REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE
DREJTORIA E ANALIZËS SË SIGURISË KIBERNETIKE

Fushatë Phishing
hostingseo-24

Versioni: 1.0
Datë: 03/03/2025

TLP:CLEAR

PËRMBAJTJA

LISTA E FIGURAVE

Ky raport ka kufizime dhe duhet interpretuar me kujdes!

Disa nga këto kufizime përfshijnë:

Faza e parë:
Burimet e informacionit: Raporti është bazuar në informacionet të vendosura në dispozicion në momentin e përgatitjes së tij. Ndërkohë, disa aspekte mund të jenë të ndryshme nga zhvillimet aktuale.

Faza e dytë:
Detajet e analizës: Për shkak të kufizimeve burimore, disa aspekte të skedarit keqdashës mund të mos jenë analizuar thellësisht. Çdo informacion shtesë i panjohur mund të reflektojë në ndryshime të raportit.

Faza e tretë:
Siguria e informacionit: Për të mbrojtur burimet dhe informacionet konfidenciale, disa detaje mund të jenë të zbutura ose jo të përfshira në raport. Ky vendim është marrë për të mbajtur integritetin dhe sigurinë e të dhënave të përdorura.

AKSK rezervon të drejtën për të ndryshuar, përditësuar, ose ndryshuar çfarëdo pjesë të këtij raporti pa lajmërim paraprak.

Ky raport nuk është një dokument përfundimtar.

Gjetjet e raportit bazohen në informacionin e disponueshëm gjatë kohës së hetimit dhe analizës. Nuk ka garanci në lidhje me ndryshime të mundshme apo përditësime të informacioneve të raportuara gjatë periudhës në vijim. Autorët e raportit nuk marrin përgjegjësi për përdorimin e gabuar ose pasojat e ndonjë vendimmarrjeje të bazuar në këtë raport.

Informacione Teknike

Është raportuar qarkullimi i një fushate **Phishing** në Shqipëri ku përmbajtja e email paraqet nevojën për të paguar një host të skaduar me dërgues nga domain jo legjitim ***noreply@hosting-seo24[.]com.*** Ky email phishing i është dërguar klientëve që kanë shërbime ***hosting/domain*** në të cilin kërkohet të kryhet pagesa për rinovim.

Analiza e Phishing

Nga analiza e kryer evidentohet se, dërguesi i e-mail është ***noreply@hosting-seo24[.]com*** dhe domain i krijuar enkas për fushatën, rezulton të jetë krijuar rreth një muaj më parë.

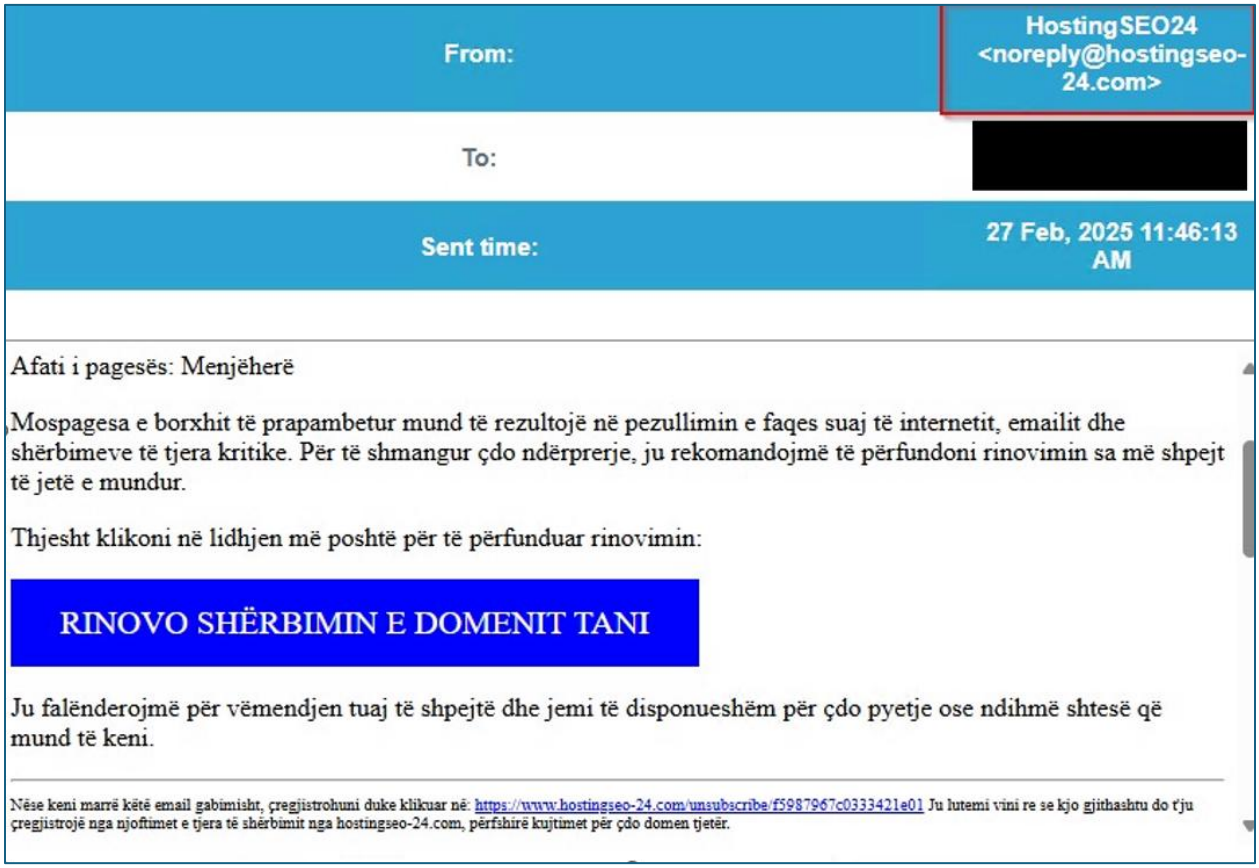


Figura 1: Përmbajtja e E-mail Phishing

Në përmbajtje të e-mail, evidentohet një buton i cili mund të klikohet, për të vazhduar me **URL** ku mund të kryhet pagesa. **URL** në vetvete është legjitime duke qenë se përdoret kompania **Stripe** për kryerje pagesash online.

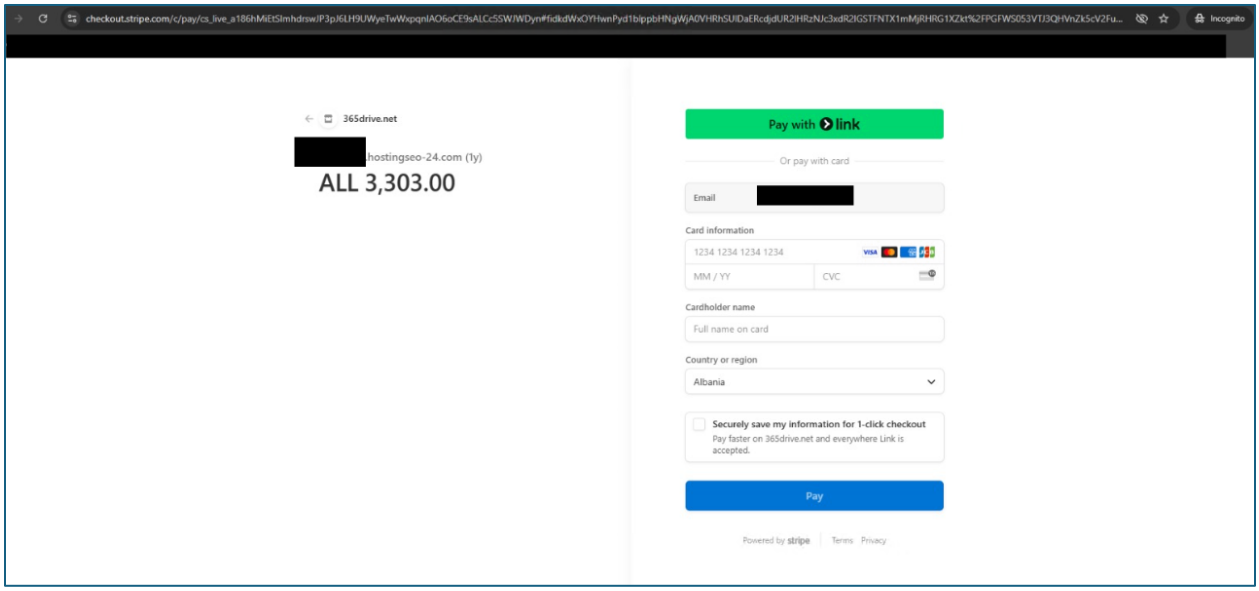


Figura 2: URL për kryerjen e pagesës

Pas klikimit të butonit për kryerjen e pagesës, evidentohet se e-mail i kompanisë është i para-plotësuar, çka paraqet dyshime për metodën e phishing.

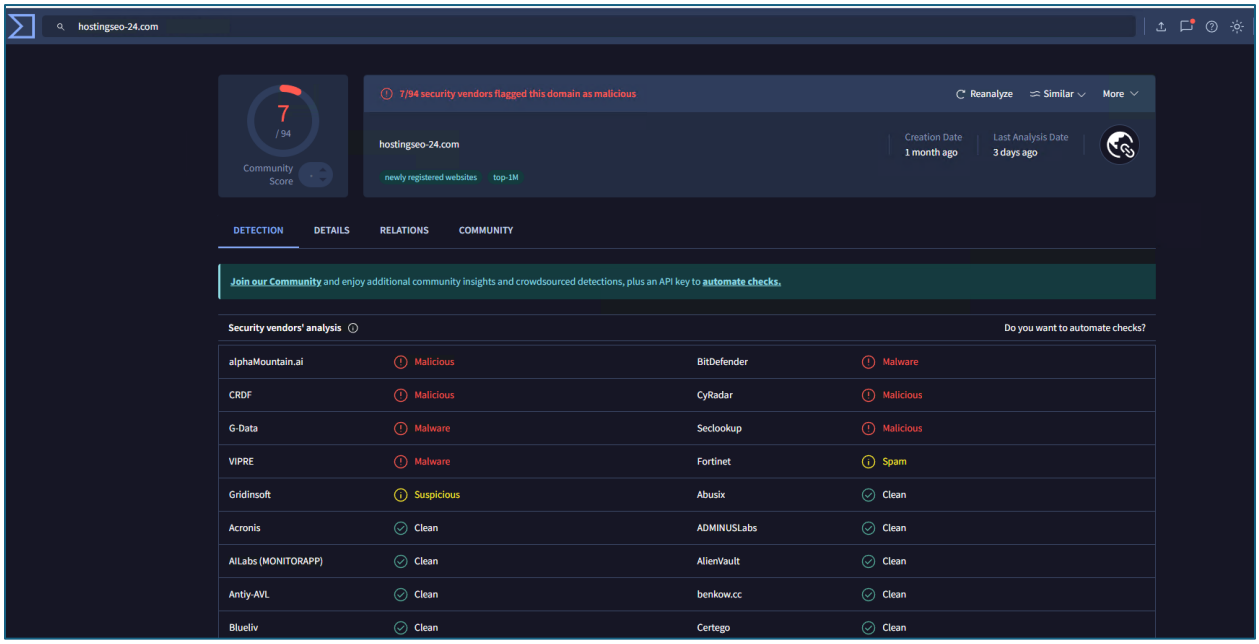


Figura 3: Kategorizimi i domain hosting-seo24

Gjithashtu nga analiza e e-mail header, evidentohet që dërguesi përdor VPS për dërgimin e e-mail si dhe për të fshehur gjurmët. IP e dërguesit **{57[.]128[.]228[.]145}** ka lidhje me shumë domain-e që lidhen me këtë fushatë.

```
Received: from vps-c9ecbdc9.vps.ovh.net (vps-c9ecbdc9.vps.ovh.net. [57.128.228.145])
        by mx.google.com with ESMTPS id a640c23a62f3a-abf0c77ad31si147126366b.489.2025.02.27.03.46.14
        for [redacted]
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Thu, 27 Feb 2025 03:46:14 -0800 (PST)
```

Figura 4:Të dhënat nga e-mail header

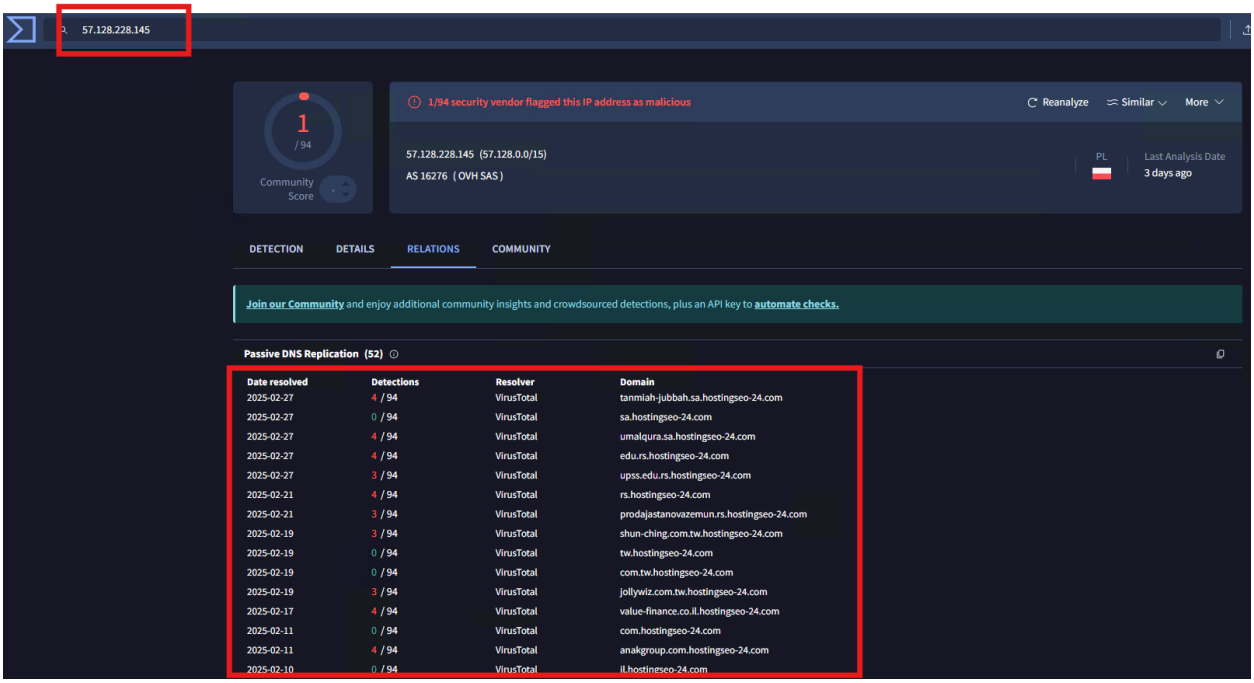
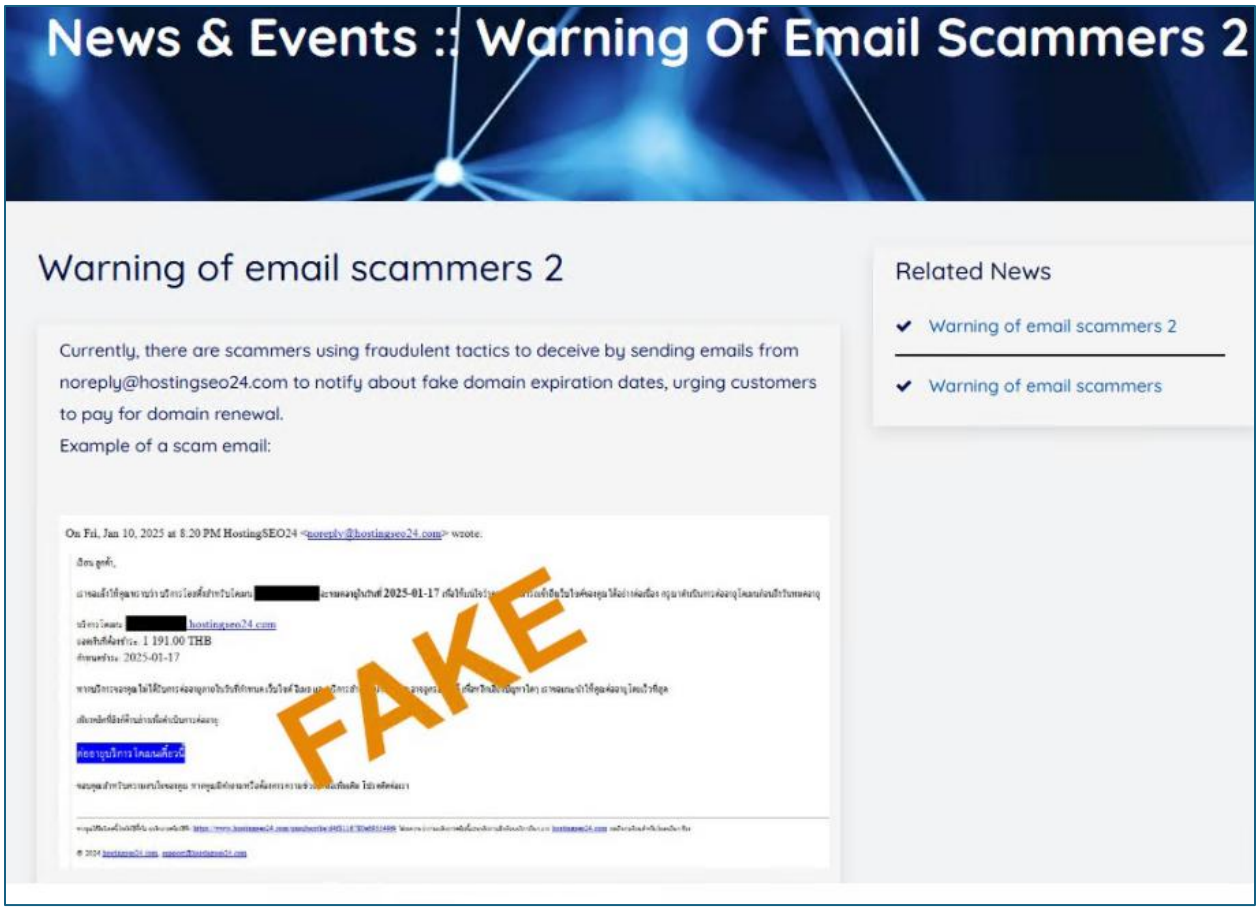


Figura 5: Analiza e IP të dërguesit

Nga analiza **OSINT** evidentohet që fushata të tilla janë raportuar më parë, por janë aktualisht aktive, ku pretendohet që klientët të bien viktima të plotësimit të formës me të dhëna bankare dhe për të kryer pagesën.


Academia International College
3d ·
Warning of email scammers
Currently, there are scammers using fraudulent tactics to deceive by sending emails from noreply@hostingseo24.com to notify about fake domain expiration dates, urging customers to pay for domain renewal.


News & Events :: Warning Of Email Scammers 2
Warning of email scammers 2
Currently, there are scammers using fraudulent tactics to deceive by sending emails from noreply@hostingseo24.com to notify about fake domain expiration dates, urging customers to pay for domain renewal.
Example of a scam email:
Related News
Warning of email scammers 2
Warning of email scammers
FAKE

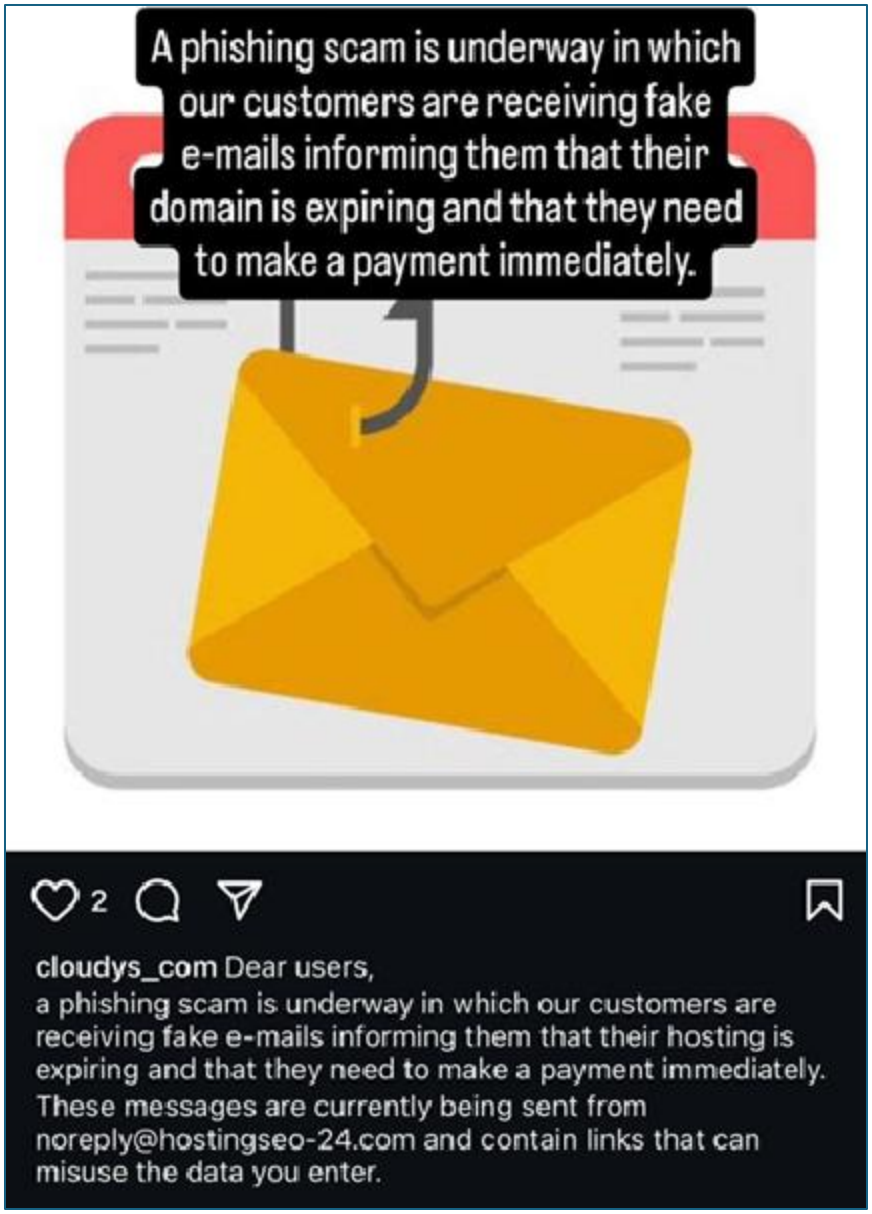


Figura 6: Raportime për Phishing

.

Indikatorët e Komprometimit

noreply@hosting-seo24[.]com	**E-mail Sender**
57[.]128[.]228[.]145	**IP**
vps-c9ecbdc9[.]vps[.]ovh[.]net	**DNS**
hosting-seo24[.]com	**Domain**

Rekomandime

Autoriteti Kombëtar për Sigurinë Kibernetike rekomandon:

- Bllokimin e menjëhershëm të Indikatorëve të Kompretimit, të përmendura më sipër në pajisjet tuaja mbrojtëse.
- Analizimin e vazhdueshëm të logeve që vijnë nga SIEM (Security information and Event Management).
- Aktivizimin e MFA (Multifactor Authentication) .
- Rishikimin e politikës së fjalëkalimeve dhe përditësimin e tyre.
- Kontrollin e users dhe privileges, në rast se ka ndryshim të userave dhe privilegjeve të tyre.
- Rishikimin e aksesit në internet për përdoruesit fundorë.
- Trajnimin e stafit jo-teknik rreth sulmeve "Phishing" si dhe mënyrat e shmangies së infektimit prej tyre.
- Instalimin e pajisjeve të perimetrit të rrjetit që bëjnë analizë të thellë të trafikut duke u mbështetur jo vetëm në rregullat e listave të aksesit por edhe në sjelljen e tij (Firewall-et NextGen).
- Sistemet e evidentuara të segmentohen në VLAN-e të ndryshme, duke aplikuar "Access control list për të gjithë perimetrin e rrjetit", webserviset duhet të jenë të ndarë nga Databaza e tyre, Active Directory duhet të jetë në një VLAN të ndarë.
- Aplikimin dhe përdorimin e teknikës LAPS për sistemet Microsoft, për menaxhimin e fjalëkalimeve të Administratorëve Lokal.
- Të aplikohen filtra të trafikut në rastin e aksesimit në distancë të hosteve (punonjësve/palë të treta/klientë).
- Të implementohen zgjidhje që kryen filtrimin, monitorimin dhe bllokimin e trafikut keqdashës ndërmjet aplikacioneve Web dhe internetit, Web Application Firewall (WAF).
- Të kryhen analiza të trafikut në nivel sjellje "behaviour" për pajisjet fundore, aplikimi i zgjidhjeve EDR, XDR. Kjo sjell analizën e skedarëve keqdashës jo vetëm në nivel signature por dhe në nivel behaviour.
- Të projektohet zgjidhja për menaxhimin e aksesit të përdoruesve "Identity Access Management" për të kontrolluar identitetin dhe privilegjet e përdoruesve në kohë reale sipas parimit "zero-trust".