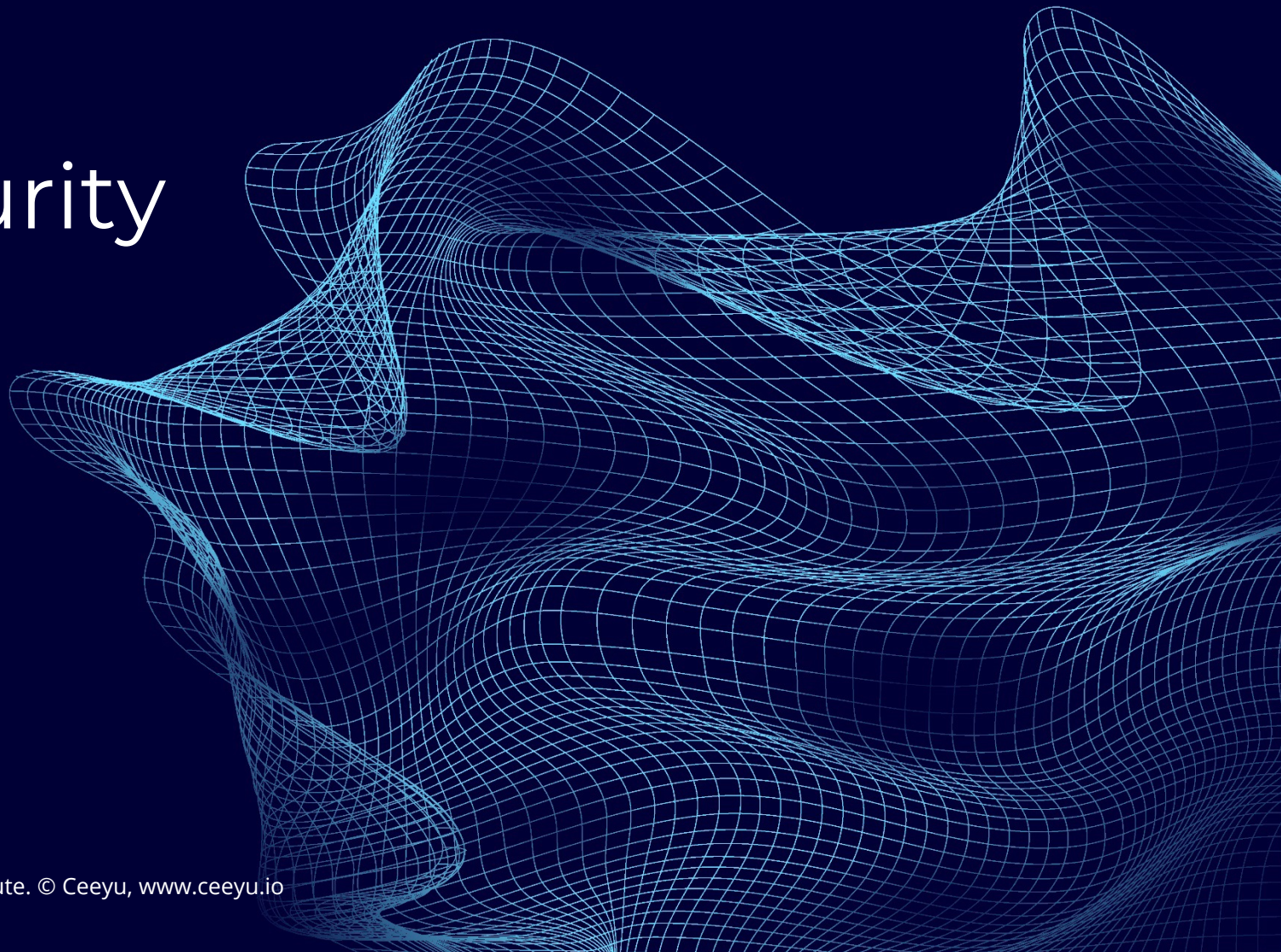
Ceeyu

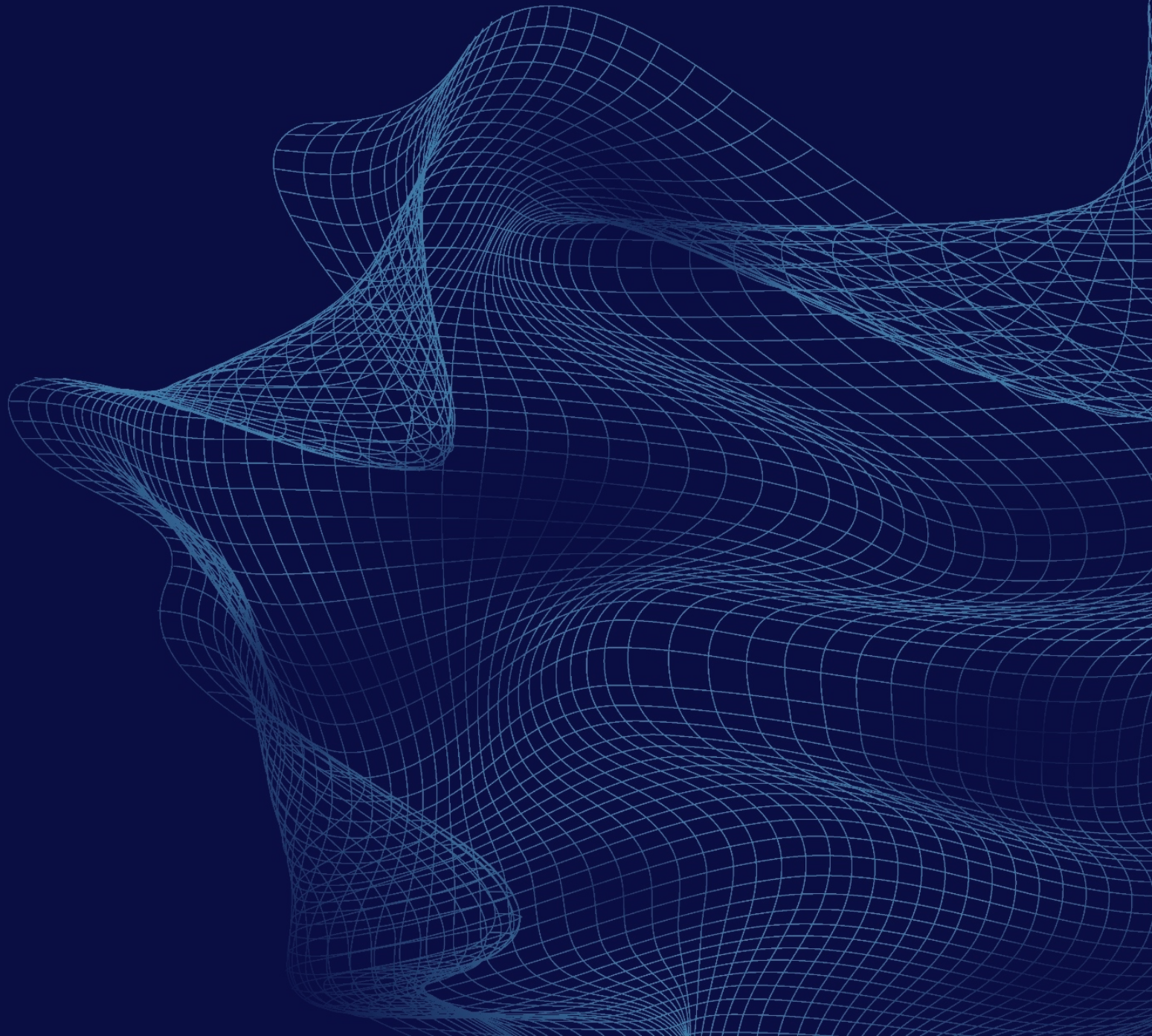
Hoe uw Cybersecurity verbeteren met Ceeyu



11 januari 2024

Company Private & Confidential, Ceeyu.io 2024. Do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Wie is Ceeyu?



Cybersecurity oplossingen worden opgedeeld in 5 domeinen

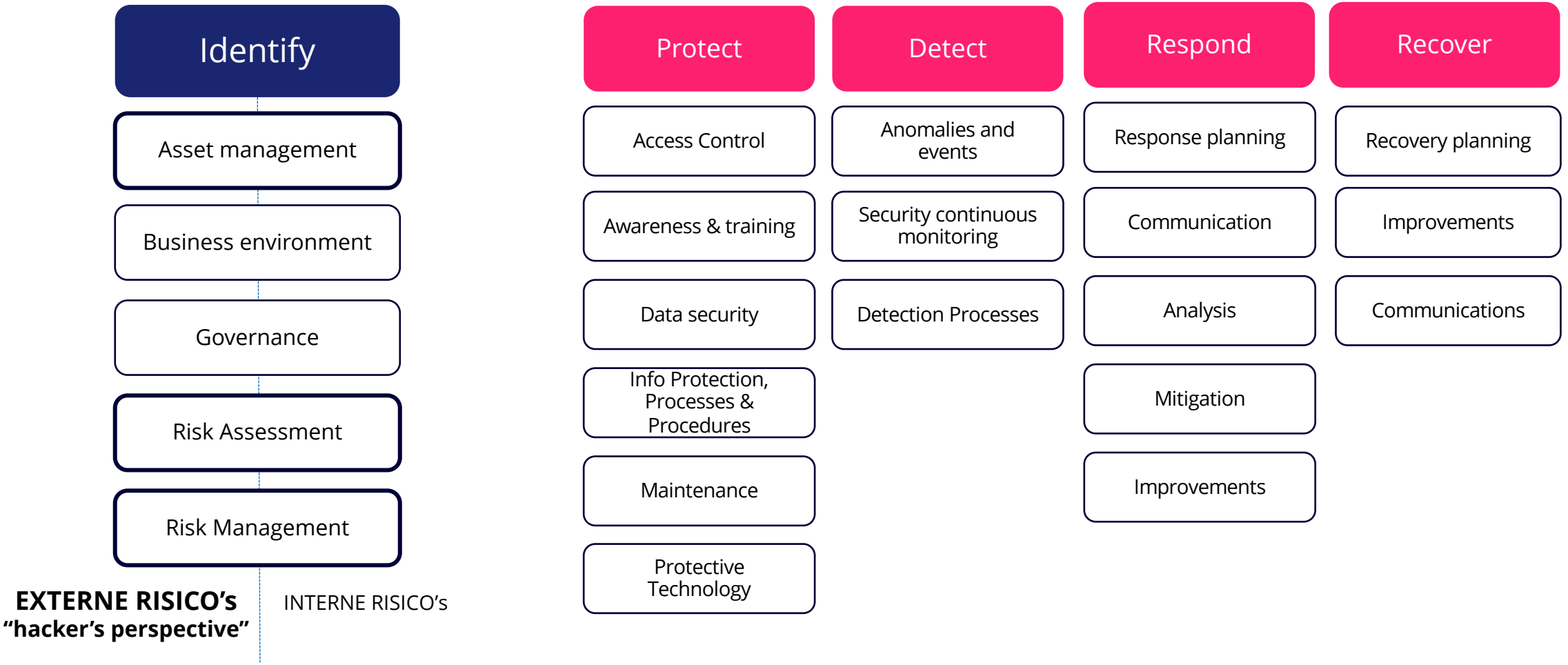
Identify	Protect	Detect	Respond	Recover
Asset management	Access Control	Anomalies and events	Response planning	Recovery planning
Business environment	Awareness & training	Security continuous monitoring	Communication	Improvements
Governance	Data security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection, Processes & Procedures		Mitigation	
Risk Management	Maintenance		Improvements	
	Protective Technology			

NIST Cybersecurity Framework

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Ceeyu helpt bedrijven bij het identificeren van externe beveiligingsrisico's

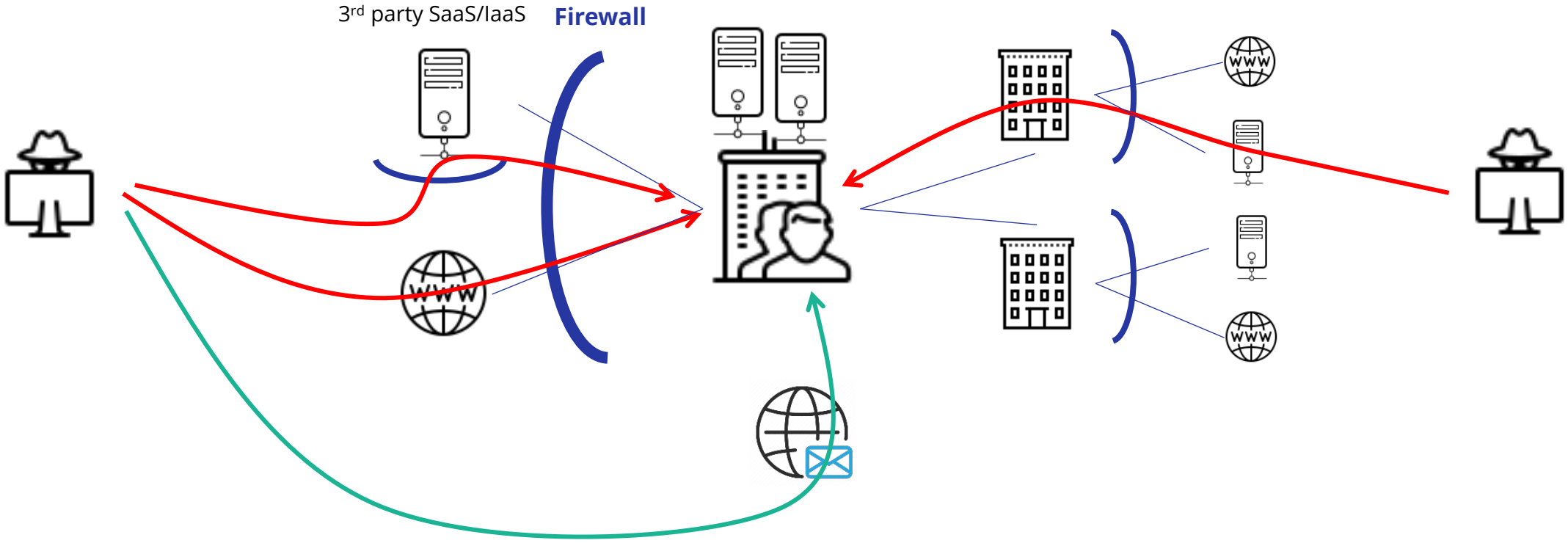


Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Het identificeren van risico's gebeurt in twee domeinen

EIGEN BEDRIJF

KRISTISCHE LEVERANCIERS



- Digital footprint mapping
- Attack surface management
- Security assessment/ratings
- External vulnerability management

- Pen testing

- Anti-virus
- Identity management
- Surveillance
- Internal vulnerability management
- IT asset management

- Third party risk management (questionnaire based)
- Security assessments/ratings (automated)

- Security audit

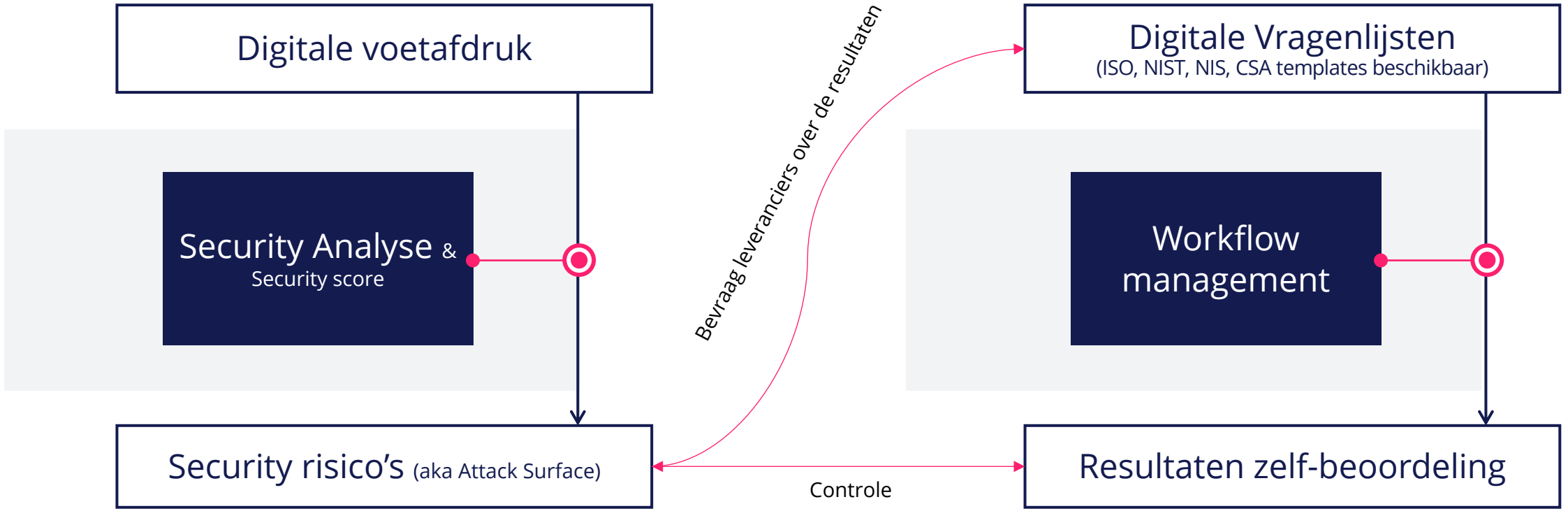
Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Hiervoor gebruikt Ceeyu twee methodes

Geautomatiseerde risico analyse

Op vragenlijsten gebaseerde analyse



Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

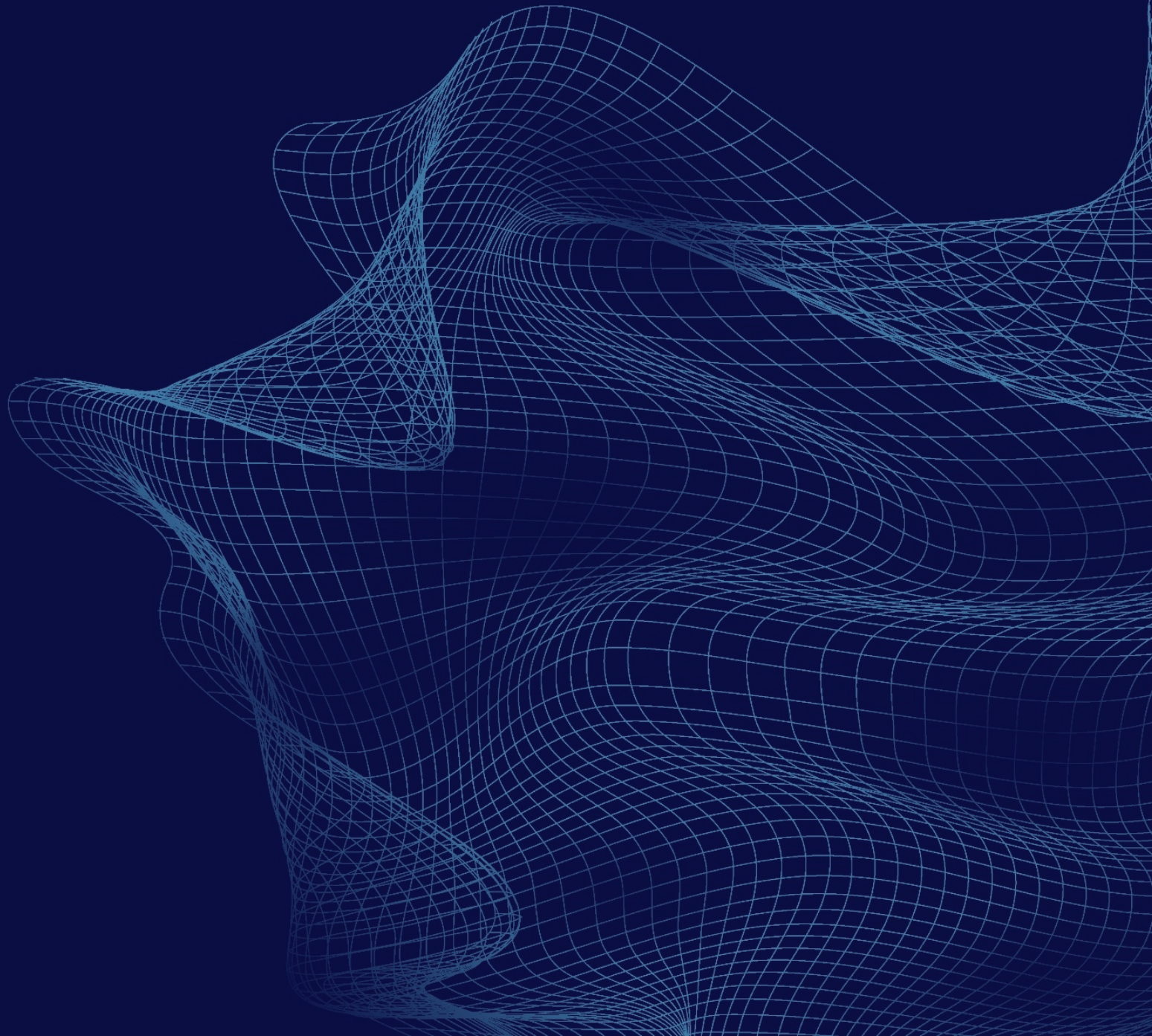
Deze bedrijven vertrouwen reeds op Ceeyu voor hun beveiliging

KONINKRIJK BELGIË
Federale Overheidsdienst
Buitenlandse Zaken,
Buitenlandse Handel en
Ontwikkelingssamenwerking

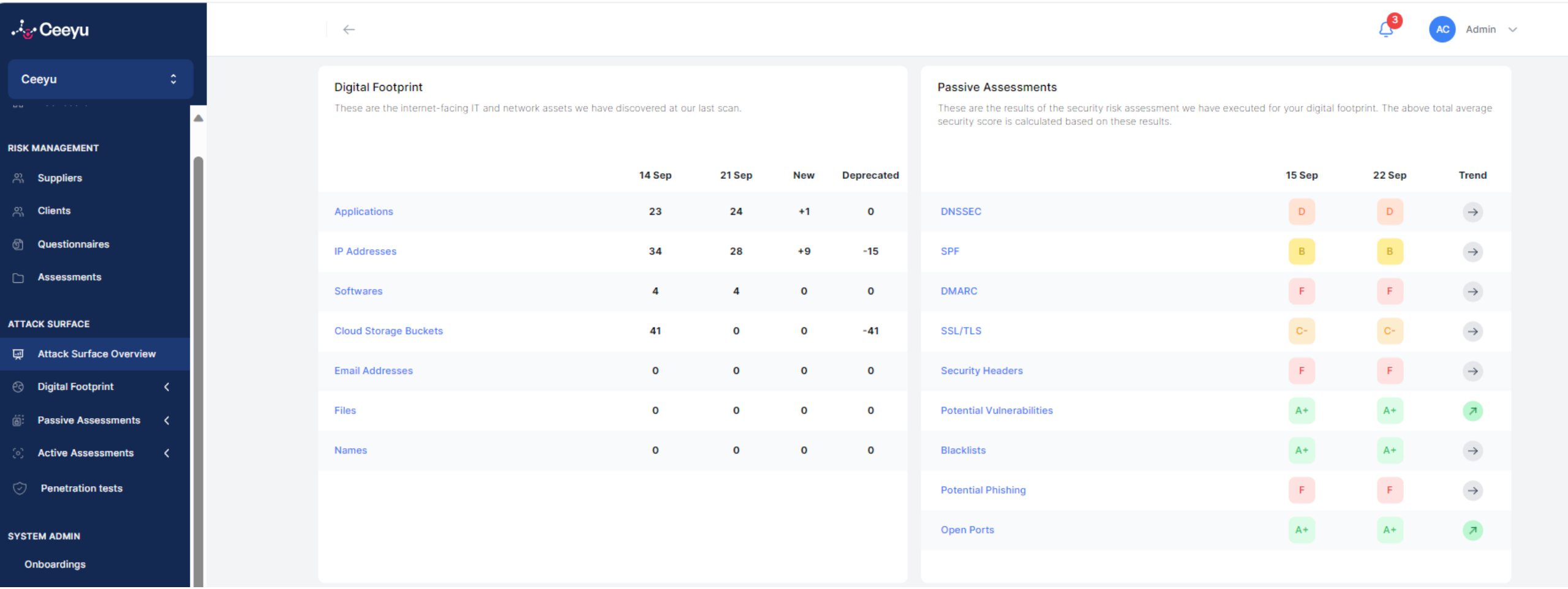
Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Hoe maakt Ceeyu uw cyberbeveiliging beter?



Overzicht van uw bedrijf, vanuit het perspectief van een hacker



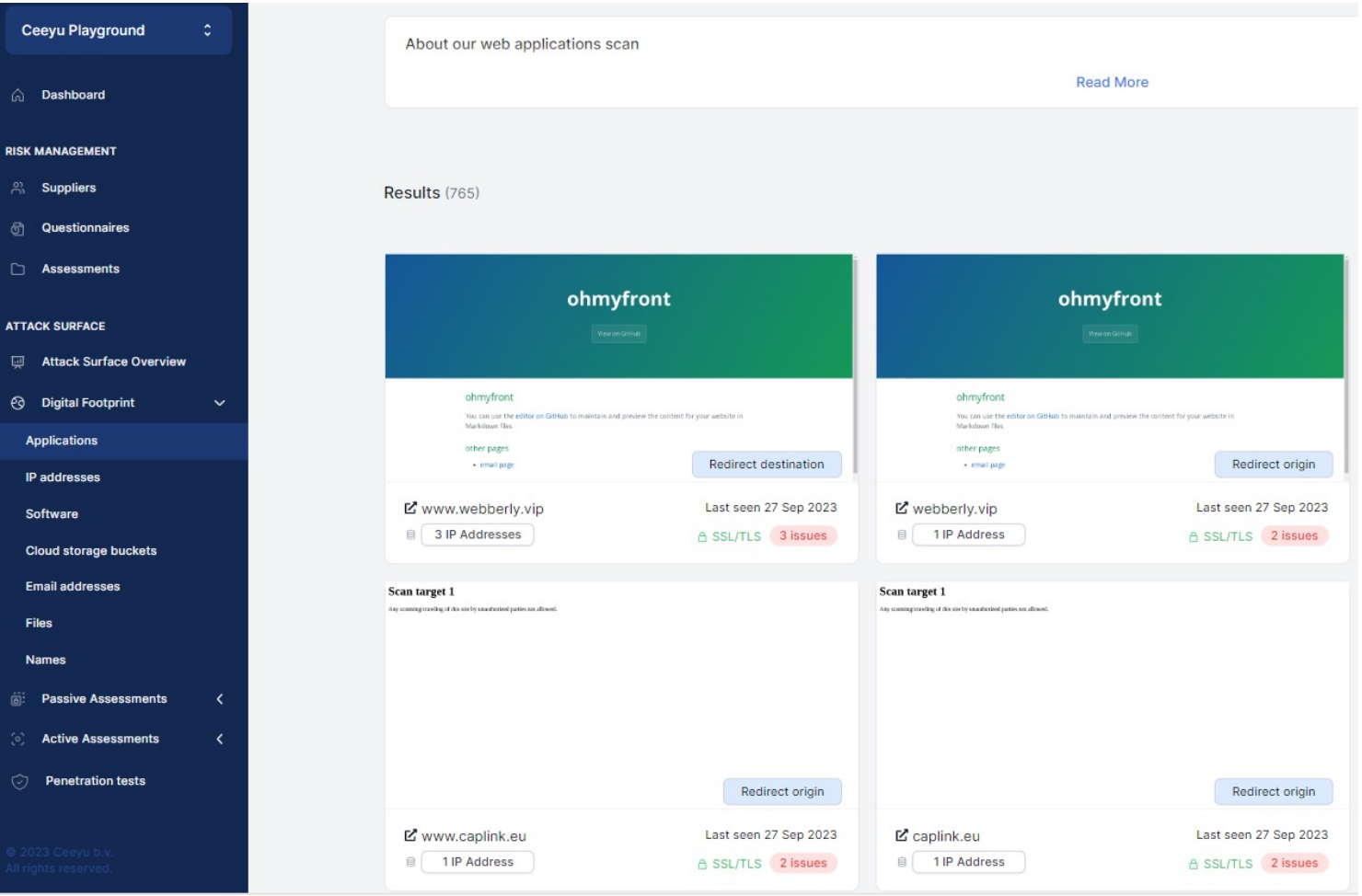
= Wat is extern zichtbaar?

= Hoe goed is wat extern zichtbaar is, beveiligd?

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Applications



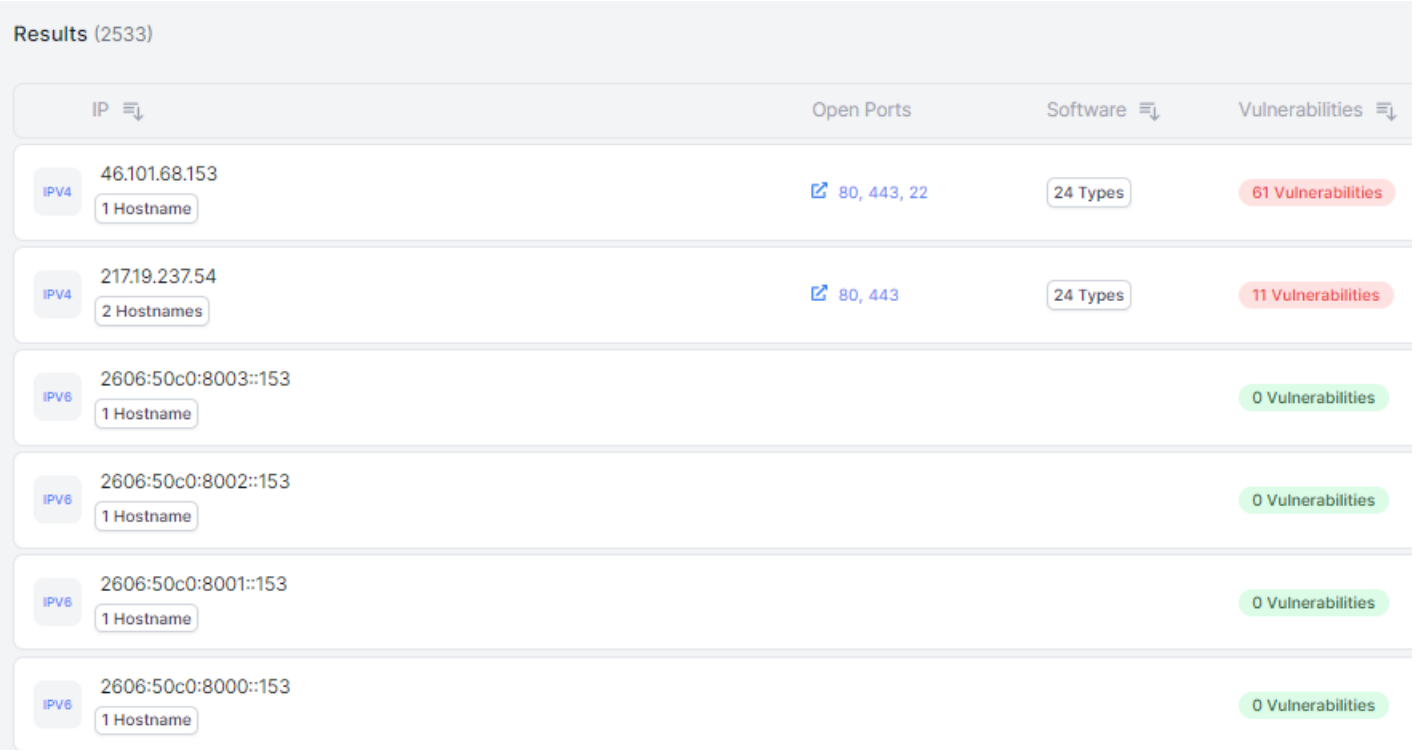
De verschillende toepassingen gelinkt aan uw domein (bv *Ceeyu.be*) die verbonden zijn met Internet, gekenmerkt door een host name (bv *mail.Ceeyu.be*).

- Website
- Webmail
- File server/Cloud storage (bv dropbox)
- Marketing landing pagina
- Klantendienst omgeving
- ….

Dit is het vertrekpunt voor hackers. Via applicaties vinden ze alle verdere info die ze nodig hebben om zwakke plekken te vinden. Zie volgende slides.

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

IP adresses



Uw applicaties gebruiken IP adressen (= post adressen van het internet) om bereikbaar te zijn voor gebruikers via het Internet.

In de DNS worden hostnames (bv mail.Ceeyu.io, www.ceeyu.io), vertaald naar IP adressen (56.222.567.45).

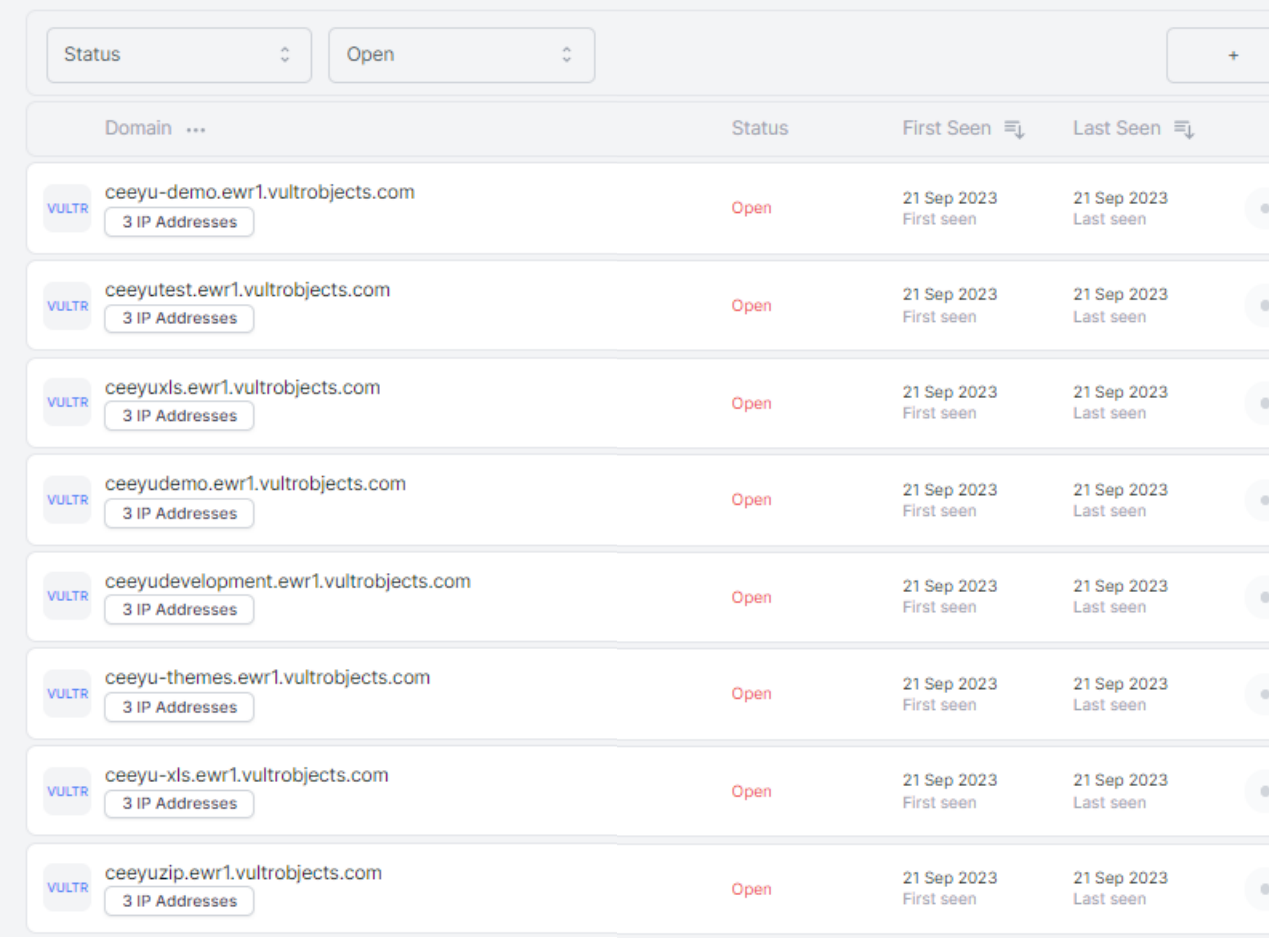
IP adressen kunnen gescand worden om te zien of er openingen zijn (= poorten) die er niet zouden moeten zijn. Te vergelijken met deuren en ramen van een huis.

Ofwel raken hackers direct binnen via een open poort, ofwel zorgt een virus (malware binnengebracht via bv. phishing) ervoor dat een deur wordt opengezet.

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Cloud storage buckets



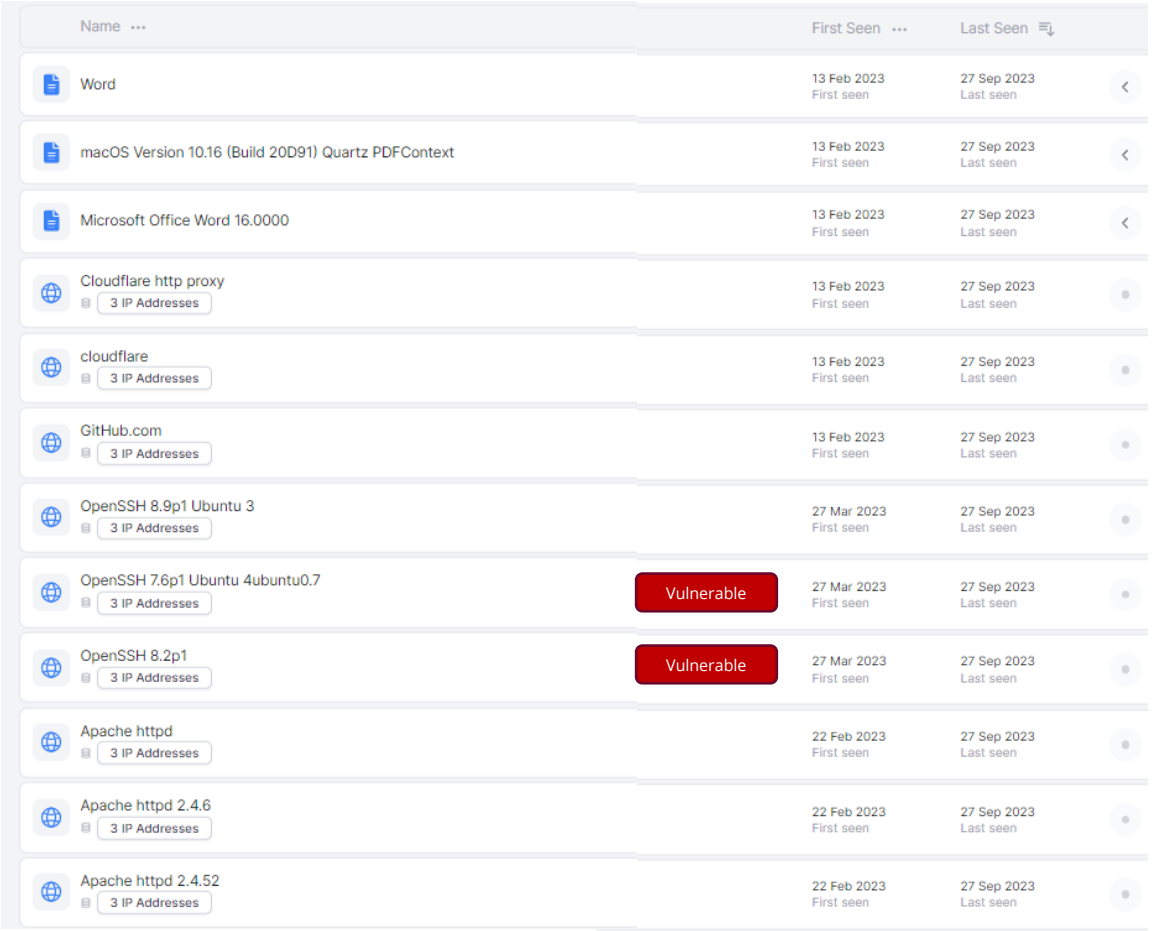
Een cloud storage bucket is een online plaats waar applicaties hun data (zoals files, video's, fotos, enz.) opslaan. Bij een website zijn die cloud storage buckets publiek toegankelijk, maar voor andere toepassingen is dat soms niet zo.

Net zoals poorten van servers soms niet open mogen staan, moeten bepaalde cloud storage buckets niet open staan (bv omdat ze in applicatie staan met authenticatie), zoniet kan confidentiele informatie gewoon vrij toegankelijk zijn.

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Software



Name		First Seen	Last Seen
Word		13 Feb 2023 First seen	27 Sep 2023 Last seen
macOS Version 10.16 (Build 20D91) Quartz PDFContext		13 Feb 2023 First seen	27 Sep 2023 Last seen
Microsoft Office Word 16.0000		13 Feb 2023 First seen	27 Sep 2023 Last seen
Cloudflare http proxy 3 IP Addresses		13 Feb 2023 First seen	27 Sep 2023 Last seen
cloudflare 3 IP Addresses		13 Feb 2023 First seen	27 Sep 2023 Last seen
GitHub.com 3 IP Addresses		13 Feb 2023 First seen	27 Sep 2023 Last seen
OpenSSH 8.9p1 Ubuntu 3 3 IP Addresses		27 Mar 2023 First seen	27 Sep 2023 Last seen
OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 3 IP Addresses	Vulnerable	27 Mar 2023 First seen	27 Sep 2023 Last seen
OpenSSH 8.2p1 3 IP Addresses	Vulnerable	27 Mar 2023 First seen	27 Sep 2023 Last seen
Apache httpd 3 IP Addresses		22 Feb 2023 First seen	27 Sep 2023 Last seen
Apache httpd 2.4.6 3 IP Addresses		22 Feb 2023 First seen	27 Sep 2023 Last seen
Apache httpd 2.4.52 3 IP Addresses		22 Feb 2023 First seen	27 Sep 2023 Last seen

Door berichten naar applicaties te sturen, en het antwoord te analyseren kan soms de software waarmee de applicatie “gemaakt” is achterhaald worden.

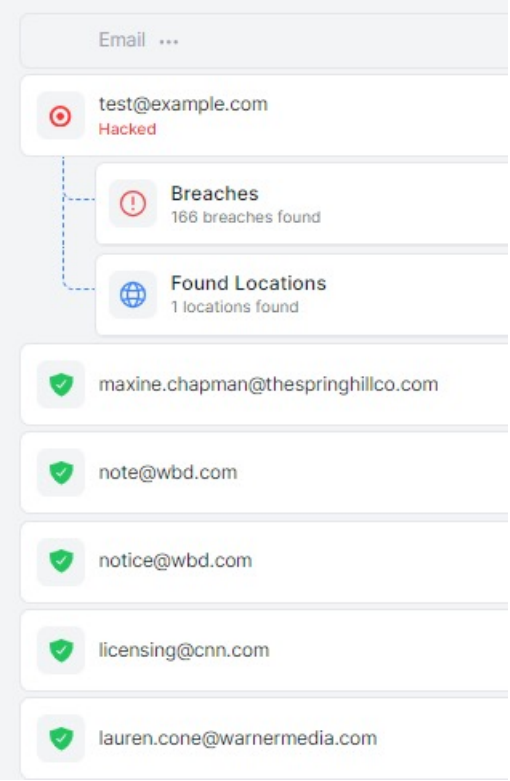
Het is belangrijk deze info zo goed mogelijk te verbergen, of ervoor te zorgen dat de software de laatste versie heeft (die minder kwetsbaar is).

Vaak gebeurt een aanval door het uitbuiten van een fout in een software programma (vulnerability). Deze fout wordt door een hacker gebruikt, ofwel rechstreeks, ofwel via malware, om data te stelen of een applicatie te blokkeren.

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Email addresses



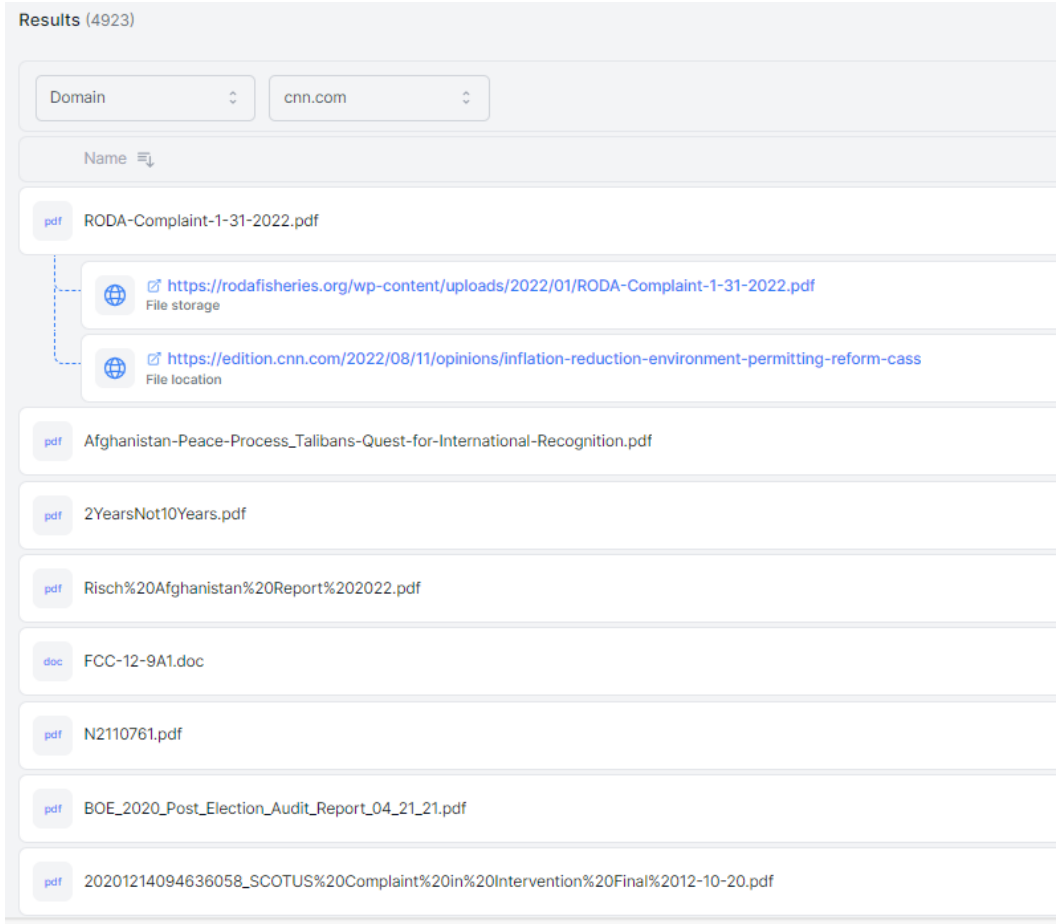
Hier vind je email adressen van je bedrijf die vindbaar zijn in de Applications. We checken of deze email adressen bekend zijn in “password breach databases”, dwz of de combinatie email adres en paswoord reeds door een hacker publiek gemaakt zijn.

Een hacker kan deze email en paswoord combinaties proberen in allerhande applicaties (gmail, Hotmail, linkedin, enz) om gegevens te stelen, of om een phishing email credibeler te doen lijken.

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Files



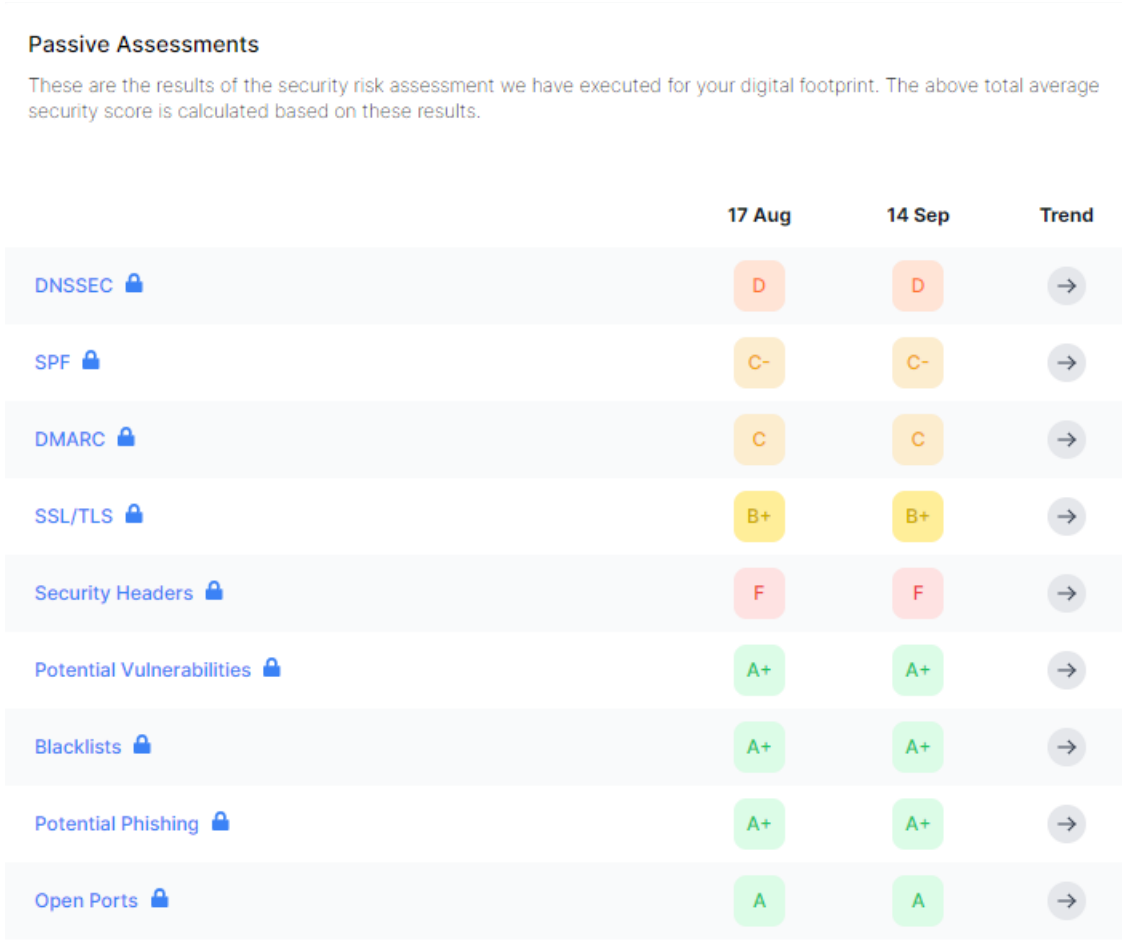
Hier vind je de bestanden die we terugvinden in uw voetafdruk, en die dus publiek toegankelijk zijn.

Het loont te moeite om hier af en toe eens een kijkje naar te nemen om er zeker van te zijn dat er geen bestanden tussen staan die niet vindbaar zouden moeten zijn.

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Evaluatie van uw beveiliging



Passive Assessments

These are the results of the security risk assessment we have executed for your digital footprint. The above total average security score is calculated based on these results.

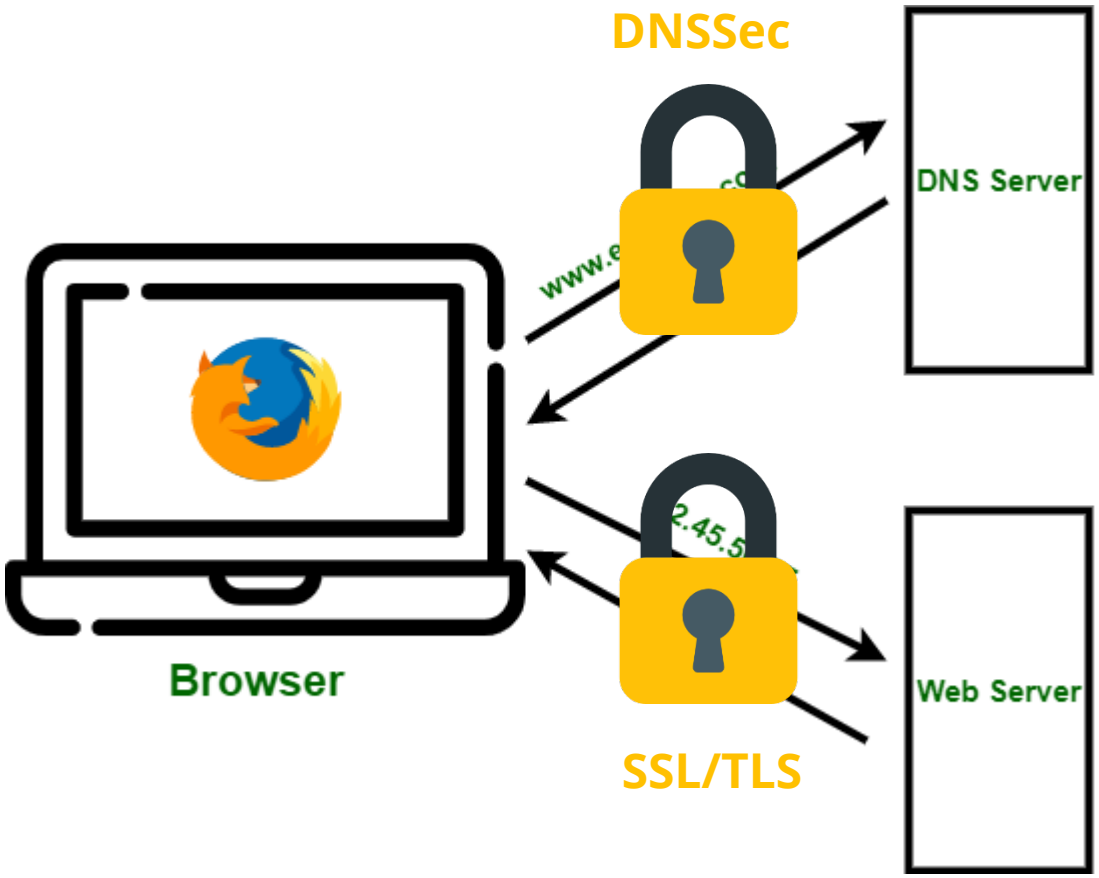
	17 Aug	14 Sep	Trend
DNSSEC	D	D	→
SPF	C-	C-	→
DMARC	C	C	→
SSL/TLS	B+	B+	→
Security Headers	F	F	→
Potential Vulnerabilities	A+	A+	→
Blacklists	A+	A+	→
Potential Phishing	A+	A+	→
Open Ports	A	A	→

- **Score**: A (91-100, zeer goed) => F (< 40, zeer slecht)
- **Totaal score**: gewogen gemiddelde van individuele scores (bv open ports = hoge impact, Potential phishing = lage impact)
- **Trend**: Vergelijking tussen individuele score laatste en voorlaatste scan
- **MINDER GOEDE SCORE (vanaf C)**: laat een IT expert dit domein bekijken! Zeker voor SPF/DMARC, SSL/TLS, Potential vulnerabilities en open ports.

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

DNSSec



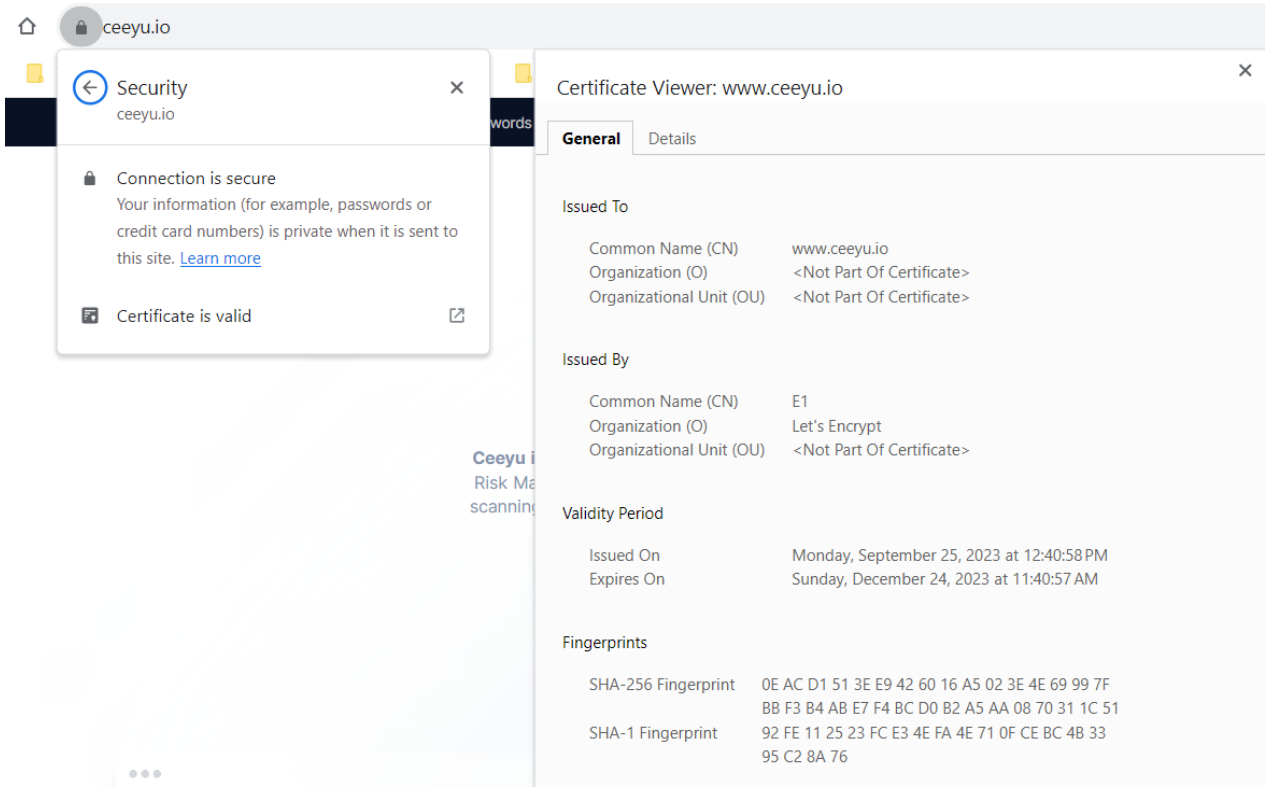
Met DNSsec bewijs je dat een domeinnaam (en de instellingen) echt van jou is, in de DNS (vertaalt domeinamen in IP adressen) .

Door zwakheden in de DNS kan een hacker een domein omleiden naar zijn IP adres, en niet dat van jouw applicatie.

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

SSL/TLS



Met SSL/TLS bewijs je dat de domein/host naam die je voor een applicatie gebruikt gebruikt echt van jou is, in de applicatie zelf.

Daarnaast zorg je met SSL/TLS dat alle communicatie tussen de applicatie en de gebruiker geencrypteerd is (en niet onderschept en gelezen kan worden).

Een SSL/TLS certificaat kan door om het even wie worden uitgegeven, dus ook door een hacker zelf. Eigenlijk moet je kijken naar de betrouwbaarheid van de uitgever, maar wie doet dat?

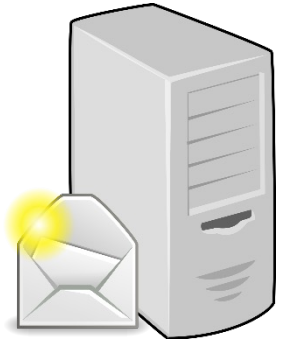
Ceeyu

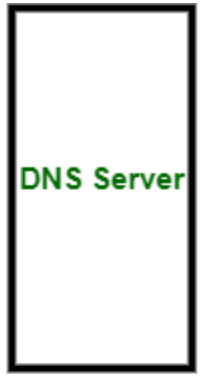
Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

SPF/DMARC

Jouw email server (Google, Microsoft 365, Combell,...)

Ontvangende email server





SPF: Komt deze email van een geautoriseerde server voor emails van @ceeyu.be?

DMARC: Wat moet er gebeuren met email die niet voldoet aan wat er in SPF (of DKIM) staat?

Als je geen SPF record hebt in de DNS, dan kan een phisher onbeperkt jouw domein gebruiken om emails te sturen.

Als je geen DMARC record hebt, dan kan een phisher jouw domain gebruiken om emails te sturen, al zal hij hier en daar geblokkeerd worden.

Als SPF en DMARC niet goed geconfigueerd zijn, dan kan “goede” email toch in de SPAM folder terechtkomen en is de kans vele malen groter dat een spam wel bij de gebruiker terechtkomt.

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Security headers

▼ General

Request URL: https://www.jetnexus.com/
Request Method: GET
Status Code: 200 OK
Remote Address: 104.47.140.215:443

▼ Response Headers view source

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: Keep-Alive
Content-Length: 26834
Content-Type: text/html; charset=UTF-8
Date: Wed, 13 Apr 2016 09:13:00 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
Link: <https://www.jetnexus.com/>; rel=shortlink
Link: <https://www.jetnexus.com/wp-json/>; rel="https://api.w.org/"
Pragma: no-cache
Set-Cookie: _icl_current_language=en; expires=Thu, 14-Apr-2016 09:13:00 GMT; path=/
Set-Cookie: _icl_current_language=en; expires=Thu, 14-Apr-2016 09:13:00 GMT; path=/
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Vary: User-Agent, Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Pingback: https://www.jetnexus.com/xmlrpc.php
X-XSS-Protection: 1; mode=block

Security headers zijn extra informatie in een webapplicatie die de kans op het “kapen” van een sessie verder verkleint.

Zeker belangrijk voor ecommerce en beveiligde toepassingen! Minder voor websites.

Hackers kunnen, zonder deze bescherming, een bezoek aan een applicatie (“sessie”) overnemen en leiden naar een zeer gelijkaardige website om daar dan gegevens van je te vragen en te stelen.

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Potential vulnerabilities

Hostnames

ns.mybns.com

Ports

PORT NUMBER	STATE	SERVICE NAME	SERVICE PRODUCT
53	Open	domain	PowerDNS Authoritative Server 4.6.2
80	Open	http	Apache httpd 2.4.41
443	Open	https	Gunicorn 20.0.4

Het Ceeyu platform geeft weer hoeveel kwetsbaarheden (theoretisch) aanwezig zijn in een applicatie op basis van de ZICHTBARE software.

Het eindpunt van zowat elke “hack” is een fout in software die door een applicatie wordt gebruikt, uit te buiten.

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES | SEARCH AND STATISTICS

Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Keyword (text search): cpe:2.3:a:apache:http_server:2.4.41:*:*:*:*:*:*:*
- CPE Name Search: true

There are **51** matching records.
Displaying matches **1** through **20**.

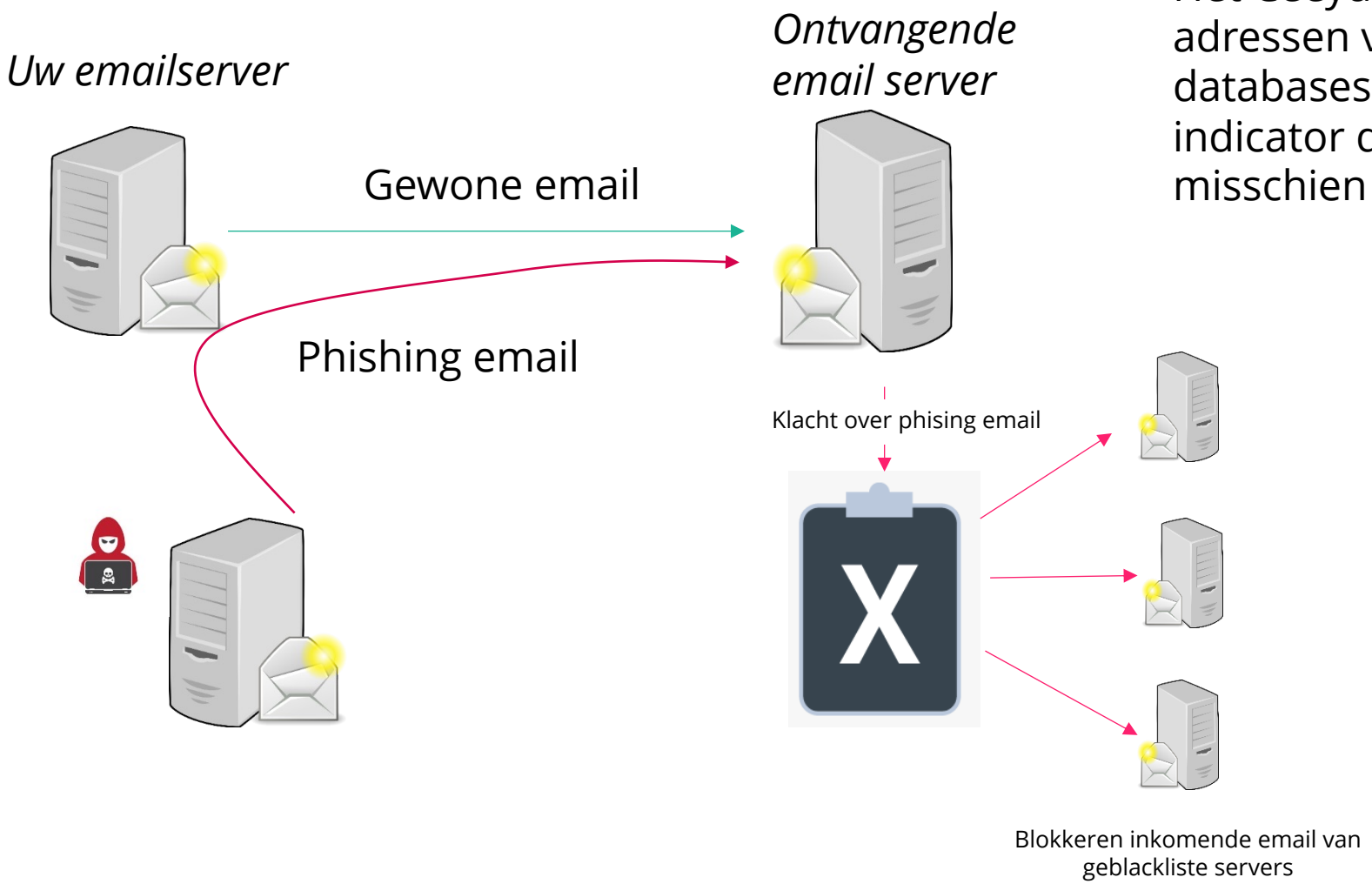
1 2 3 > >>

Vuln ID	Summary	CVSS Severity
CVE-2023-27522	HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client. **Published:** March 07, 2023; 11:15:09 am -0500	*V3.1:* 7.5 HIGH *V2.0:*(not available)
CVE-2023-25690	Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server. **Published:** March 07, 2023; 11:15:09 am -0500	*V3.1:* 9.8 CRITICAL *V2.0:*(not available)

Ceeyu

Blacklists

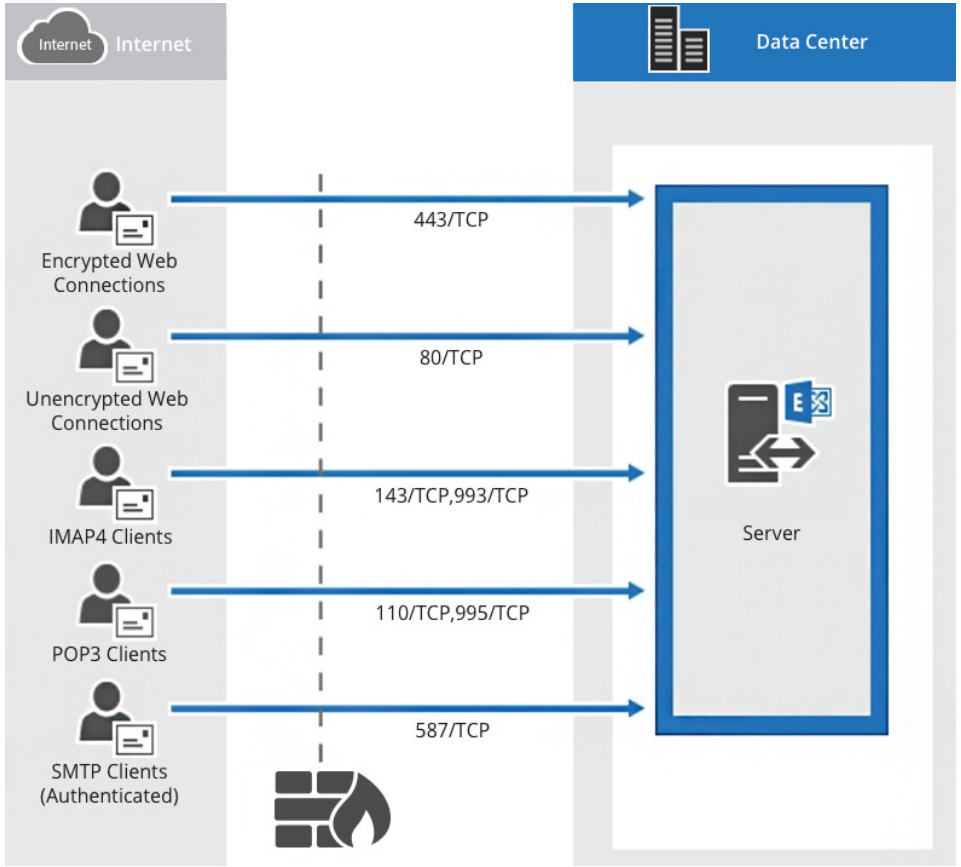
Voorbeeld



Het Ceeyu platform checkt of uw IP adressen voorkomen in blacklist databases. Zoja, dan is dat een indicator dat u gehackt bent, en het misschien nog niet weet....

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Open ports



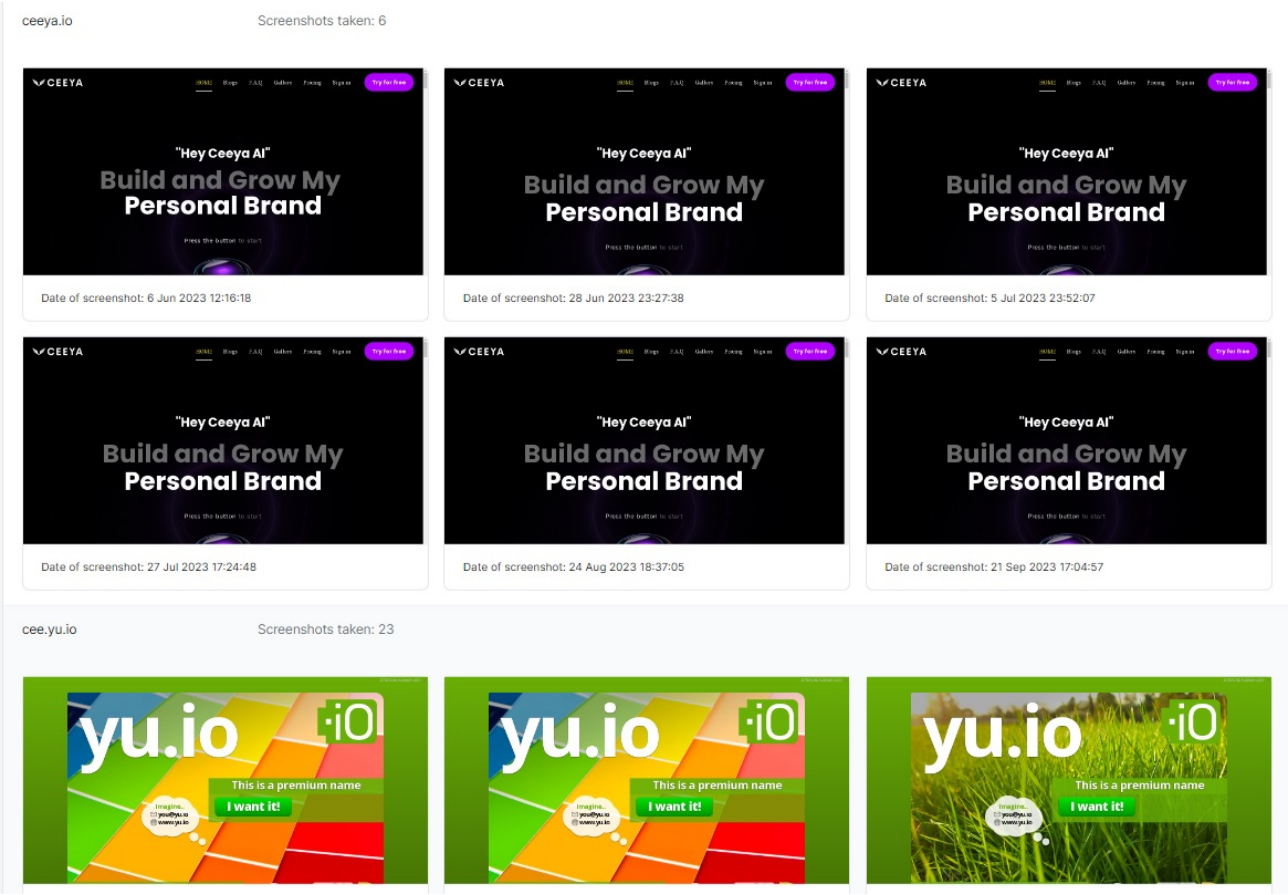
Het Ceeyu platform geeft aan welke poorten van uw applicaties bereikbaar zijn van buitenaf. Als er poorten zijn die normaal gezien niet zouden moeten openstaan (afhankelijk van de applicatie) dan wordt dat aangegeven.

Open poorten in een applicatie voor hackers, zijn zoals open deuren en ramen in een huis voor inbrekers. In het gemakkelijkste scenario wordt via de open poort uw applicatie gebruikt voor aanvallen op andere doelen = andere bedrijven).

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Potential Phishing



Het Ceeyu platform zoekt of er domeinen zijn die lijken op dat van uw bedrijf, met een website. Van de website wordt een screenshot genomen.

Hoe meer gelijkaardige domeinen in gebruik, hoe groter het risico.

Hackers maken een website die lijkt op die van u, en leiden bezoekers via phishing email naar deze valse website. Hoe meer de email, website (incl domein) op die van u lijkt, hoe groter de kans op succes!

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Dienstverlening

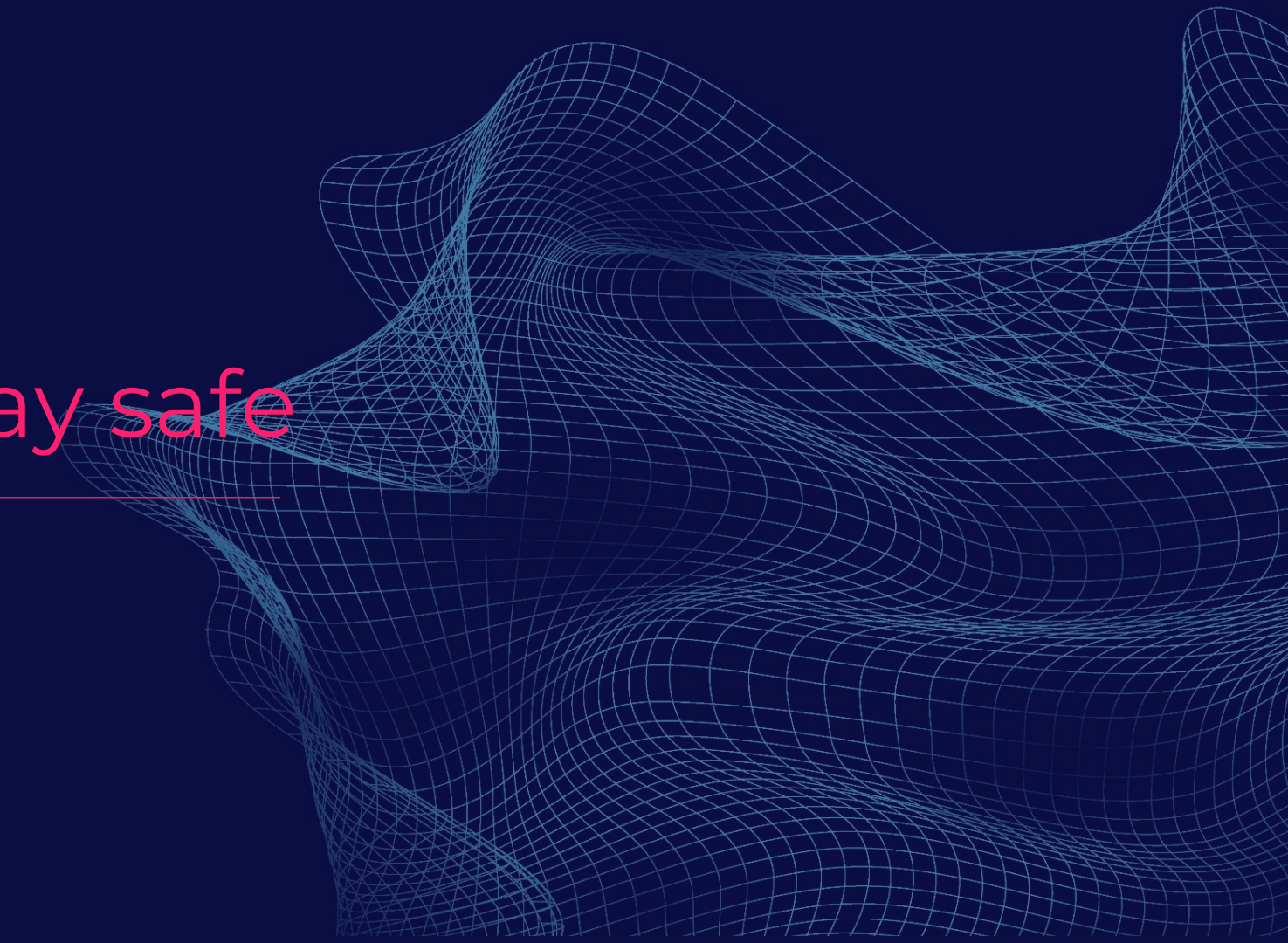
- **Gratis account**: overzicht van digitale voetafdruk en risico analyse
- Betalende account (195 €/maand) biedt **inzicht in de specifieke problemen** en hoe deze op te lossen. Daarbij is inbegrepen een scan/audit van 5 kritische **leveranciers.**
- **Actieve scans** (geautomatiseerde testen om werklijk aanwezige zwakheden in applicaties bloot te leggen)
- **Penetratietesten** (testen uitgevoerd om om werklijk aanwezige zwakheden in applicaties bloot te leggen)

Ceeyu

Confidential Information, do not reproduce or redistribute. © Ceeyu, www.ceeyu.io

Ceeyu

Because prevention is cheaper than cure



Thank you... and stay safe

CEEYU bv

hello@ceeyu.io
+32(0)15 48 14 14

www.ceeyu.io