ACCESS42
Cybersecurity

Cybersecurity Summit 2023

tenable mimecast

COFENSE Security Scorecard SALT Delinea VECTRA CROWDSTRIKE

Lookout

CCV CYBER PENTEST DigiTrust NEN 7510 DigiTrust ISO 27001

ACCESS42 Cybersecurity

CYBERCRIMINALS

are leading the **innovation race**

Staying ahead of the evolving threat landscape is key to strengthening resilience to security risks.

CCV CYBER PENTEST

Digitrust NEN 7510

Digitrust ISO 27001

ACCESS42 Cybersecurity

2023 trends

- **The rise of Artificial Intelligence**
  - Deepfake / voice cloning
  - ChatGPT
  - Ransomware with AI powered targeting

CCV CYBER PENTEST
Digitrust NEN 7510
Digitrust ISO 27001
Access42 Cybersecurity

2023

- **The ris**
  - Deep
  - Chat
  - Rans

rtlnieuws

12 °

Een echte video en een nepfilmpje van Facebook-ceo Mark Zuckerberg

Een meerderheid in de Tweede Kamer wil deepfake-technologie waarmee echt lijkende nepvideo's worden gemaakt in bepaalde gevallen verbieden.

Een ruime Kamermeerderheid ondertekent een motie van de VVD die moet voorkomen dat de technologie wordt ingezet voor 'kwaadaardige doeleinden'. Zo is onlangs een neppornofilmpje verspreid waarop presentatrice Welmoed Sijtsma te zien is.

2023 trends

- **Phishing**: the main attackers' weapon of choice

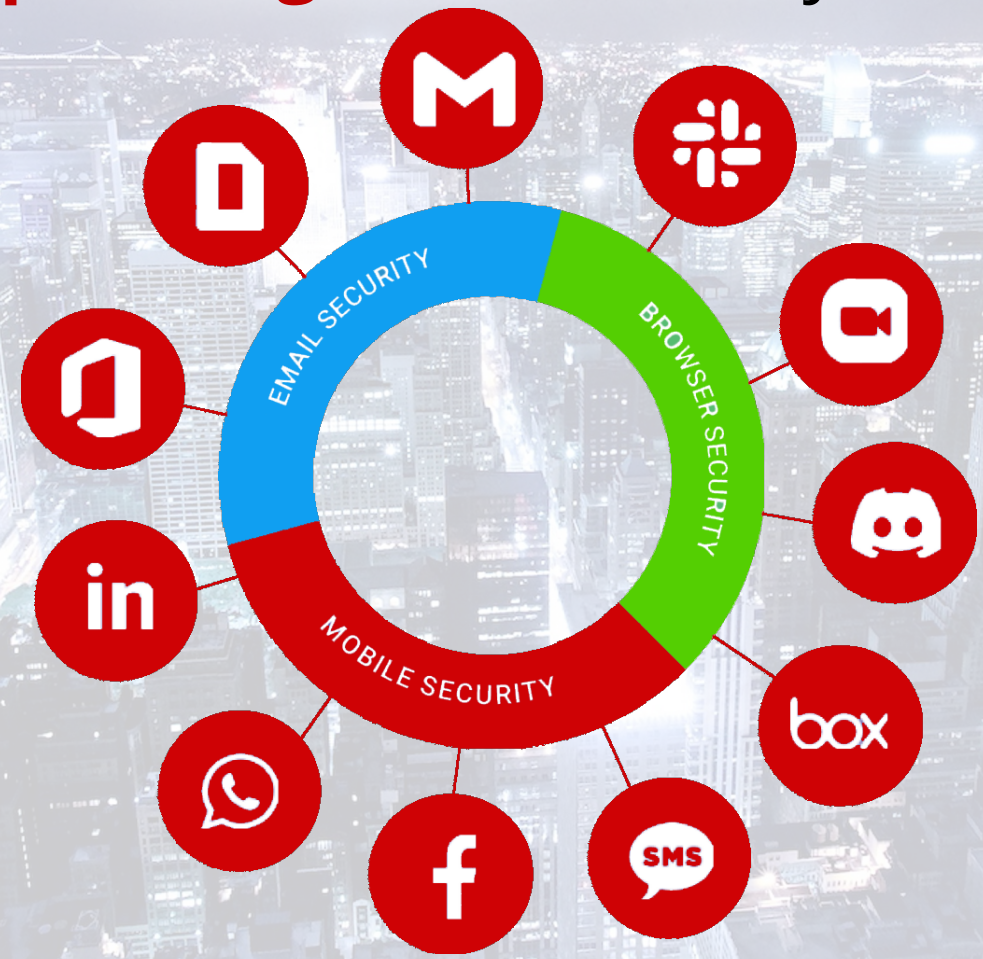
2023 Key findings in the Netherlands

- **88%** companies were harmed by a ransomware attack
- **99%** of companies provide some form of cyber awareness training to their workforce
- **57%** of respondents say they need more cybersecurity budget to protect their organization
- **66%** have implemented or plan to implement measures to monitor and protect against email-borned attacks or data leaks in internal to internal emails

Source: Mimecast - The State of Email Security Report 2023

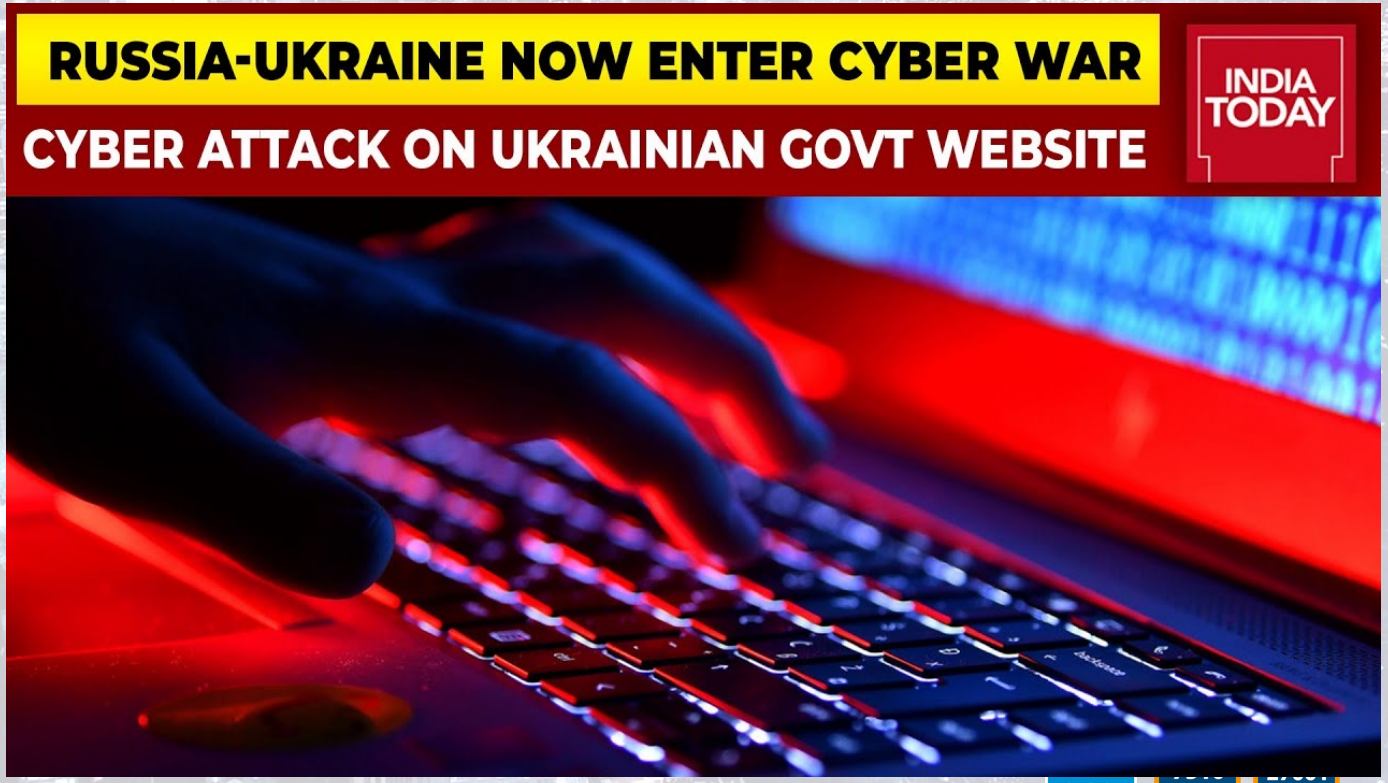
2023 trends

- **Multi-channel phishing**: Email security is not (good) enough anymore



2023 trends

- **Geopolitical**: Taking advantage of the increasing global fragmentation



2023 trend

- **Geopolitical**: T … easing global fragmentation

Anonymous Sudan

Anonymous Sudan and geopolitical cyber attacks

Contrary to its name, Anonymous Sudan is not associated with the Sudan administration or the country's cause, The Cyber Express reported earlier. Instead, there are indications that it may have connections to Russia's Killnet hacking group.

Anonymous Sudan has been directing its attacks towards Israel and India, two countries that have recently maintained friendly relations with Russia. This makes it challenging to discern the true intentions and patterns behind the threat group's actions.

While initially launching DDoS attacks on firms in Sweden, the Netherlands, Australia, and Germany, citing retaliation for anti-Muslim activities, further investigation has uncovered undisclosed connections.

Trustwave SpiderLabs researchers have revealed that Anonymous Sudan is likely a sub-group of Killnet, a threat actor group aligned with pro-Russian interests, with whom they have openly associated..

https://thecyberexpress.com/microsoft-hack-onedrive-outage-anonymous-sudan/amp/

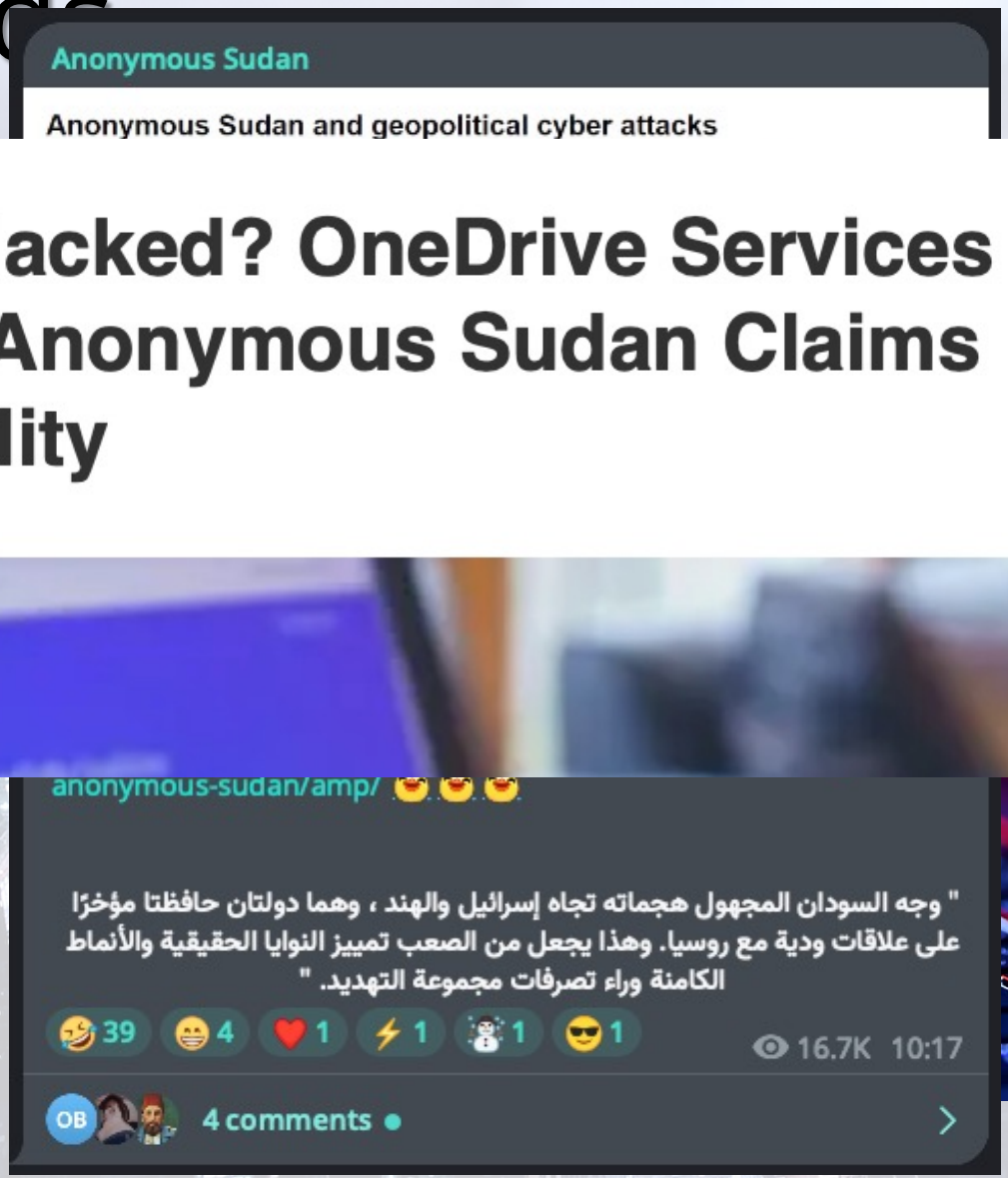
" وجه السودان المجهول هجماته تجاه إسرائيل والهند ، وهما دولتان حافظتا مؤخرًا على علاقات ودية مع روسيا. وهذا يجعل من الصعب تمييز النوايا الحقيقية والأنماط الكامنة وراء تصرفات مجموعة التهديد. "

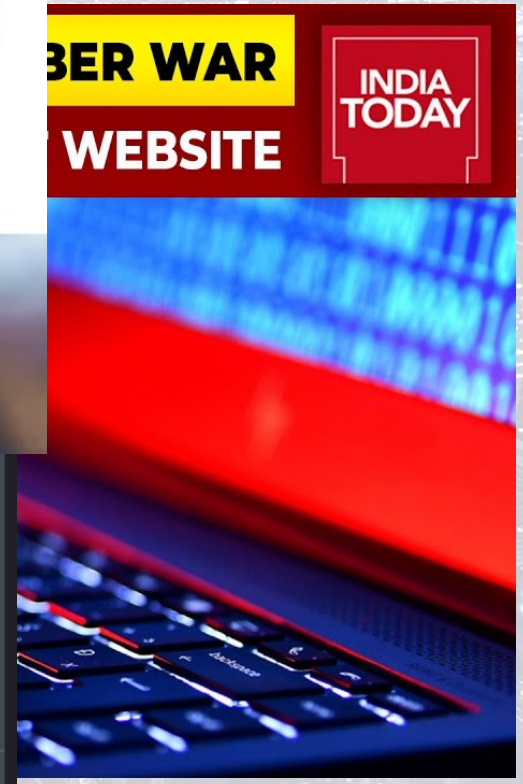
39 4 1 1 1 1 16.7K 10:17

OB 4 comments

2023 trends

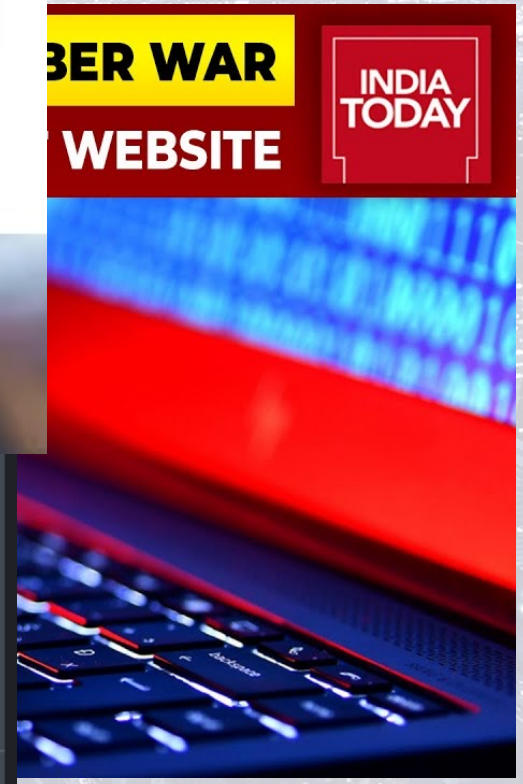
- G … asing global fr…



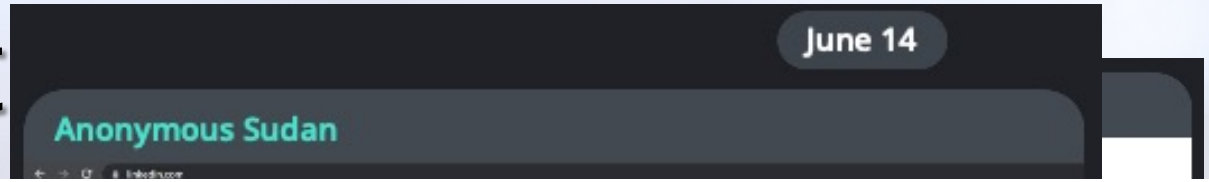


2023 t

- G Micros … asing global
  fr Disrup … es
  Respo … ns



2023 t



LinkedIn

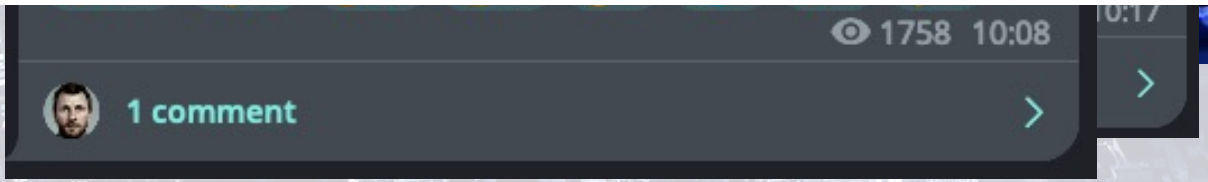
English (English)

Your LinkedIn Network Will Be Back Soon

We've notified our operations staff that you are having a problem reaching LinkedIn. We'll get you reconnected soon.

You can leave this window open and we'll automatically take you back to your LinkedIn home page in a few minutes.

We apologize for the interruption.



CCV CYBER PENTEST

DigiTrust NEN 7510

DigiTrust ISO 27001

Access42 Cybersecurity

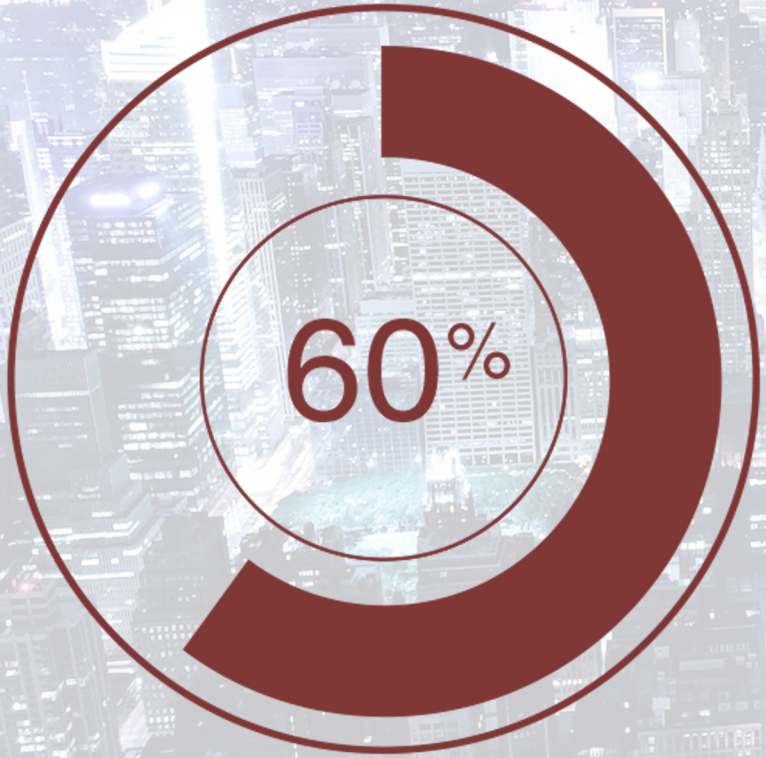
2023 trends

- **Burnout in cybersecurity** and beyond: Cybercriminals never had it easier

- Feeling overwhelmed by the never-ending stream of cyber threats and cyber security trends
- Feeling constantly on edge and anxious about potential attacks
- Losing interest in and enjoyment of work
- Becoming cynical or pessimistic about the prospects of preventing or deterring cyber attacks
- Feeling detached from colleagues and/or other members

2023 trends

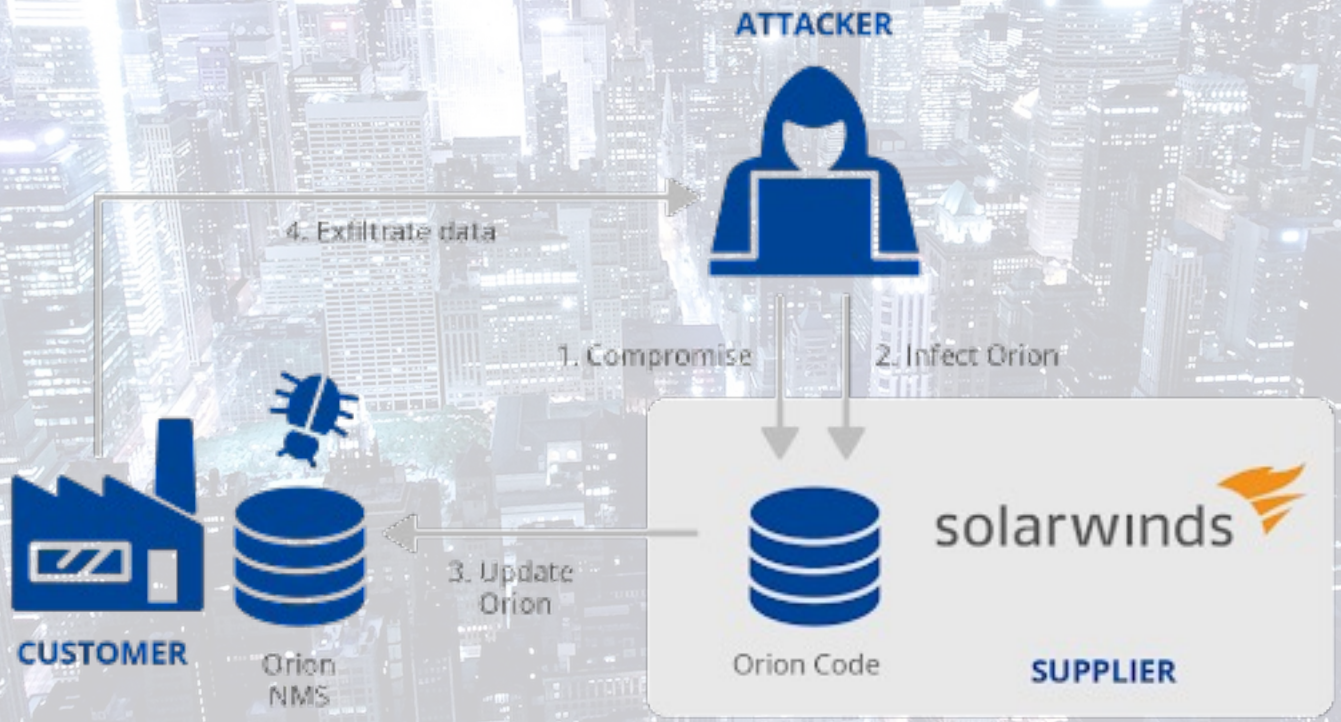
- **Burnout in cybersecurity** and beyond: Cybercriminals never had it easier



Of companies had difficulties retaining qualified cybersecurity professionals in 2022

2023 trends

- **Digital supply chain attacks**: we are all interconnected



2023 trends

- **Digital supply** onnected

Barracuda zero-day abused since 2022 to drop new malware, steal data

By **Sergiu Gatlan** May 30, 2023 04:25 PM 0

Image: Bing Image Creator

Network and email security firm Barracuda today revealed that a recently patched zero-day vulnerability had been exploited for at least seven months to backdoor customers' Email Security Gateway (ESG) appliances with custom malware and steal data.

CUSTOM

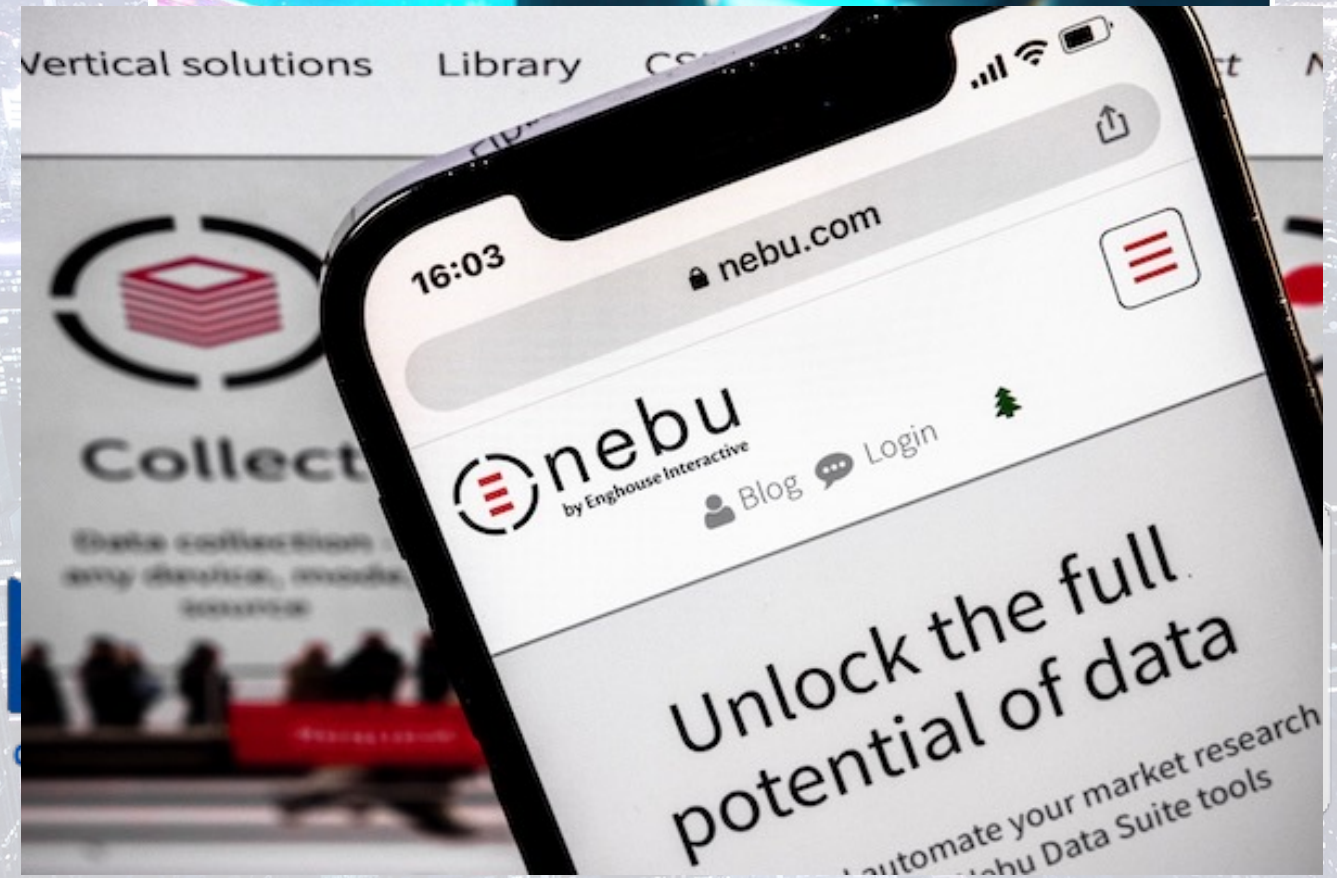
NMS

2023 trends

- **Digital supply** onnected

Barracuda zero-day abused since 2022 to drop new malware, steal data

By **Sergiu Gatlan** May 30, 2023 04:25 PM 0



2023 trends

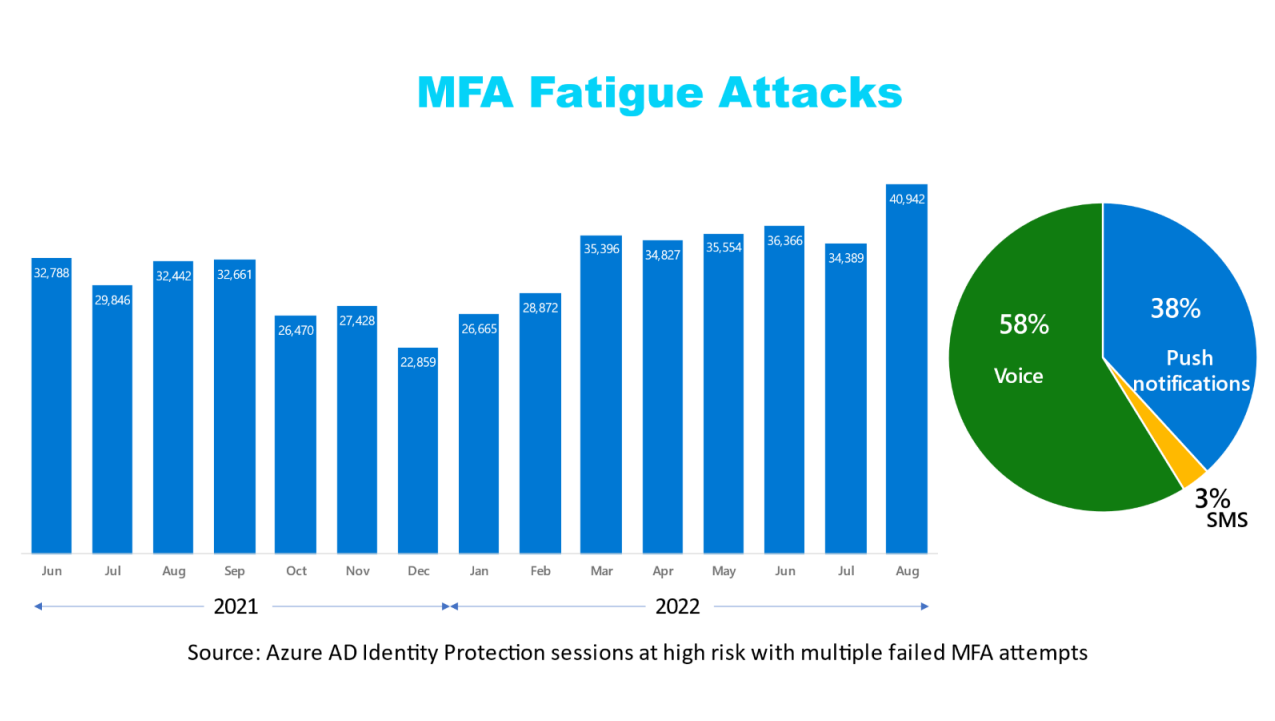
- **Ransomware-as-a-service**: Online blackmail and extortion at the touch of a button
- 2022: highest average cost of data breaches (1)
  - $4.35 million global average cost of a databreach
  - Highest cost in the US, $9.44 million!

"It's not just about stealing files; it's about threatening to publish them"

(1) Source: IBM Cost of a Data Breach Report

2023 trends

- **Multi-factor authentication failing**: **Not as safe as** we thought

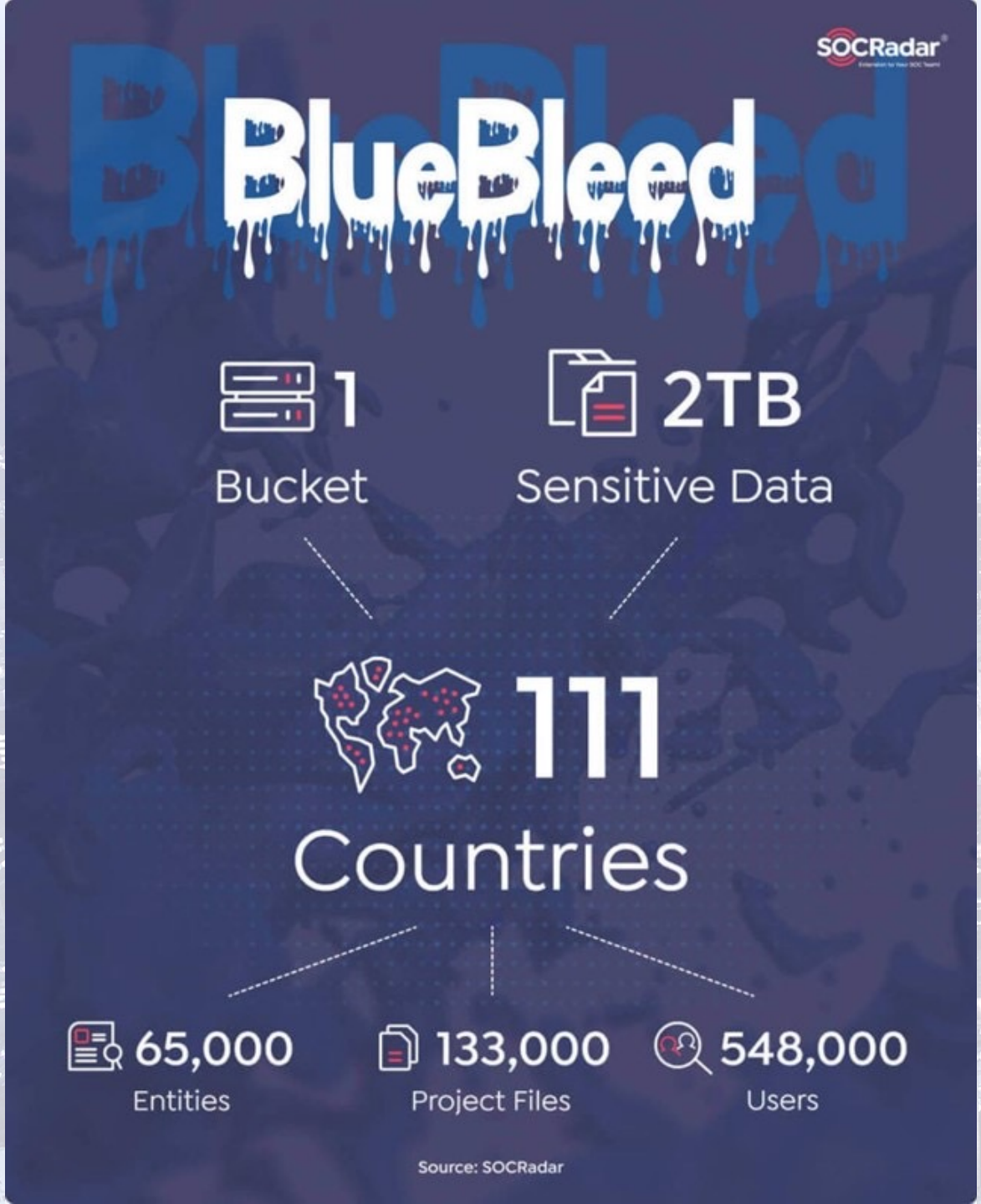


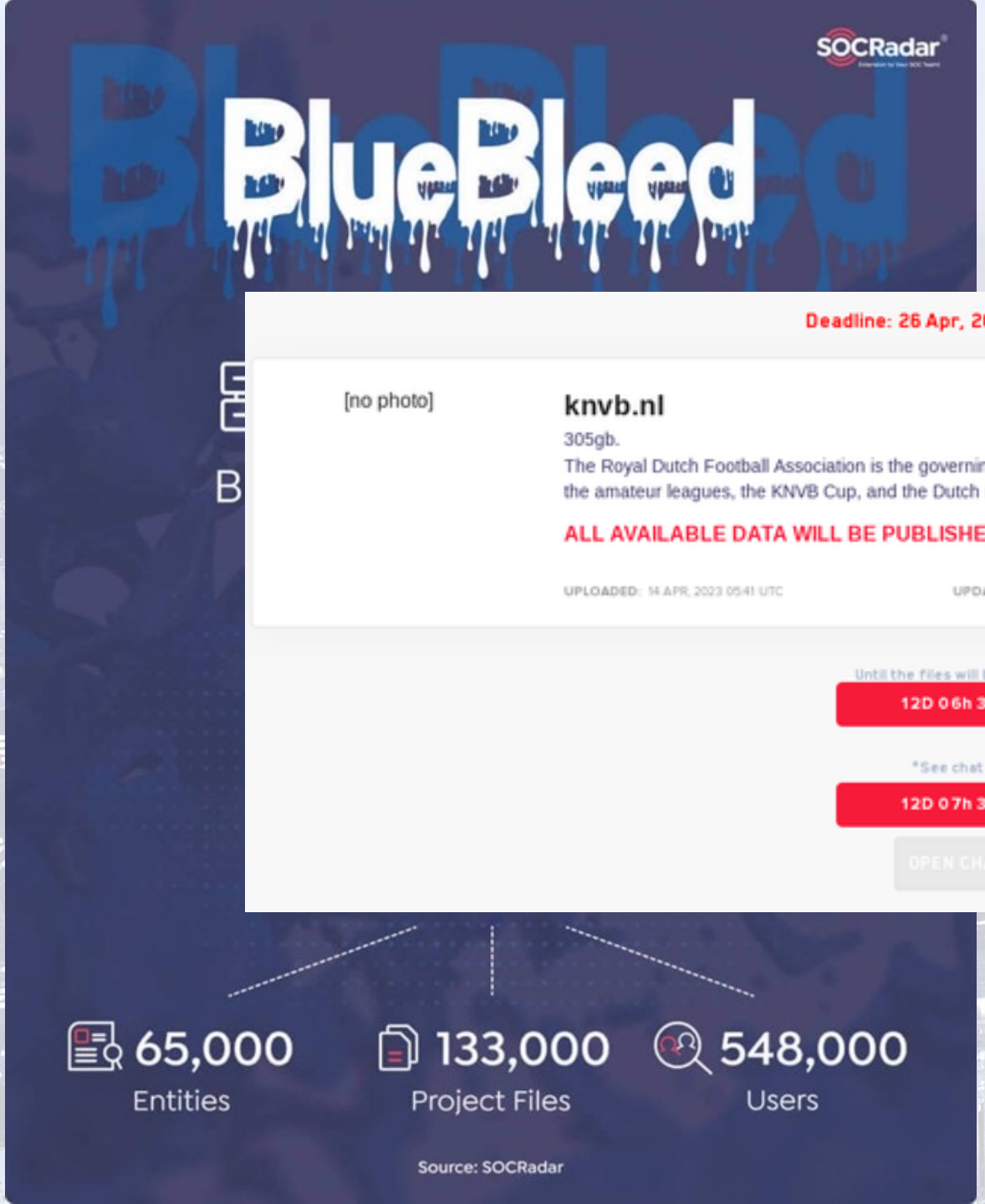
Some Facts and statistics

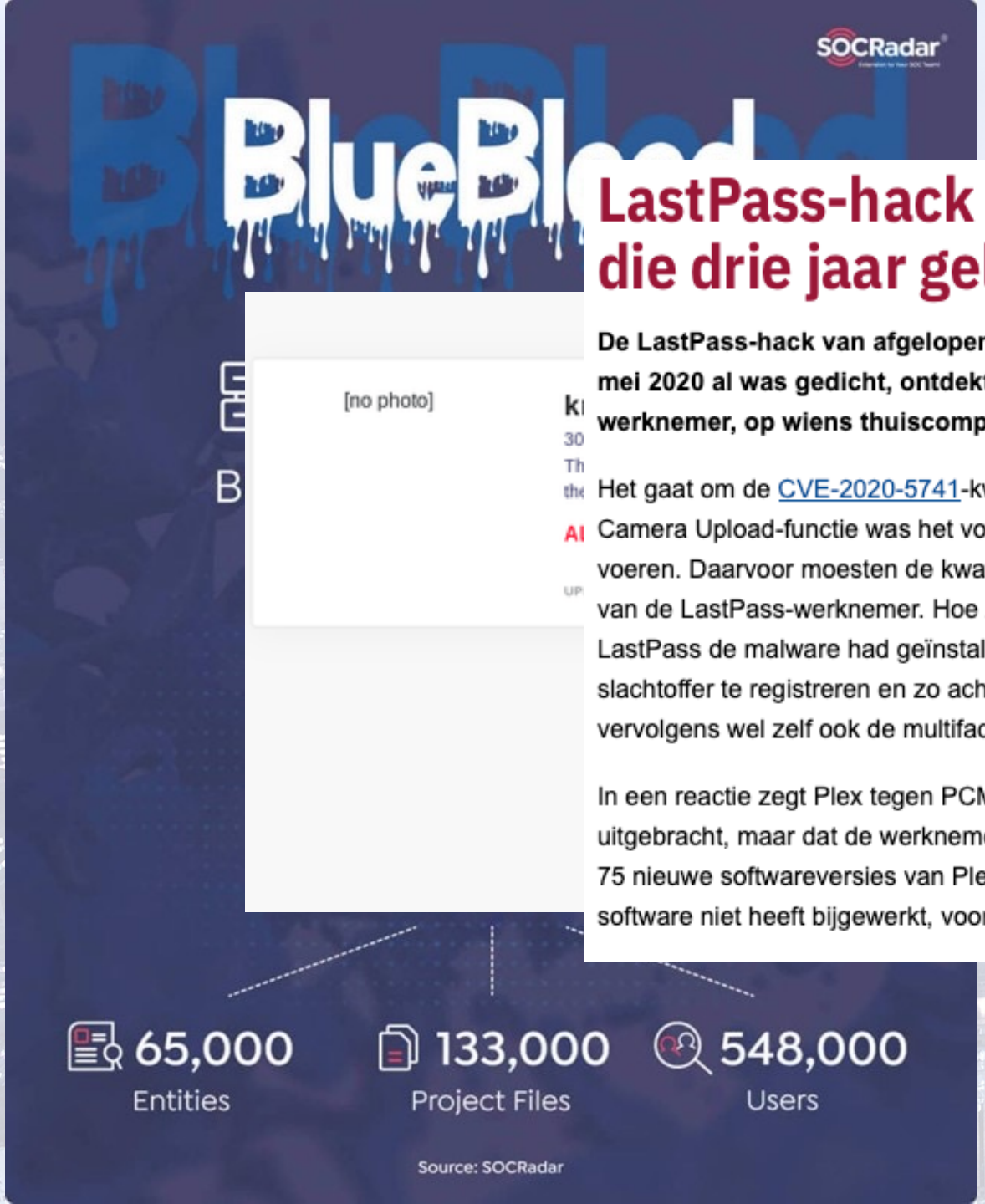
- 2022 had 25.227 vulnerabilities, avg +/- 69 per day
  - > 4000 were critical
  - 25% Growth
- Over 7,000 vulnerabilities were published in Q1 of 2023
  - More than 16% of vulnerabilities have a critical score
- More than one in four companies are still vulnerable to WannaCry!!

5 Common Initial Attack Vectors

- Phishing
- Vulnerability Exploit
- Misconfigurations
- Compromised Credentials
- Supply Chain Vendors


SOCRadar
BlueBleed
1
Bucket
2TB
Sensitive Data
111
Countries
65,000
Entities
133,000
Project Files
548,000
Users
Source: SOCRadar


SOCRadar
BlueBleed
Deadline: 26 Apr, 2023 17:41:56 UTC
[no photo]
knvb.nl
305gb.
The Royal Dutch Football Association is the governing body of football in the Netherlands. It organises the main Dutch football leagues, the amateur leagues, the KNVB Cup, and the Dutch men's and women's national teams.
ALL AVAILABLE DATA WILL BE PUBLISHED !
UPLOADED: 14 APR, 2023 05:41 UTC
UPDATED: 14 APR, 2023 05:41 UTC
Until the files will be available left
12D 06h 32m 24s
*See chat history
12D 07h 32m 24s
OPEN CHAT
65,000
Entities
133,000
Project Files
548,000
Users
Source: SOCRadar



LastPass-hack gebruikte Plex-kwetsbaarheid die drie jaar geleden al was gedicht

De LastPass-hack van afgelopen november maakte gebruik van een kwetsbaarheid in Plex die in mei 2020 al was gedicht, ontdekte PCMag. De hack had voorkomen kunnen worden als de werknemer, op wiens thuiscomputer de malware werd geïnstalleerd, de software had geüpdatet.

Het gaat om de CVE-2020-5741-kwetsbaarheid in de software Plex Media Server, schrijft PCMag. Via de Camera Upload-functie was het voor aanvallers mogelijk om de server schadelijke code uit te laten voeren. Daarvoor moesten de kwaadwillenden wel al beheerderstoegang hebben tot het Plex-account van de LastPass-werknemer. Hoe ze daarin slaagden is niet bekend. Nadat de devops-programmeur van LastPass de malware had geïnstalleerd, waren de hackers in staat om de toetsaanslagen van het slachtoffer te registreren en zo achter het masterwachtwoord te komen. De LastPass-werknemer heeft vervolgens wel zelf ook de multifactorauthenticatieaanvraag goedgekeurd.

In een reactie zegt Plex tegen PCMag dat er in mei 2020 een patch voor de kwetsbaarheid was uitgebracht, maar dat de werknemer in kwestie de software nooit geüpgraded heeft. Sindsdien zijn er al 75 nieuwe softwareversies van Plex uitgebracht. Het is onduidelijk waarom de programmeur al die tijd de software niet heeft bijgewerkt, vooral omdat veel van de updates automatisch horen plaats te vinden.

SOCRadar

Landal GreenParks waarschuwt 12.000 gasten voor mogelijk datalek

donderdag 8 juni 2023, 15:34 door **Redactie**, 4 **reacties**

Landal Greenparks heeft twaalfduizend gasten gewaarschuwd voor een mogelijk datalek nadat criminelen toegang wisten te krijgen tot het MOVEit Transfer-systeem dat het bedrijf gebruikt voor het uitwisselen van gegevens, zo laat een woordvoerder aan Security.NL weten. Bij de aanval zijn mogelijk naam, geboortedatum, geslacht, adresgegevens en e-mailadres buitgemaakt, medlt Landal Greenparks in een e-mail aan gasten.

MOVEit Transfer is een applicatie oor het uitwisselen van bestanden. Allerlei organisaties maken er gebruik van om onder andere vertrouwelijke informatie binnen de organisatie te delen. Door middel van SQL Injection is het mogelijk voor een aanvaller om ongeautoriseerde toegang tot de database van een MOVEit-server te krijgen, om zo vertrouwelijke data te stelen. Daarnaast blijkt dat de aanvallers een webshell op het systeem installeren om zo toegang te behouden. Misbruik van de **kwetsbaarheid** vindt al plaats voordat een patch beschikbaar was.

Ontwikkelaar Progress Software kwam op 31 mei met een beveiligingsupdate en stelde dat klanten hun systemen voor minstens de afgelopen dertig dagen op aanwijzingen van ongeautoriseerde toegang moesten controleren. Vanwege de impact kwamen de Amerikaanse, Duitse en **Nederlandse** autoriteiten met waarschuwingen. De aanvallen tegen MOVEit-servers zijn volgens Microsoft het werk van de criminelen achter de Clop-ransomware. Ook de Amerikaanse overheid kwam met een **waarschuwing** voor misbruik van het lek door de ransomwaregroep.

"Omdat we na onderzoek niet kunnen uitsluiten dat de internetcriminelen daadwerkelijk persoonsgegevens hebben buitgemaakt, brengen wij je hiervan op de hoogte. Wij betreuren dit incident ten zeerste, het incident is inmiddels opgelost en bij de Autoriteit Persoonsgegevens gemeld als mogelijke datalek", zo laat de e-mail van Landal weten. "We betreuren het incident, helaas ligt dit beveiligingsrisico buiten onze invloedsfeer."

Entities Project Files Users

Source: SOCRadar

arheid

n Plex die in
ls de
geüpdatet.

CMag. Via de
te laten
ex-account
grammeur van
an het
emer heeft

was
ien zijn er al
r al die tijd de
te vinden.

CCV CYBER PENTEST

DigiTrust NEN 7510

DigiTrust ISO 27001

ACCESS42 Cybersecurity

MOVEit Transfer Critical Vulnerability (May 2023)

Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment.

Jun 7, 2023 · Knowledge

Title
MOVEit Transfer Critical Vulnerability (May 2023)

URL Name
MOVEit-Transfer-Critical-Vulnerability-31May2023

Article Number
000234532

Information

Revision History

Date	Description
31-May-2023	Original posting
	All supported MOVEit Transfer fixes posted
01-Jun-2023	Enhanced remediation steps, added Indicators of Compromise
	CVE preliminary text
02-Jun-2023	Added products not impacted
	Added MOVEit Transfer 2020.1 (12.1) patch information.
	Published CVE ID added, added section 2.a.vi, added new Indicators of Compromise
03-Jun-2023	Added Revision History, added upgrade and migration guide, updated CVE description, added new Indicators of Compromise, added References
04-Jun-2023	Updated version table to include MOVEit Cloud, converted IOC table to .csv, added new IOCs, updated References
05-Jun-2023	Updated CVE language, updated References to include Microsoft Intel. post
	Added guidance on IIS files to section (2.a iv), updated verbiage on section (2.a i), updated IOCs
06-Jun-2023	Updated Cloud versions table to include Test, updated References
07-Jun-2023	Updated steps to include removing active sessions, added CISA advisory to References, clarified language on APP_WEB_*[random]*.dll files

MOVEit Transfer Critical Vulnerability (May 2023)

Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment.

dond Jun 7, 2023 · Knowledge

Toyota lekt klantgegevens door verkeerd geconfigureerde cloudomgeving

woensdag 31 mei 2023, 17:23 door **Redactie**, 4 **reacties**

Autofabrikant Toyota heeft door een verkeerd geconfigureerde cloudomgeving de **gegevens van klanten gelekt**. Het is het tweede datalek in korte tijd waar het bedrijf mee te maken krijgt. Op 12 mei **meldde** Toyota dat door een verkeerde ingestelde cloudomgeving de locatiegegevens en andere informatie van meer dan twee miljoen klanten bijna tien jaar lang voor iedereen toegankelijk waren.

Vandaag laat de autofabrikant weten dat er opnieuw gegevens van klanten via een verkeerd geconfigureerde cloudomgeving zijn gelekt. Het gaat om informatie over het navigatiesysteem van zo'n 260.000 Japanse klanten die sinds 2015 via internet te vinden was. Daarnaast zijn ook gegevens van klanten in verschillende landen in Azië en Oceanië gelekt, waaronder naam, adresgegevens, telefoonnummer, e-mailadres, klant-id, voertuigregistratienummer en voertuigidentificatienummer. Deze data was vanaf oktober 2016 publiek toegankelijk. Toyota zegt dat het medewerkers opnieuw uitgebreid zal trainen om herhaling te voorkomen. Details over de configuratiefouten zijn niet gegeven.

03-Jun-2023	Added Revision History, added upgrade and migration guide, updated CVE description, added new Indicators of Compromise, added References
04-Jun-2023	Updated version table to include MOVEit Cloud, converted IOC table to .csv, added new IOCs, updated References
05-Jun-2023	Updated CVE language, updated References to include Microsoft Intel. post
	Added guidance on IIS files to section (2.a iv), updated verbiage on section (2.a i), updated IOCs
06-Jun-2023	Updated Cloud versions table to include Test, updated References
07-Jun-2023	Updated steps to include removing active sessions, added CISA advisory to References, clarified language on APP_WEB_*[random]*.dll files

Entities

ACCESS42 Cybersecurity

MOVEit Transfer Critical Vulnerability (May 2023)

Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment.

dond Jun 7, 2023 · Knowledge

Toyota lekt klantgegevens door verkeerd geconfigureerde cloudomgeving

woensdag 31 mei 2023, 17:23 door **Redactie**, 4 **reacties**

Autofabrikant Toyota heeft door een verkeerd geconfigureerde cloudomgeving de **gegevens van klanten**

Stadgenoot waarschuwt 15.000 huurders voor datalek bij marktonderzoeksbureau

donderdag 30 maart 2023, 10:08 door **Redactie**, 7 **reacties**

De Amsterdamse woningcorporatie **Stadgenoot** waarschuwt vijftienduizend huurders voor een datalek dat zich heeft voorgedaan bij marktonderzoeksbureau **USP Marketing Consultancy**. Dit bedrijf voert voor klanten tevredenheidsonderzoeken uit en maakt hierbij gebruik van bepaalde software. De leverancier van deze software heeft te maken gekregen met een datalek.

"Op 24 maart kregen wij schriftelijk bericht dat er sprake was van onbevoegde toegang tot het netwerk van de softwareleverancier. Op 28 maart bevestigde deze leverancier dat er daadwerkelijk data is ontvreemd. Dit betreuren wij zeer en wij hebben onze opdrachtgevers hierover ingelicht. Wij weten nog niet wat er exact is ontvreemd", zo laat het marktonderzoeksbureau weten.

Een van de klanten van USP Marketing Consultancy is Stadgenoot. Vanwege het datalek bij het marktonderzoeksbureau kunnen ook gegevens zijn gelekt van huurders die in het verleden voor één of meer tevredenheidsonderzoeken van

	section (2.a i), updated IOCs
06-Jun-2023	Updated Cloud versions table to include Test, updated References
07-Jun-2023	Updated steps to include removing active sessions, added CISA advisory to References, clarified language on APP_WEB_*[random]*.dll files

Entities

ACCESS42 Cybersecurity

MOVEit Transfer Critical Vulnerability (May 2023)

Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment.

FBI: aanvallen met Royal-ransomware voornamelijk via phishing en RDP

vrijdag 3 maart 2023, 16:38 door **Redactie**, 5 **reacties**

Sinds september zijn allerlei Amerikaanse bedrijven in vitale sectoren het doelwit geworden van aanvallen met de Royal-ransomware, zo stelt de FBI. De aanvallers weten daarbij vooral via phishing en het gebruik van RDP (remote desktop protocol) binnen te komen. Dat meldt de Amerikaanse opsporingsdienst in een aparte **cybersecurity advisory** over de Royal-ransomware.

Onder andere ziekenhuizen, zorginstellingen, productiebedrijven, communicatieaanbieders en onderwijsinstellingen zijn het doelwit geweest. De aanvallers vragen losgeldbedragen die tot elf miljoen dollar kunnen oplopen. In twee derde van de gevallen zouden de aanvallers via phishingaanvallen zijn binnengekomen, gevolgd door RDP. Zodra de aanvallers eenmaal toegang hebben volgen ze de standaard werkwijze van ransomwaregroepen, waarbij er lateraal door het netwerk wordt bewogen en voor de uitrol van de ransomware gegevens worden gestolen.

Om dergelijke aanvallen te voorkomen doet de FBI meerdere aanbevelingen, waaronder het maken van offline, versleutelde back-ups, het uitschakelen van command-line en scripting activiteiten en rechten, het uitschakelen van ongebruikte poorten, updaten van software, toepassen van netwerksegmentatie en multifactorauthenticatie en het verplichten van beheerdersrechten voor het kunnen installeren van software.

Een van de klanten van USP Marketing Consultancy is Stadgenoot. Vanwege het datalek bij het marktonderzoeksbureau kunnen ook gegevens zijn gelekt van huurders die in het verleden voor één of meer tevredenheidsonderzoeken van

	section (2.a i), updated IOCs
06-Jun-2023	Updated Cloud versions table to include Test, updated References
07-Jun-2023	Updated steps to include removing active sessions, added CISA advisory to References, clarified language on APP_WEB_*[random]*.dll files

Entities

ContiLeaks: Chats Reveal Over 30 Vulnerabilities Used by Conti Ransomware – How Tenable Can Help

Satnam Narang | Cyber Exposure Alerts
March 24, 2022 | 10 Min Read

Private messages between Conti members uncover invaluable information about how the infamous ransomware group hijacks victims' systems.

ContiLeaks: Chats Reveal Over 30 Vulnerabilities Used by Conti Ransomware – How Tenable Can Help

Satnam Narang | Cyber Exposure Alerts
March 24, 2022 | 10 Min Read

Private messages between Conti mer
about how the infamous ransomware

Initial access vulnerabilities

CVE	Description	CVSS Score	VPR
CVE-2018-13379	Fortinet FortiOS Path Traversal/Arbitrary File Read Vulnerability	9.8	9.8
CVE-2018-13374	Fortinet FortiOS Improper Access Control Vulnerability	8.8	8.4
CVE-2020-0796	Windows SMBv3 Client/Server Remote Code Execution Vulnerability ("SMBGhost")	10	10.0
CVE-2020-0609	Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability	9.8	8.4
CVE-2020-0688	Microsoft Exchange Validation Key Remote Code Execution Vulnerability	8.8	9.9
CVE-2021-21972	VMware vSphere Client Remote Code Execution Vulnerability	9.8	9.5
CVE-2021-21985	VMware vSphere Client Remote Code Execution Vulnerability	9.8	9.4
CVE-2021-22005	VMware vCenter Server Remote Code Execution Vulnerability	9.8	9.6
CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability ("ProxyLogon")	9.8	9.9

ContiLeaks: Chats Reveal Over 30 Vulnerabilities Used by Conti Ransomwa How Tenable Can Help

Satnam Narang | Cyber Exposure Alerts
March 24, 2022 | 10 Min Read

Private messages between Conti mer about how the infamous ransomware

Initial access vulnerabilities

CVE	Description
CVE-2018-13379	Fortinet FortiOS Path Trave
CVE-2018-13374	Fortinet FortiOS Improper A
CVE-2020-0796	Windows SMBv3 Client/Ser
CVE-2020-0609	Windows Remote Desktop (
CVE-2020-0688	Microsoft Exchange Validat
CVE-2021-21972	VMware vSphere Client Ren
CVE-2021-21985	VMware vSphere Client Ren
CVE-2021-22005	VMware vCenter Server Ren
CVE-2021-26855	Microsoft Exchange Server

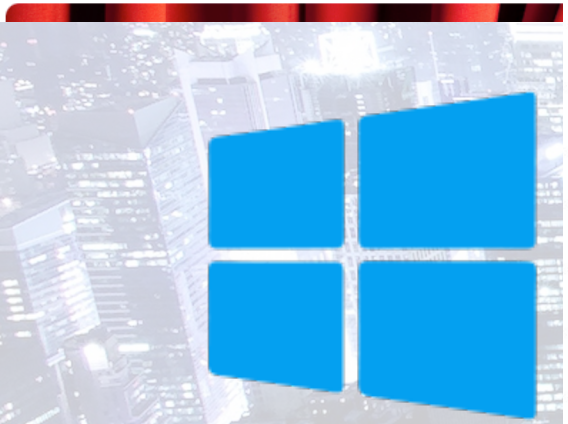
Elevation of privilege vulnerabilities

CVE	Description	CVSS Score	VPR
CVE-2015-2546	Win32k Memory Corruption Elevation of Privilege Vulnerability	6.9	9.6
CVE-2016-3309	Windows Win32k Elevation of Privilege Vulnerability	7.8	9.7
CVE-2017-0101	Windows Elevation of Privilege Vulnerability	7.8	9.7
CVE-2018-8120	Windows Win32k Elevation of Privilege Vulnerability	7	9.8
CVE-2019-0543	Microsoft Windows Elevation of Privilege Vulnerability	7.8	9.0
CVE-2019-0841	Windows Elevation of Privilege Vulnerability	7.8	9.8
CVE-2019-1064	Windows Elevation of Privilege Vulnerability	7.8	9.2
CVE-2019-1069	Windows Task Scheduler Elevation of Privilege Vulnerability	7.8	9.0
CVE-2019-1129	Windows Elevation of Privilege Vulnerability	7.8	8.9
CVE-2019-1130	Windows Elevation of Privilege Vulnerability	7.8	6.7
CVE-2019-1215	Windows Elevation of Privilege Vulnerability	7.8	9.5
CVE-2019-1253	Windows Elevation of Privilege Vulnerability	7.8	9.7
CVE-2019-1315	Windows Error Reporting Manager Elevation of Privilege Vulnerability	7.8	9.0
CVE-2019-1322	Microsoft Windows Elevation of Privilege Vulnerability	7.8	9.0
CVE-2019-1385	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability	7.8	5.9

ContiLeaks: Chats Reveal Over 30 Vulnerabilities Used by Conti Ransomwa How Tenable Can Help

Satnam Narang | Cyber Exposure Alerts
March 24, 2022 | 10 Min Read

Private messages between Conti mer about how the infamous ransomware



Initial access vulnerabilities

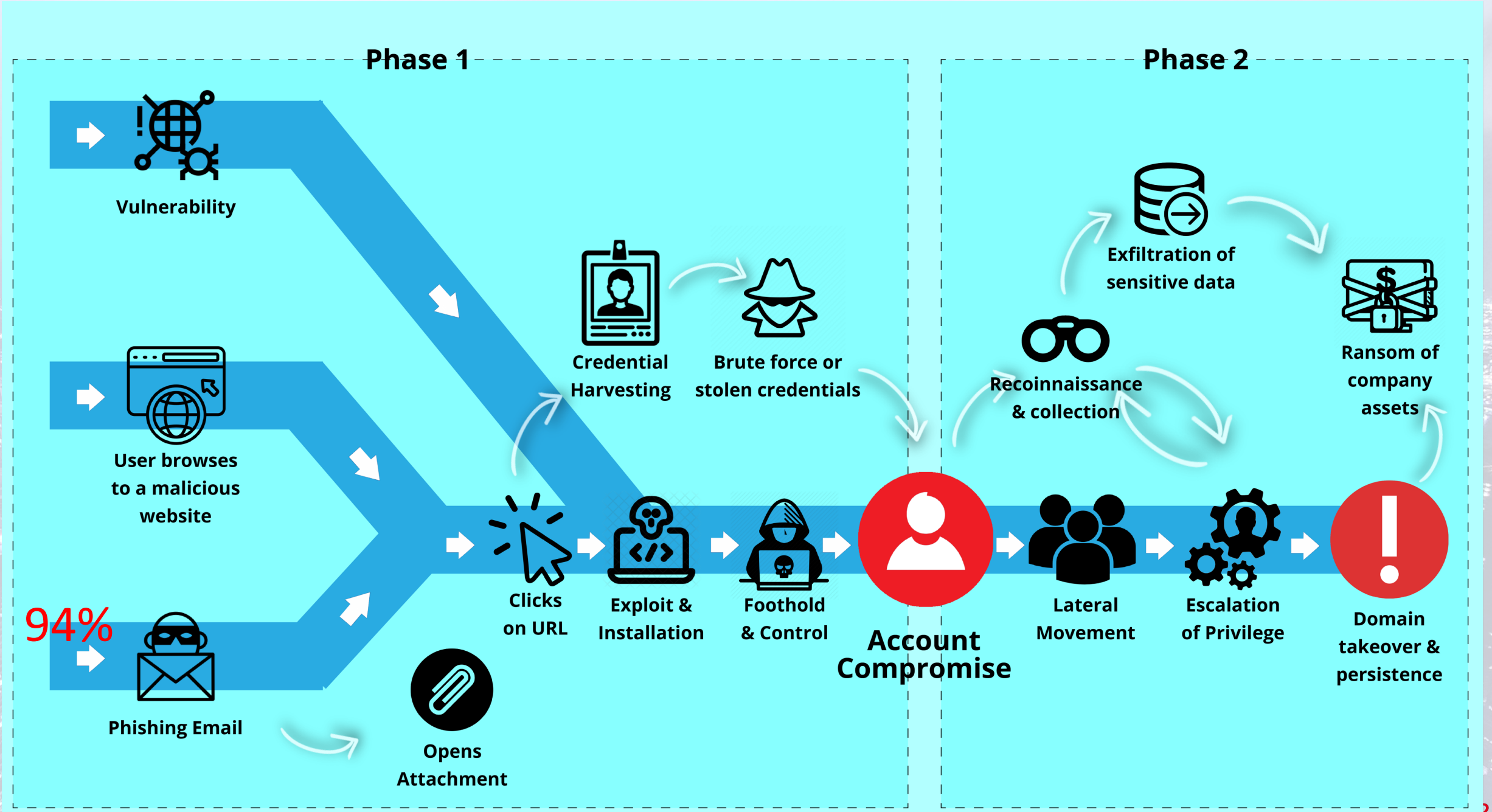
CVE	Description
CVE-2018-13379	Fortinet FortiOS Path Trave
CVE-2018-13374	Fortinet FortiOS Improper A
CVE-2020-0796	Windows SMBv3 Client/Ser
CVE-2020-0609	Windows Remote Desktop
CVE-2020-0688	Microsoft Exchange Validat
CVE-2021-[illegible]	VMware vSphere Client Rem
CVE-20[illegible]-21985	Vmware vSphere Clien[illegible]en
CVE-2021-22005	VMware vCenter Server Rer
CVE-2021-26855	Microsoft Exchange Server

Elevation of privilege vulnerabilities

CVE	Description	CVSS Score	VPR
CVE-2015-2546	Win32k Memory Corruption Elevation of Privilege Vulnerability	6.9	9.6
CVE-2016-3309	Windows Win32k Elevation of Privilege Vulnerability	7.8	9.7
CVE-2017-0101	Windows Elevation of Privilege Vulnerability	7.8	9.7
CVE-2018-8120	Windows Win32k Elevation of Privilege Vulnerability	7	9.8
CVE-2019-0543	Microsoft Windows Elevation of Privilege Vulnerability	7.8	9.0
CVE-2019-0841	Windows Elevation of Privilege Vulnerability	7.8	9.8
CVE-2019-1064	Windows Elevation of Privilege Vulnerability	7.8	9.2
CVE-2019-1069	Windows Task Scheduler Elevation of Privilege Vulnerability	7.8	9.0
CVE-2019-1129	Windows [illegible] of Privilege Vulnerability	7.8	8.9
CVE-2019-[illegible]	Windows [illegible]levation of Privilege [illegible]erability	[illegible]	6.7
CVE-2019-[illegible]	Windows [illegible]levation of Privilege [illegible]erability	[illegible].8	9.5
CVE-2019-1253	Windows Elevation of Privilege Vulnerability	7.8	9.7
CVE-2019-1315	Windows Error Reporting Manager Elevation of Privilege Vulnerability	7.8	9.0
CVE-2019-1322	Microsoft Windows Elevation of Privilege Vulnerability	7.8	9.0
CVE-2019-1385	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability	7.8	5.9

Microsoft Active Directory

CCV CYBER PENTEST · DigiTrust NEN 7510 · DigiTrust ISO 27001 · Access42 Cybersecurity


Phase 1
Phase 2
Vulnerability
User browses to a malicious website
94%
Phishing Email
Opens Attachment
Credential Harvesting
Brute force or stolen credentials
Clicks on URL
Exploit & Installation
Foothold & Control
Account Compromise
Recoinnaissance & collection
Exfiltration of sensitive data
Ransom of company assets
Lateral Movement
Escalation of Privilege
Domain takeover & persistence

How do we do it?

CCV CYBER PENTEST
NEN 7510
ISO 27001
ACCESS42 Cybersecurity

A SIEMless SOC

"**SIEMs** are now part of the problem"

Unable to identify meaningful trends, nor do they offer automated detection or response capabilities.

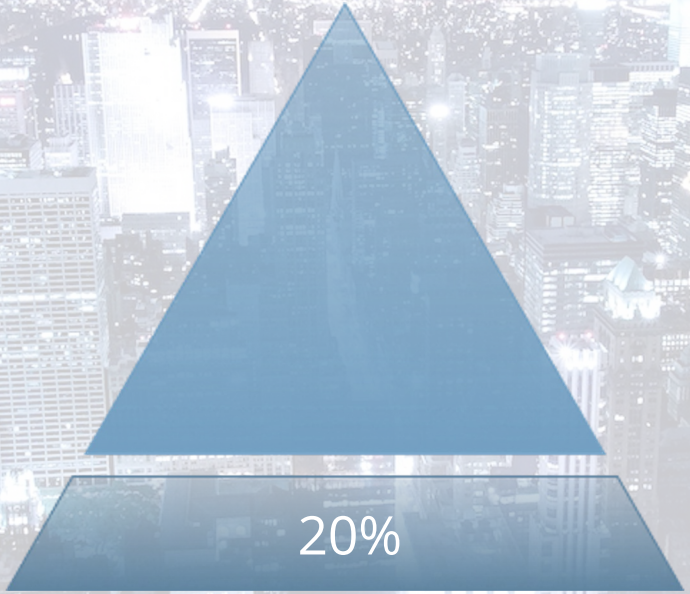
SIEM HAS BECOME OBSOLETE

- Data volumes and cost are **unmanageable,** leading to **poor security outcomes**
- Your team **plays catch up** with detection rule-writing
- Analysts are **drowning in noise**
- Incident investigation and triage are **too lengthy and cumbersome**

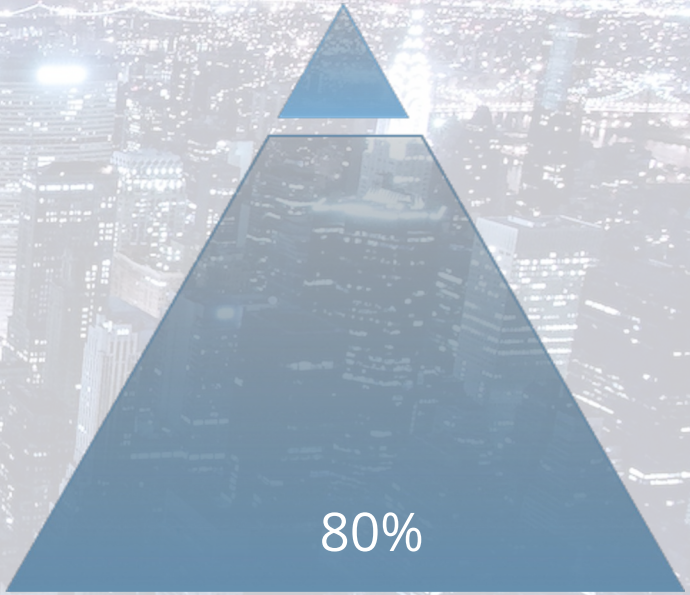
Automated Threat Detection

Bespoke use cases

Common use cases



Without Access42



With Access42

Move Beyond SIEM

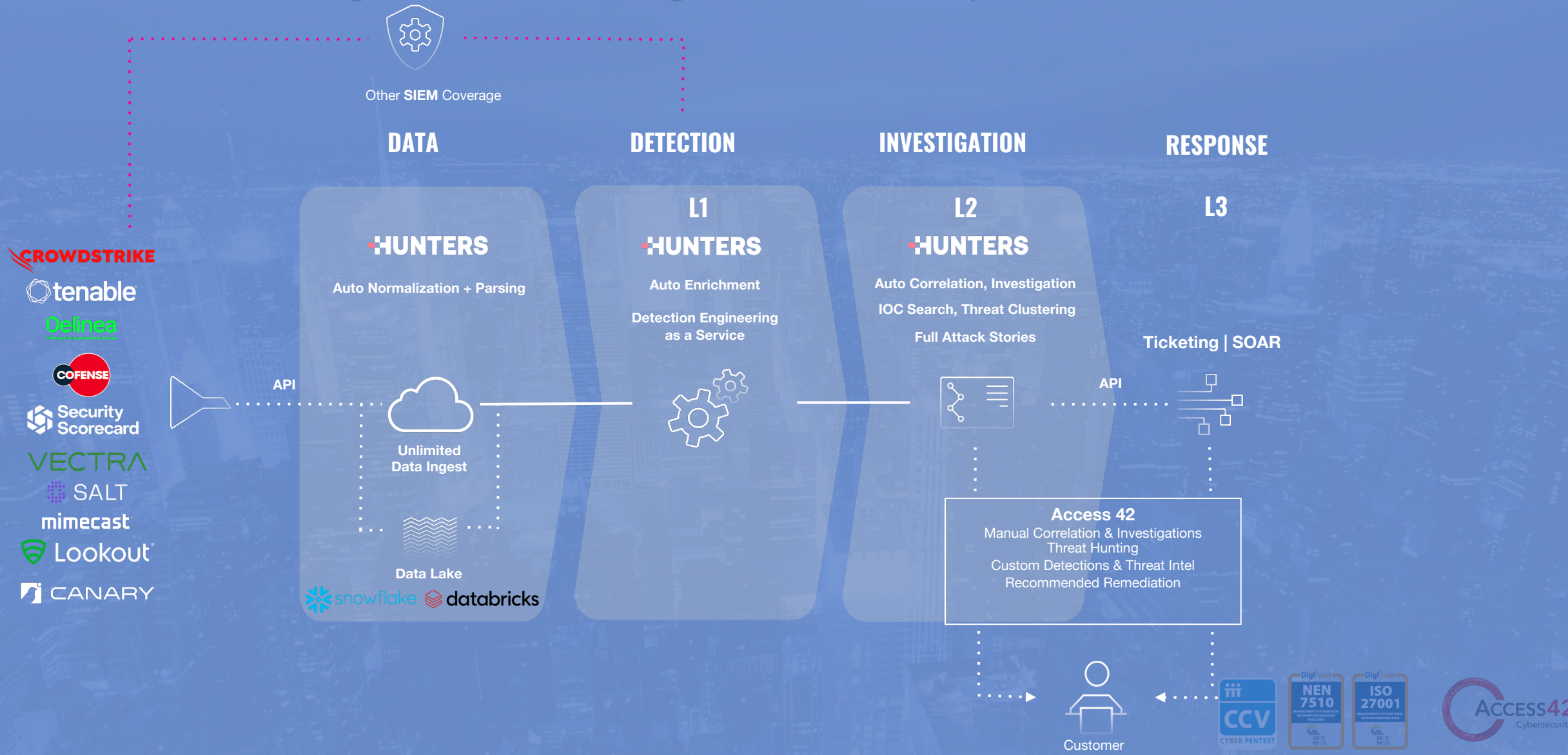
Move Beyond SIEM

- CyberTIM – Managed Security Services (SOC)
  - Awareness
  - Email security and triage
  - Detection of vulnerabilities (IT, Cloud, (I)OT)
  - Managed Detection and Response
    - Endpoint Protection and EDR
    - Network Detection and Response
  - API Security
  - Privileged Account Management
  - AD Security
  - Third Party Risk Management
  - Automating detection, investigation and response

Automation across the SOC workflow

The Access42 & Hunters Architecture

From data through detection, investigation and into response



24/7 eyes on the screen

CCV CYBER PENTEST

DigiTrust NEN 7510

DigiTrust ISO 27001

ACCESS42 Cybersecurity

Key Takeaways

- Strengthen the overall security culture by supporting employees
- Invest in education and training of tomorrow’s cybersecurity professionals
- Prevent harmful (multi-channel) messages such as emails from reaching end users
- Checking in on supplier performance and tracking changes in the relationship
- Get insight in your vulnerabilities: IT, OT, Apps, API's etc.
- Prioritize based on risk, including context.
- Protect endpoints with EDR, but also provide network visibility with NDR.
- Strengthen AD security, continuously audit permissions of accounts
- Automate your incident response - Move Beyond SIEM: Reduce Risk, Complexity, and Cost for the SOC
- Tabletop exercises

www.cybersecuritysummit.nl

CCV CYBER PENTEST
DigiTrust NEN 7510
DigiTrust ISO 27001
ACCESS42 Cybersecurity