#) [opent in een nieuw venster] met de DigiD helpdesk.

Pagina ID: IN.10A

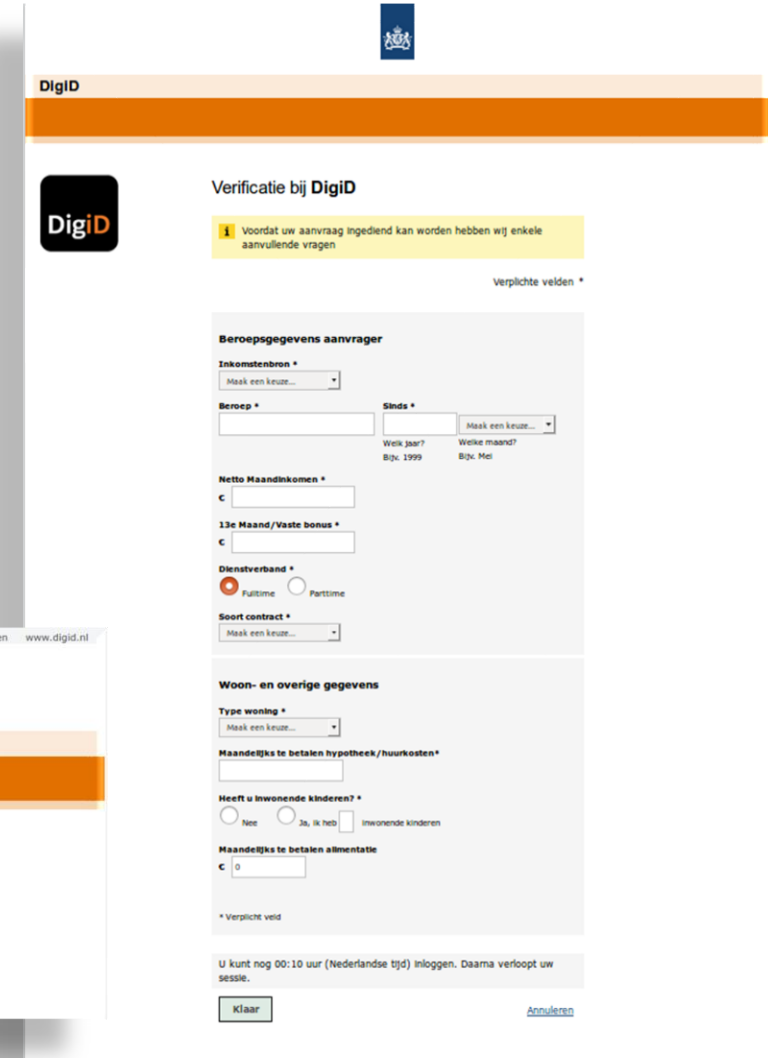


DigiD Je eigen inlogcode voor de hele overheid

Aanvraag verstuurd

Uw aanvraag (van de toeslag) is succesvol ontvangen.

Uw zult binnen 14 werkdagen een schriftelijke bevestiging van uw aanvraag ontvangen.



DigiD

Verificatie bij DigiD

I Voordat uw aanvraag ingediend kan worden hebben wij enkele aanvullende vragen

Verplichte velden *

Beroepsgegevens aanvrager

Inkomstenbron *

Maak een keuze...

Beroep *

Sinds *

Maak een keuze...

Welk jaar? Welke maand?

Bijv. 1999 Bijv. Mei

Netto Maandinkomen *

€

13e Maand/Waste bonus *

€

Dienstverband *

☒ Fulltime ☐ Parttime

Soort contract *

Maak een keuze...

Woon- en overige gegevens

Type woning *

Maak een keuze...

Maandelijks te betalen hypotheek/huurkosten *

€

Heeft u inwonende kinderen? *

☐ Nee ☐ Ja, ik heb ☐ inwonende kinderen

Maandelijks te betalen alimentatie

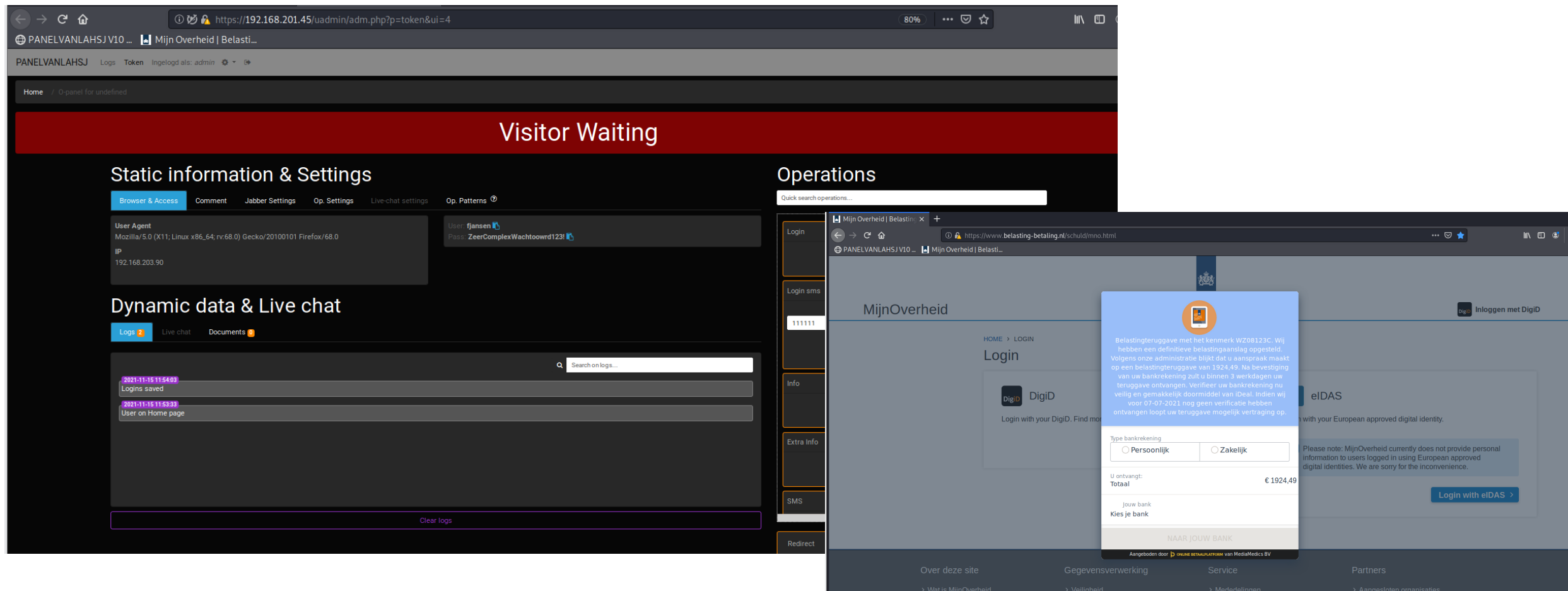
€

* Verplichte veld

U kunt nog 00:10 uur (Nederlandse tijd) inloggen. Daarna verloopt uw sessie.

[Annuleren](#)

Outside to outside - Phishing, SMishing, and SPAM



The screenshot displays a web application interface, likely a phishing site, with two main panels.

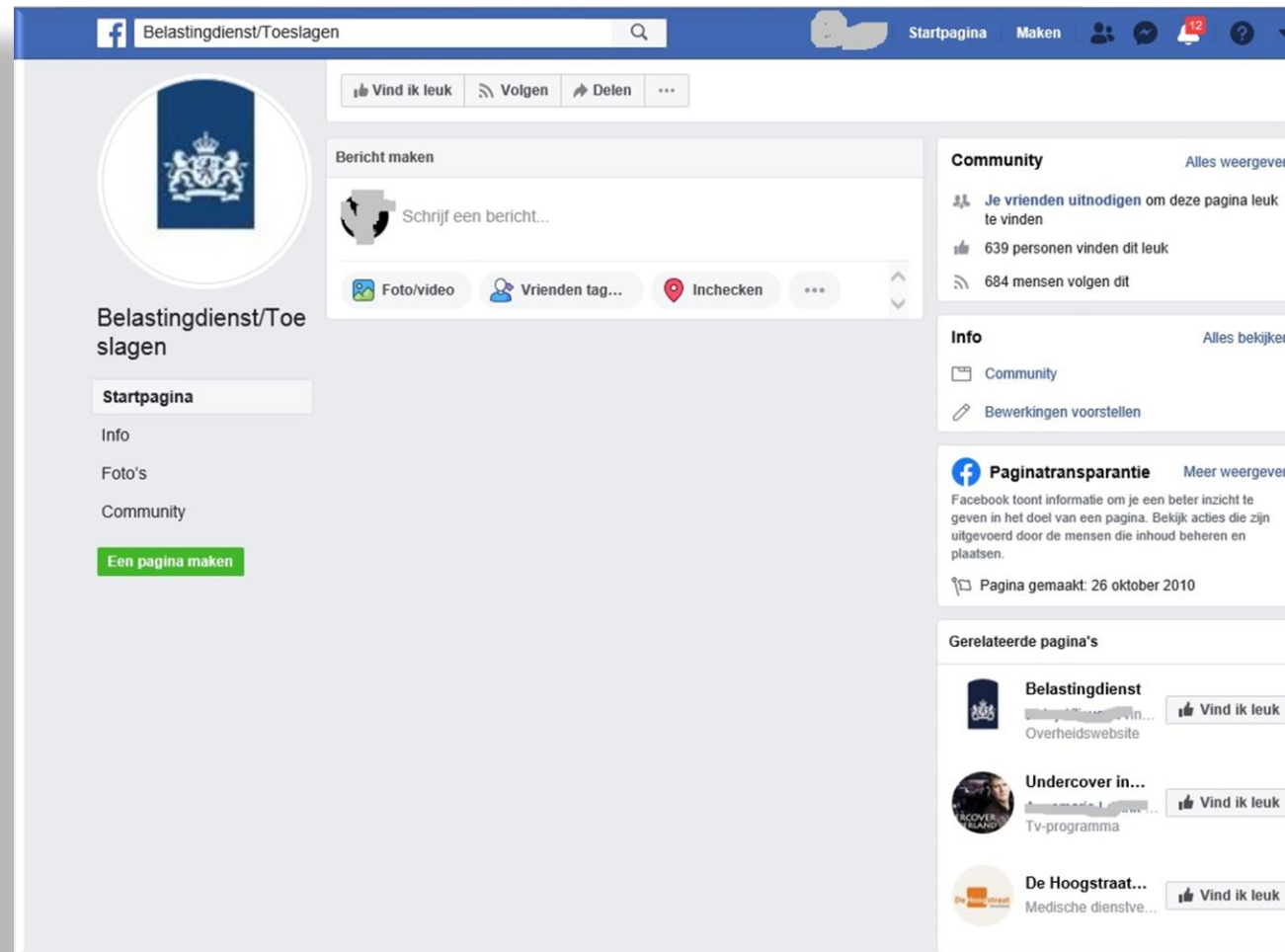
Left Panel (Internal Interface):

- Header:** PANELVANLAHSJ V10 ... Mijn Overheid | Belasti...
- Navigation:** Home / O-panel for undefined
- Static information & Settings:**
 - Browser & Access:** User Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0; IP: 192.168.203.90
 - Dynamic data & Live chat:** Logs, Live chat, Documents. Search on logs... (2021-11-15 11:54:03) Logins saved; (2021-11-15 11:53:33) User on Home page; Clear logs
- Operations:** Quick search operations... (Login, Login sms, Info, Extra Info, SMS, Redirect)

Right Panel (User Interface):

- Header:** MijnOverheid
- Navigation:** HOME > LOGIN
- Login Section:** Login with your DigiID. Find mo... (DigiD logo)
- Warning Overlay:** Belastingteruggave met het kenmerk WZ08123C. Wij hebben een definitieve belastingaanslag opgesteld. Volgens onze administratie blijkt dat u aanspraak maakt op een belastingteruggave van 1924,49. Na bevestiging van uw bankrekening zult u binnen 3 werkdagen uw teruggave ontvangen. Verifieer uw bankrekening nu veilig en gemakkelijk doormiddel van iDeal. Indien wij voor 07-07-2021 nog geen verificatie hebben ontvangen loopt uw teruggave mogelijk vertraging op. Type bankrekening: ☐ Persoonlijk ☐ Zakelijk. U ontvangt: Totaal € 1924,49. U ontvangt: Totaal € 1924,49. Kies je bank. NAAR JOUW BANK. Aangeboden door UNIBRE BELASTINGEN van MediaMedics BV.
- Footer:** Over deze site, Gegevensverwerking, Service, Partners. Wat is MijnOverheid, Veiligheid, Mededelingen, Aangesloten organisaties.

Outside to Outside – Phishing, SMishing, and SPAM



Outside to outside - Phishing, SMishing and SPAM

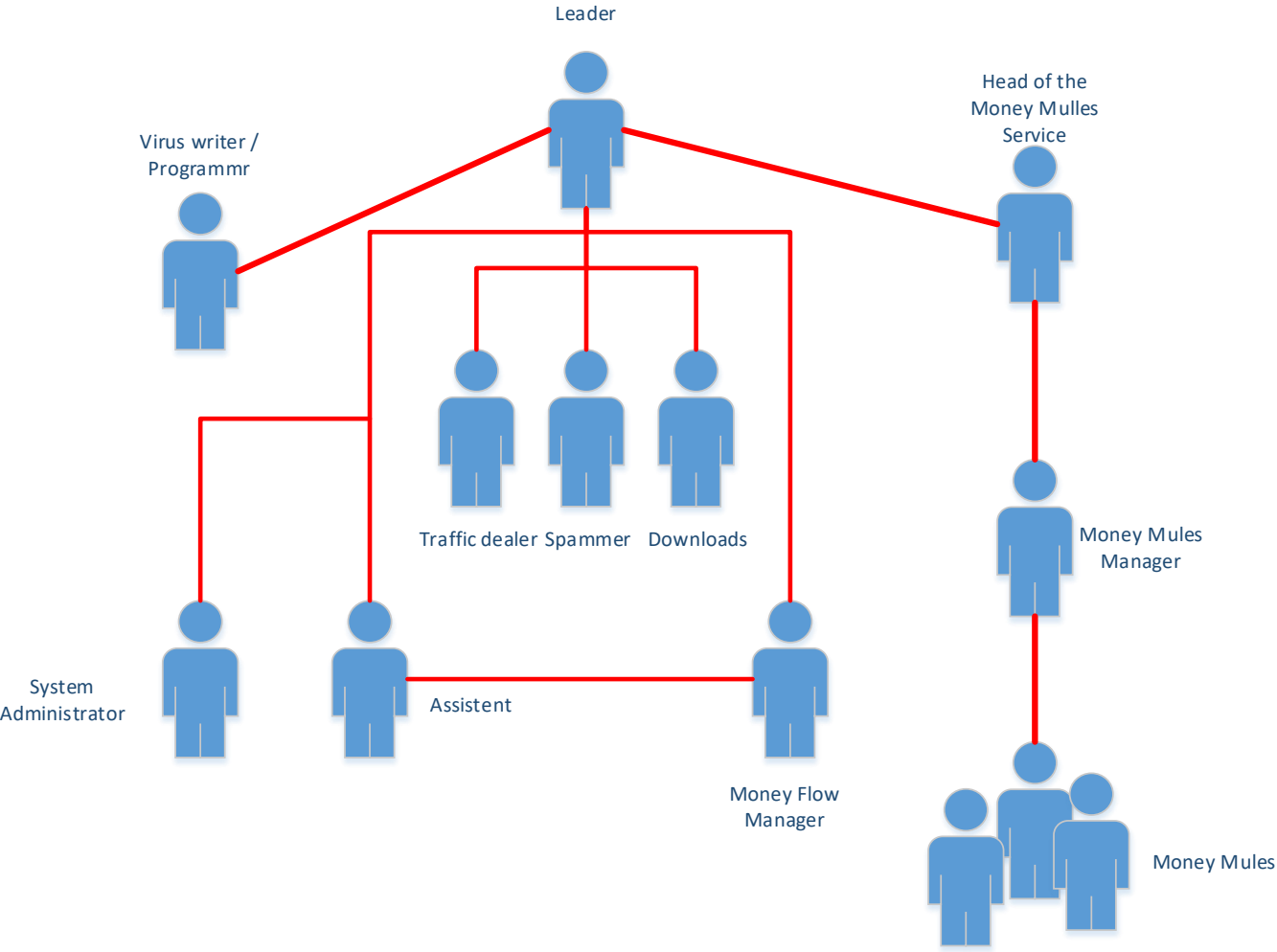


Outside to Inside – Coordinated Vulnerability Disclosure

- 69 Responsible Disclosure notifications received.
- 41 trophies awarded to the reporter for a vulnerability found.
- Multiple reports received about the same vulnerability (e.g. clickjacking).



Example of Cyber Criminal Network



Partnerships

① National Response Network

- ① goal: The National Response Network (NRN) is a collaborative effort with the goal of strengthening the joint response to cybersecurity incidents;
- ① based on a signed covenant;
- ① published in the Dutch Government Gazette.



Ministerie van Defensie



Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid



Belastingdienst



COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

Link: <https://zoek.officielebekendmakingen.nl/stcrt-2020-12976.html>

Partnerships

- ④ Dutch antiDDoS coalition.
- ④ Dutch Tax and Customs Administration is chair of the working group Exercises



- ④ Working group on fighting SMishing with banks, prosecution office, law enforcement, and internet providers. Chair is the COIN association.



Partnerships

- ④ o-IRT-o, public-private partnership between SOC/CERT within the Netherlands.
- ④ NCSC liaison consultation, PPS at tactical level.
- ④ ISACs, including the RijksISAC.
- ④ Splunk Working Group with Tax Administrations of Norway, Denmark, Netherlands and the UK.
- ④ TAX-ISAC with Tax Administrations of the UK, USA, Canada.
- ④ J-SOC, operational cooperation between SOC's within the Dutch National Government.

Joint Security Operations Center

2010 - Establishment of SOC BLD

2013 - SOC Phase 2

2013 - Establishment of SOC RWS

2014 - Nuclear Security Summit

2014 - Establishment SOC SSC-ICT

2014 - The Virtual State SOC (Noordbeek)

2015 - GCCS & ONE Conference

2015 - Idea Joint SOC

2016 - CTO Council

2017 - Threat Intel Platform

2017 - VERIS Incident Taxonomy

2017 - Joint training plan

2018 - Best practice 2.0

2018 - Connecting DICTU

2019 - Blue Team Working Group

2020 - Connecting DUO

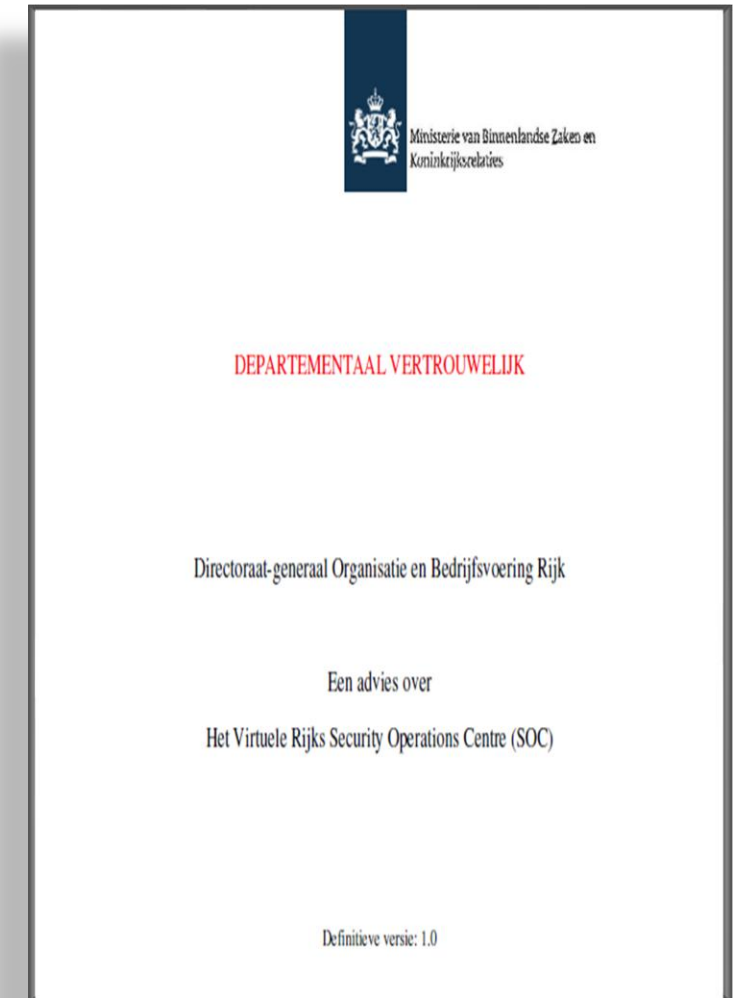
2020 - Start J-SOC Best Practice 3.0

2021 - JenV SOC connection



Origin of J-SOC

- ④ Research of Min BZK into the Virtual Governmental SOC
- ④ (BZKSOC4 Report Virtual Government SOC v1.0
- ④ Operational cooperation between:
 - ④ Tax Authority
 - ④ Rijkswaterstaat
 - ④ Shared Service Center ICT
 - ④ DICTU
 - ④ DUO
 - ④ National Cyber Security Center
 - ④ SOC MinJ&V
 - ④ Ministry of Defense
- ④ Knowledge sharing and alignment of processes/organization
- ④ Virtueel SOC. Own responsibilities.



SOC-CMM, Dutch Tax and Customs Administration, and J-SOC

- ④ The follow-up to SIM3 measurement. SIM3 measures for CERT less for SOC.
- ④ We need to compare the maturity of various services.
- ④ Starting point:
 - ④ Starting from the SOC-CMM model (version 2.1 'advanced'), where can the J-SOC improve?“
- ④ Strengthen each other " *Where are you good in and I a little less and how can you help me?*

SOC-CMM, Dutch Tax and Customs Administration, and J-SOC

- ④ Run as self-assessments and then compare results. Not a good plan. The problem is the interpretation of questions.
- ④ The self-assessment was done by SOC Team Lead with support from the SOC Manager and SOC Analysts.
- ④ The approach was:
 - ④ can a measurement result be substantiated ("Tell me");
 - ④ is the necessary evidence available for it ("Show me").
- ④ Can be resolved by having one organisation perform all SOC-CMM measurements in line with SIM3 maturity measurements.

SOC-CMM, Dutch Tax and Customs Administration, and J-SOC

- ④ Process implementation SOC-CMM self-assessment:
 - ④ kick-off session with agreements on delivery of evidence to make comparison easier;
 - ④ conduct self-assessment by SOC-Leads;
 - ④ group interview per domain;
 - ④ the highest-scoring organisation compared with the lowest-scoring organisation.

		Org1	Org2	Org3	Org4	High Score	Lowest score
Domain	Aspect						
Business	1. Business Drivers						
	2. Customers						
	3. Charter						
	4. Governance						
	5. Privacy						
Overall	Business						
People	1. Employees						
	2. Roles and Hierarchy						
	3. People Management						
	4. Knowledge Management						
	5. Training and Education						
Overall	People						

SOC-CMM, Dutch Tax and Customs Administration, and J-SOC

- ④ Follow-up steps:
 - ④ feedback is given by domain for improvement SOC-CMM;
 - ④ looking for one organisation to conduct SOC-CMM measurement for all participants;
 - ④ conduct the SOC-CMM assessment yearly;
 - ④ investigate whether that applies to all domains or a focus domain per year;
 - ④ the basis for the new J-SOC Best Practice. The good news is that there will also be a **TLP:CLEAR** version.

