Digital Exposure Analysis of the 500 Largest Portuguese Companies

Performed by:

Jorge Monteiro, CEO

jorge@ethiack.com

+351 915753364

schedule a call

Ethiack Lda, Instituto Pedro Nunes,

Rua Pedro Nunes, 3030 - 199 Coimbra, Portugal

Executive Summary

This report provides a preliminary analysis of the External Attack Surface and the Exposure Risk to cyberattacks of the 500 Largest Portuguese Companies. This was done by a passive and non-intrusive reconnaissance of the exposed digital infrastructure under 575 unique top-level domains.

The results show the number of exposed assets and provide an overview of the current security posture, from an outside perspective, including the most prevalent services, servers, 3rd parties, and technologies used by the organization.

Ethiack recommends implementing preventive tools, such as External Attack Surface Management (EASM) and Continuous Automated Red Teaming (CART) solutions, that provide vulnerability identification with actionable mitigation guides.

Overview

Total Exposed Assets: 10,880

Invalid SSL Certificates: 11.21%

Exposed Web Server Configurations: 21.77%

Methodology

The non-intrusive reconnaissance tool allows for the identification of:

- The total number of exposed assets.
- The type of web servers, services, technologies, and integrations in use.
- Exposure of information on the servers and configurations of digital certificates.

Notes and Limitations:

The tool used conducts only a preliminary reconnaissance of the relevant external attack surface, without being able to perform vulnerability identification and analysis.

This means that the tool is non-intrusive and only accesses information that is available in public databases and through legitimate accesses to web domains without employing any active testing. Additionally, this analysis only reveals exposed digital assets on the web, excluding, for example, mobile applications and internal networks and assets.

Therefore, the results are limited and may differ from the actual situation.

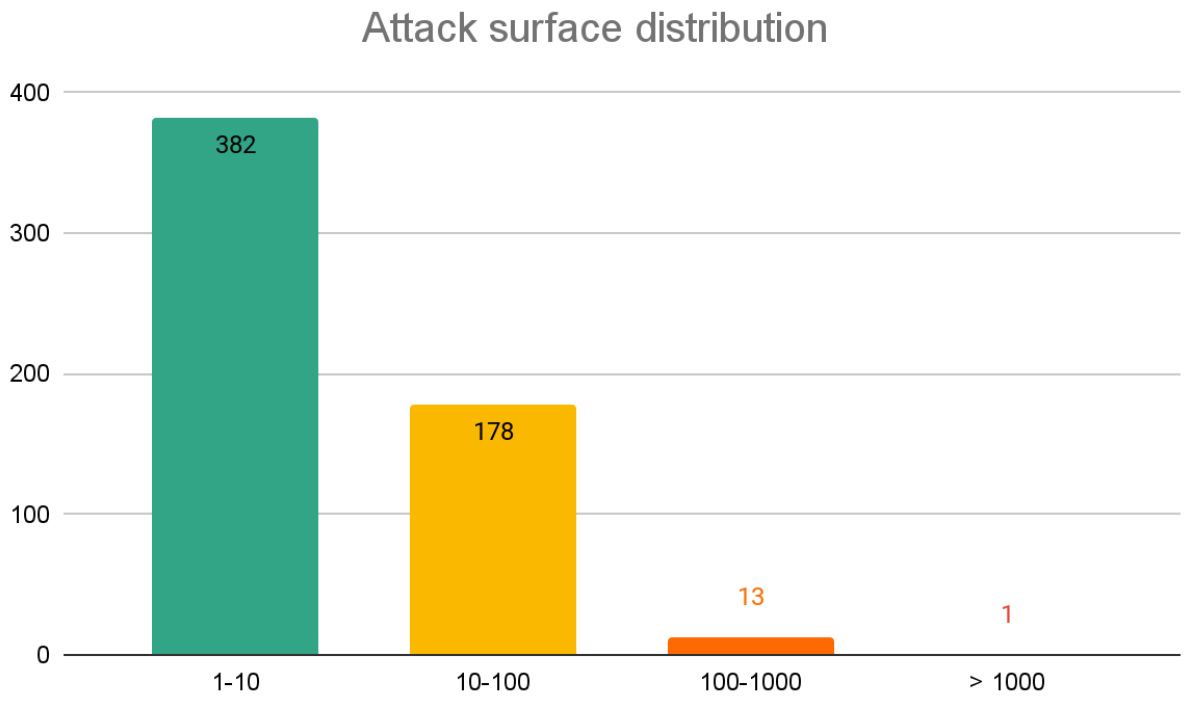
Exposure Risk Analysis

Size of the External Attack Surfaces

Total Exposed Assets: 10,880

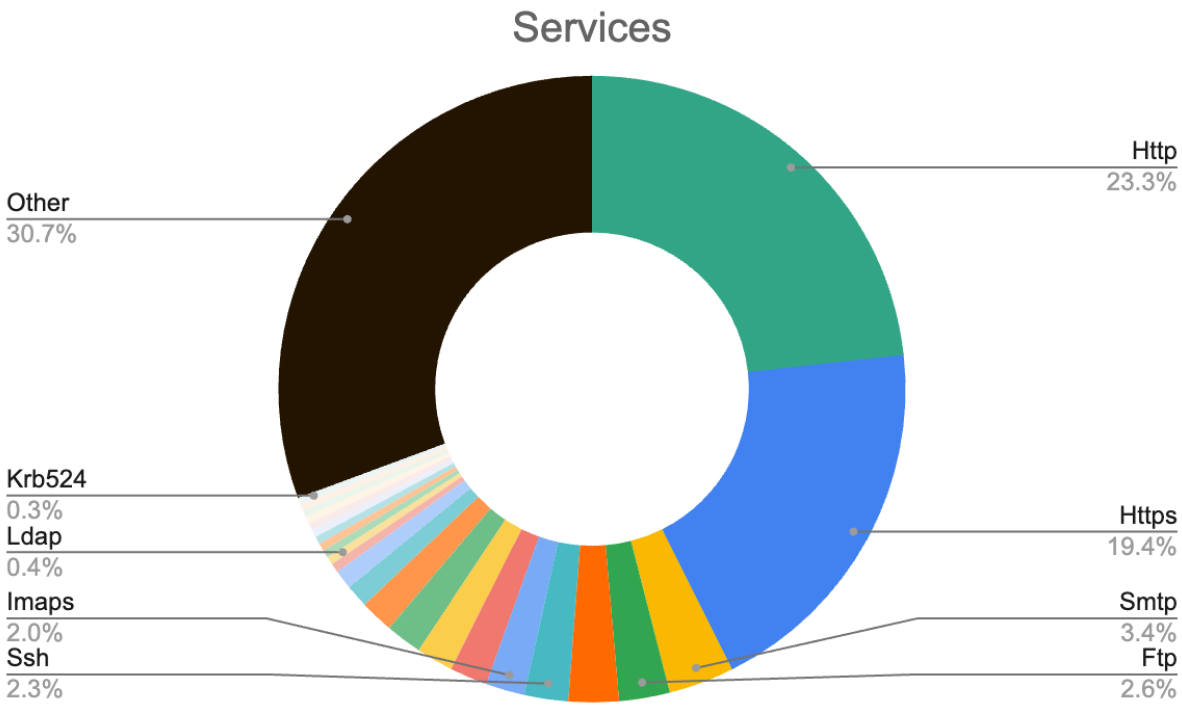
** An asset includes but is not limited to, domains, subdomains, servers, IP addresses, or web and mobile applications under a digital infrastructure.*

In general, the larger an organization's digital infrastructure, the more exposed it is to external attacks. Digital infrastructures expand as a result of business growth and the digital transformation of organizations. Agile development and third-party software make attack surfaces bigger than ever, with many exposed assets. On average, 37% of exposed assets are unknown, thus unprotected and vulnerable to cyberattacks. An EASM tool will be able to find what is exposed and hidden in an infrastructure.

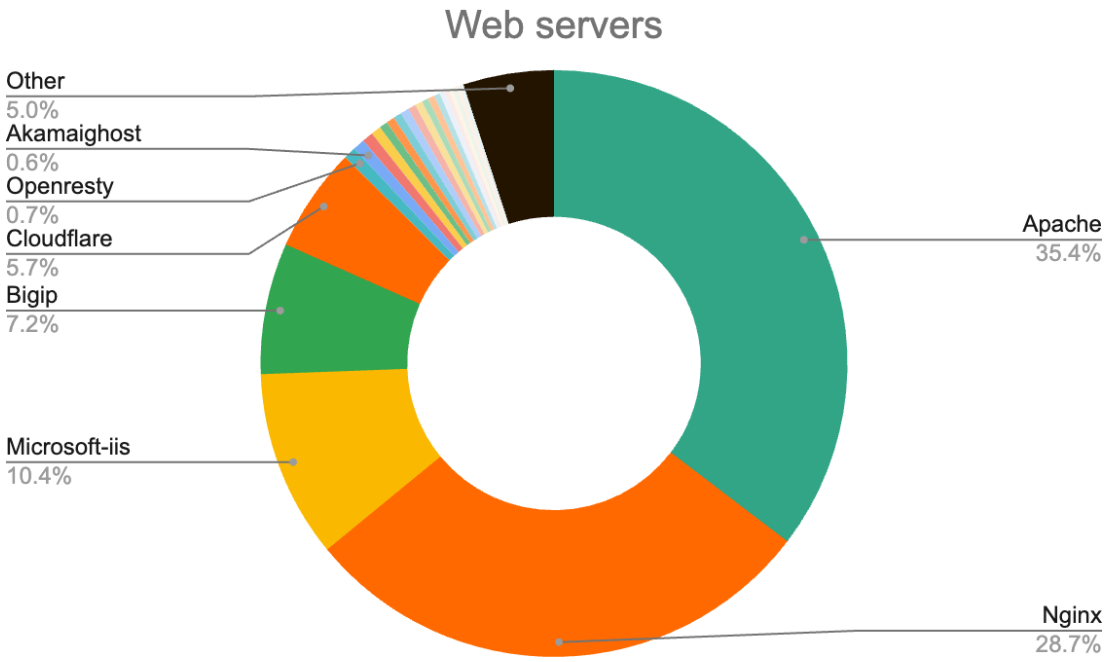


Graph 1 - Distribution of Attack Surface.

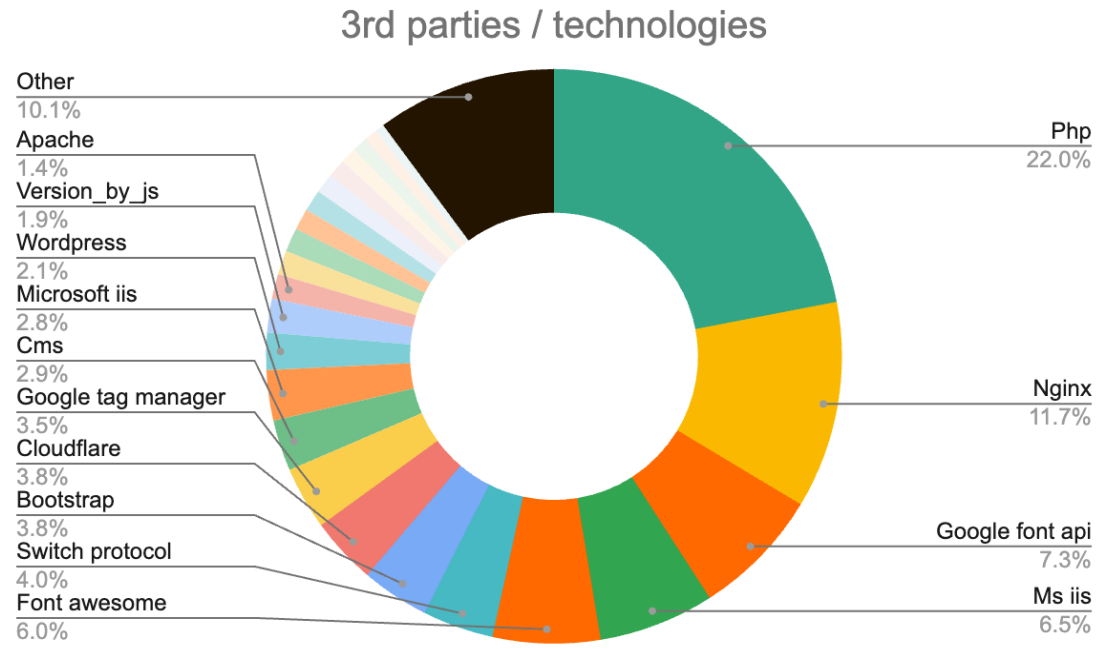
Characteristics of the External Attack Surfaces



Graph 2 - Distribution of Services.



Graph 3 - Distribution of Web Servers.

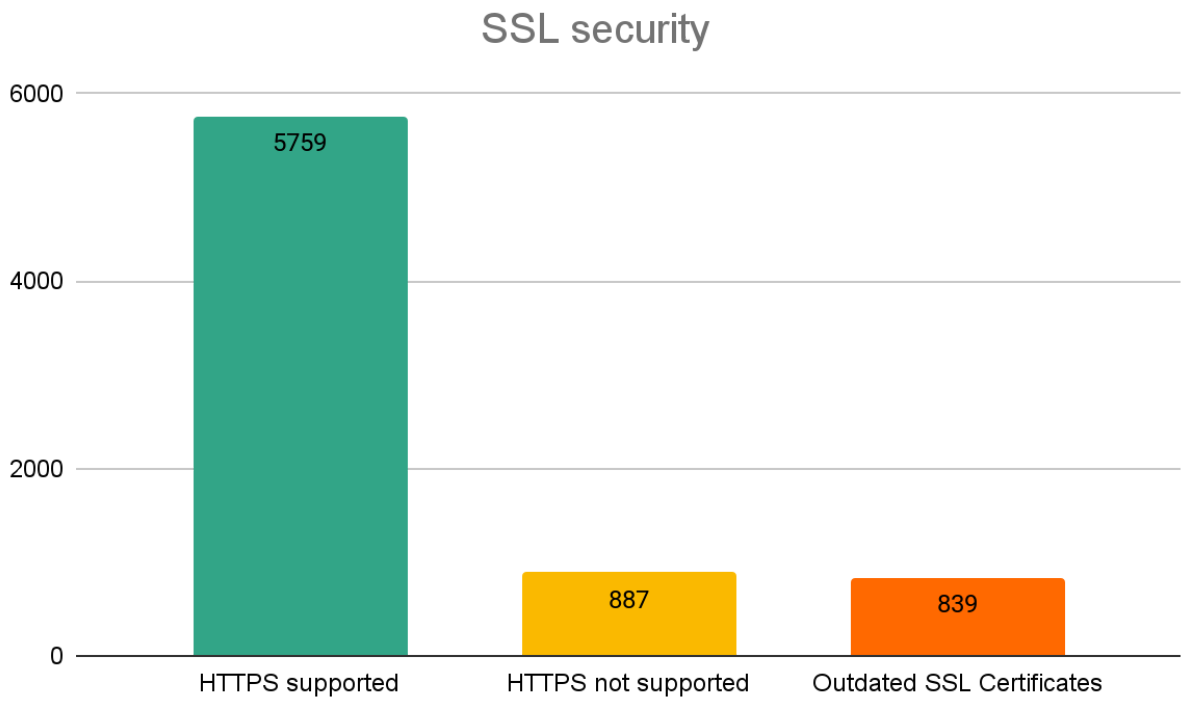


Graph 4 - Distribution of Technologies.

Exposed Security Posture

Invalid SSL Certificates: 11.21%

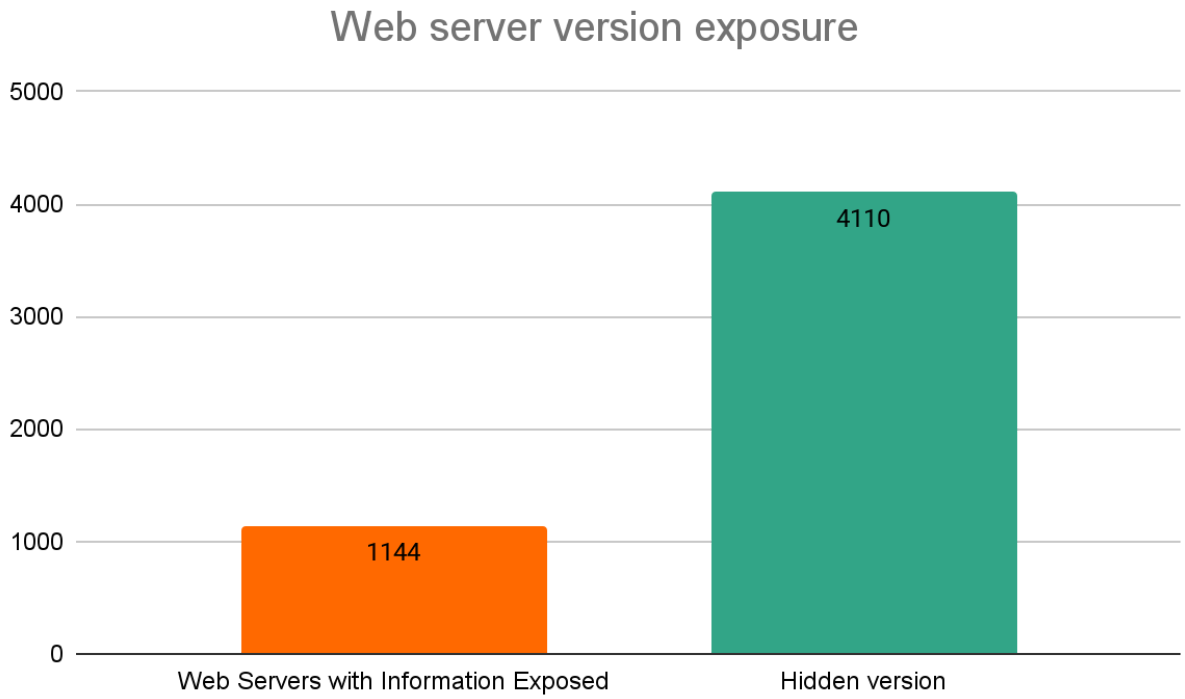
Outdated SSL certificates have invalid HTTPS protocols, which means that they are outdated and thus insecure. This allows an attacker to intercept traffic while connected to the same network, enabling attacks such as eavesdropping and man-in-the-middle.



Graph 5 - Number and Status of Digital Certificates.

Exposed Web Server Configuration Files: 21.77%

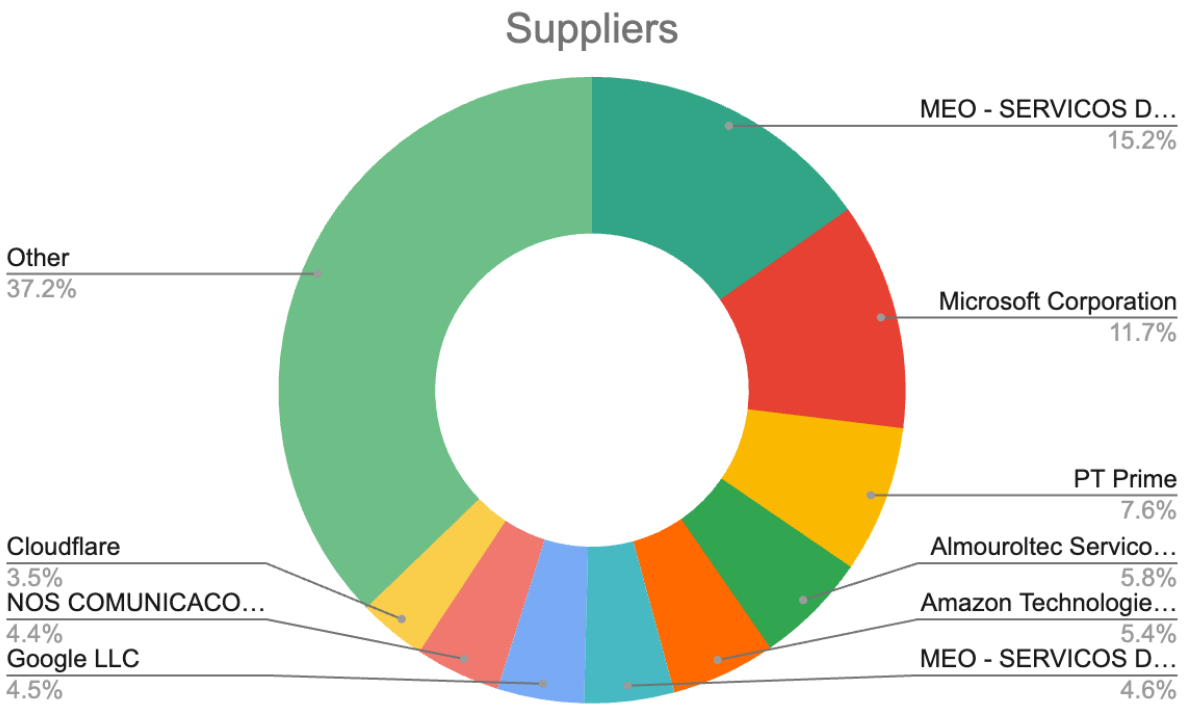
By publicly exposing information about their version and software, web servers are more vulnerable to exploitations.



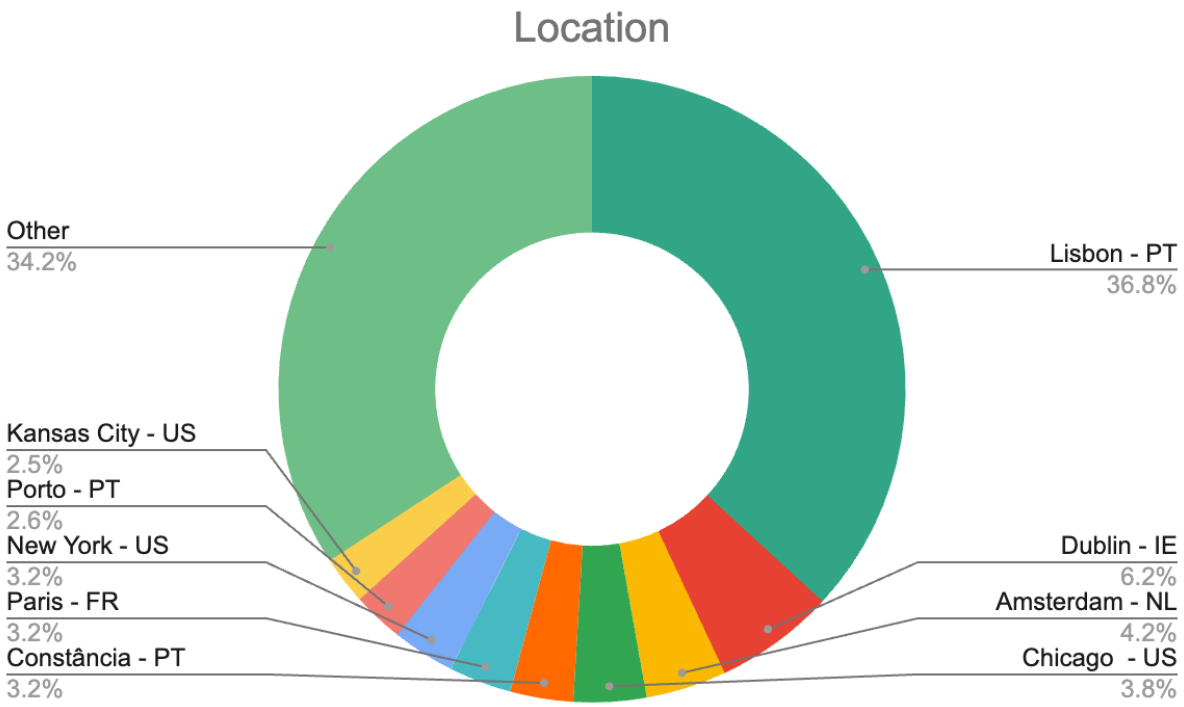
Graph 6 - Number and Status of Web Servers

Asset Inventory

Regarding the assets used by the companies in the study, we found some patterns regarding suppliers. As expected, most of these are located inside Portugal (54%), with the rest of the world still greatly represented.



Graph 7 - Suppliers



Graph 8 - Locations

Recommendations

Even if the report's results are just preliminary due to being collected through passive and non-intrusive methods, they suggest room for improvement in cybersecurity practices.

The report reveals some exposure risks and highlights the importance of adopting preventive and proactive solutions that will allow for better management of the external attack surface. Ethiack recommends the adoption of two solutions:

First, an External Attack Surface Management (EASM) tool will allow these organizations to have a complete view of the entire digital exposure and map every known and unknown asset.

Second, a Continuous Automated Red Teaming (CART) tool, combining the knowledge from both automated and manual testing, will allow for continuous and accurate

vulnerability identification with actionable insight, so that security teams are productive and always ahead of cybercriminals.

ABOUT ETHIACK

Ethiack is a SaaS cybersecurity platform that helps organizations enhance security levels and prevent cybercrime while optimizing costs and resources.

The platform performs instant, continuous, and 99% accurate security monitoring and testing, through Autonomous Ethical Hacking powered by ML/AI. This allows security teams to manage their external attack surface and to identify and mitigate vulnerabilities quickly and efficiently.

The Platform offers:

- Vulnerability Assessment and Management
- External Attack Surface Management
- Risk Exposure Management
- Dynamic Application Security Testing
- Automated and Continuous Security Testing
- Manual and On-demand Security Testing
- Triaging and Retesting of Vulnerabilities
- Compliance Reports with Mitigation Guides
- Dedicated Customer and Security Support

ETHIACK

autonomous ethical hacking