Caspi PoT v.2.0

Some of our references

hopi
FLO
BOYNER
mynet
İSTANBUL BÜYÜKŞEHİR BELEDİYESİ
isbak
Doğuş Teknoloji

Null Risk

0%

Internal Network Risk

Caspipot can operate independently of the customer data center and server architecture.

- No Internal Installation Required
- Talks to products via API
- No customer data inside

0%

Breach Data

Caspipot does not host customer data. The data on the systems are attack data and scan data created by attackers.

- No customer data inside
- The customer is not asked to enter data
- No database and data architecture

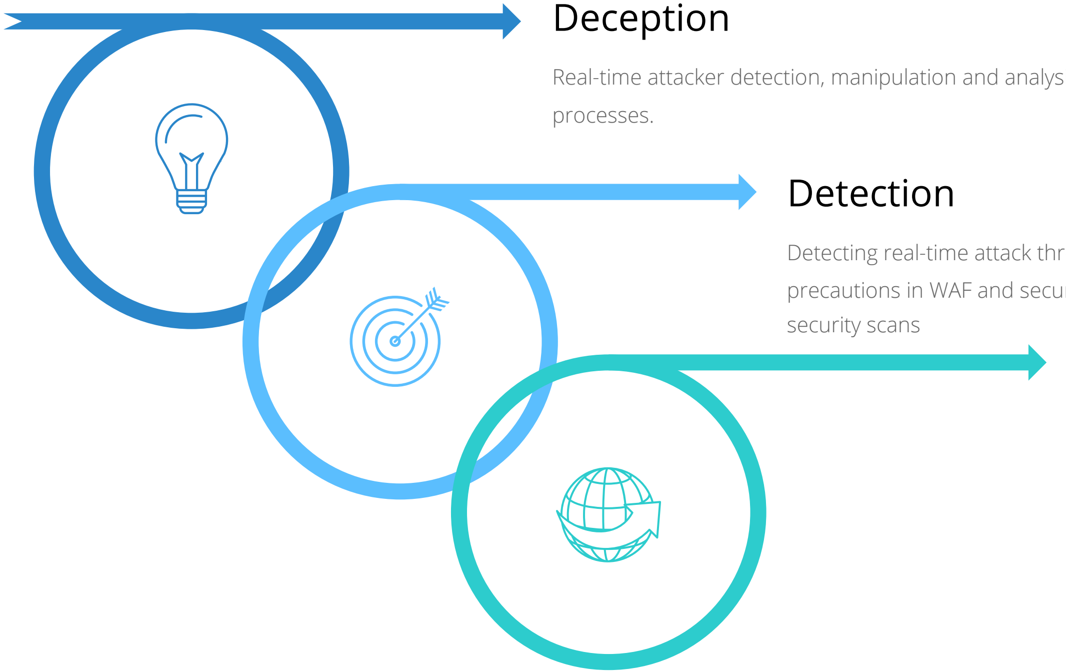
0%

Risk of Hacking

Caspipot services operate on autopilot mode. The system resets itself as soon as the rules set on the kernel change.

- No data is kept on services
- Byte by byte change detection
- All services and customers are classified separately

What we are doing?



Deception

Real-time attacker detection, manipulation and analysis processes.

Detection

Detecting real-time attack threats, automatically taking precautions in WAF and security products and performing security scans

Solution & Reporting

Direct updates and reports to products integrated with real-time data analysis and real attack data collected from attackers. Raising awareness of security teams and group-specific reporting.

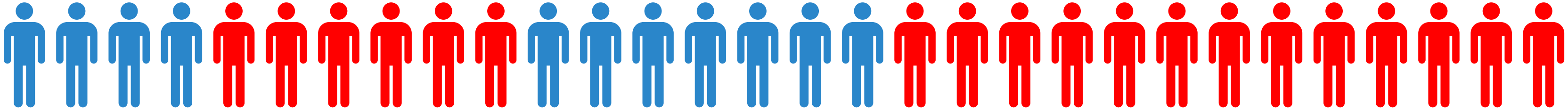
Deception (01.2024)

1.70M / Monthly

Attack data

200K / Monthly

Intrusion prevention firewall update process



200.000 Uniq attack

Attackers' New Technologies

98 Targeted attack

Continuous Attack on Specific Systems

10.000 Pre-Detection

Attacker Re-access Detection

Deception Solutions

0-day / * Detection

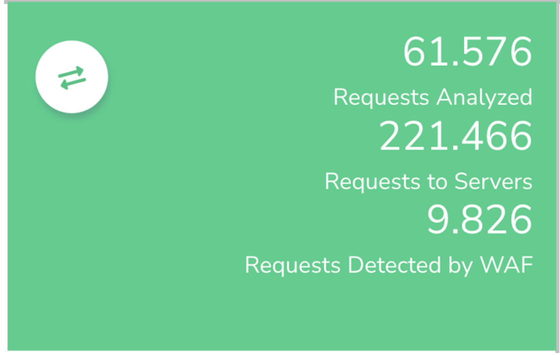
Detecting and reporting the exploitation techniques they currently use by manipulating active attackers and producing solutions.

Detailed Attacker Analysis

Analyzing attackers trying to infiltrate targeted systems, analyzing and scoring past and future threats

Integration

Direct integration with 3rd party security products. Direct integration with advanced API service



61.576

Requests Analyzed

221.466

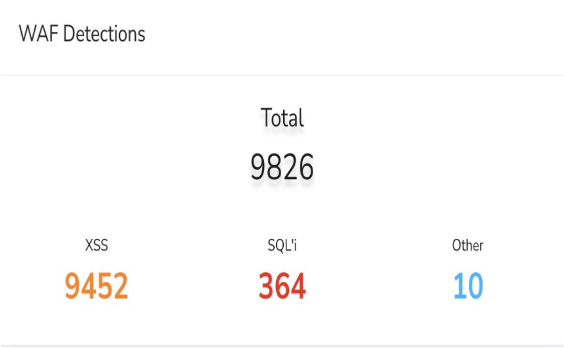
Requests to Servers

9.826

Requests Detected by WAF

Rules and Report

Detailed reports over 5 different technologies. Creation of special rule sets.



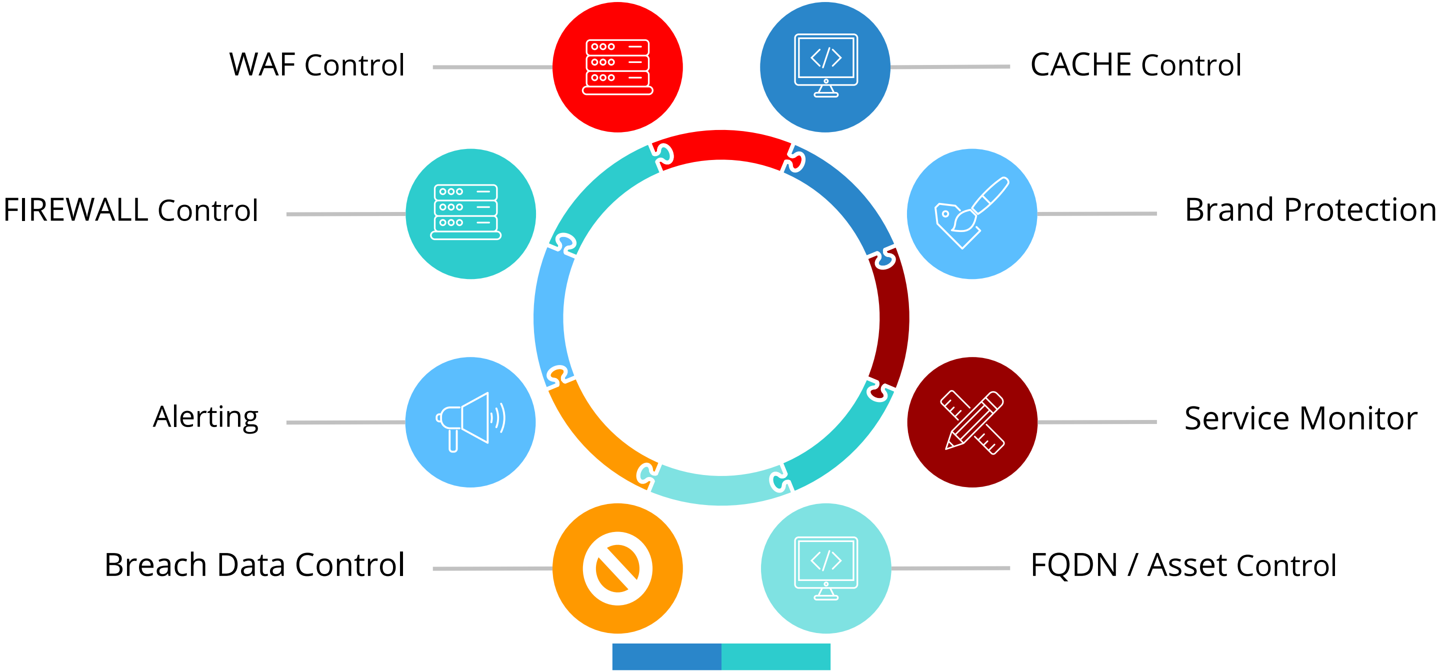
WAF Detections

Total

9826

XSS	SQL'i	Other
9452	364	10

Detection Modeles



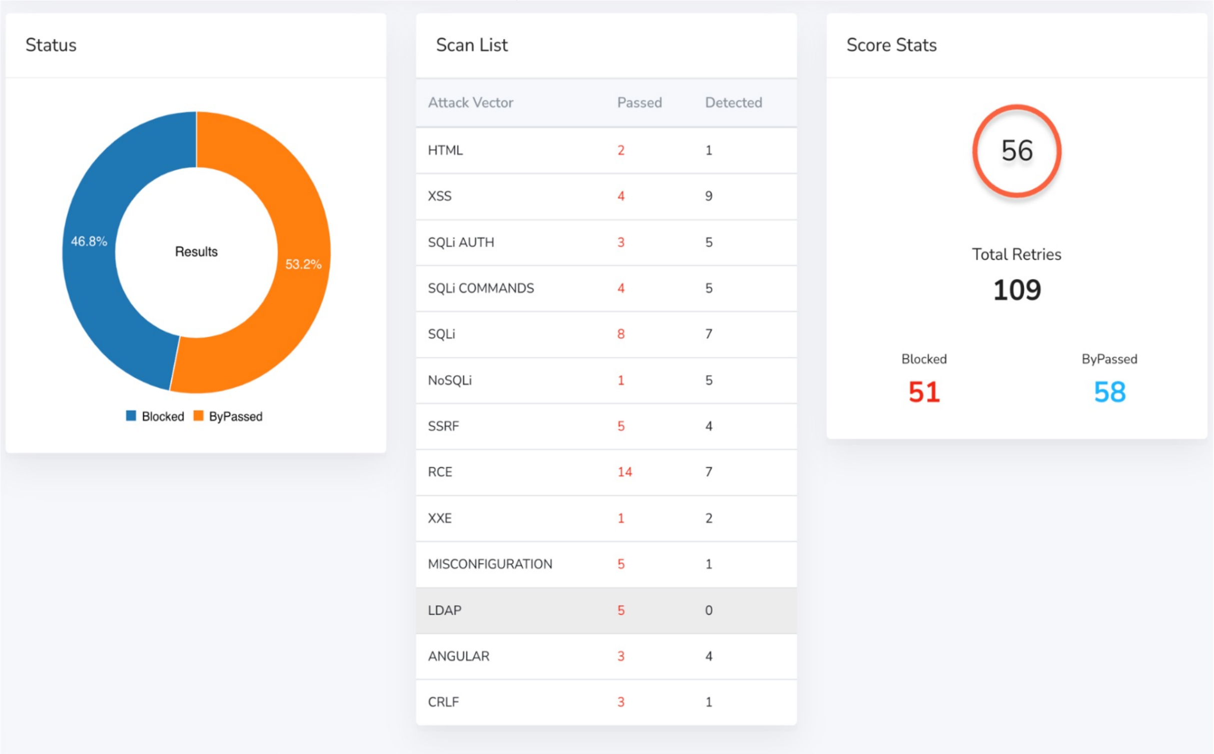
WAF / Firewall Test

Real data Tests

Create a simulation by processing real attacker data and analyze the existing firewall by subjecting designated areas to these tests

Detailed Report

See detailed reporting and analysis data through the dashboard. Sharing and direct download of reports



Scan List

Attack Vector	Passed	Detected
HTML	2	1
XSS	4	9
SQLi AUTH	3	5
SQLi COMMANDS	4	5
SQLi	8	7
NoSQLi	1	5
SSRF	5	4
RCE	14	7
XXE	1	2
MISCONFIGURATION	5	1
LDAP	5	0
ANGULAR	3	4
CRLF	3	1

Score Stats

56

Total Retries
109

Blocked
51

ByPassed
58

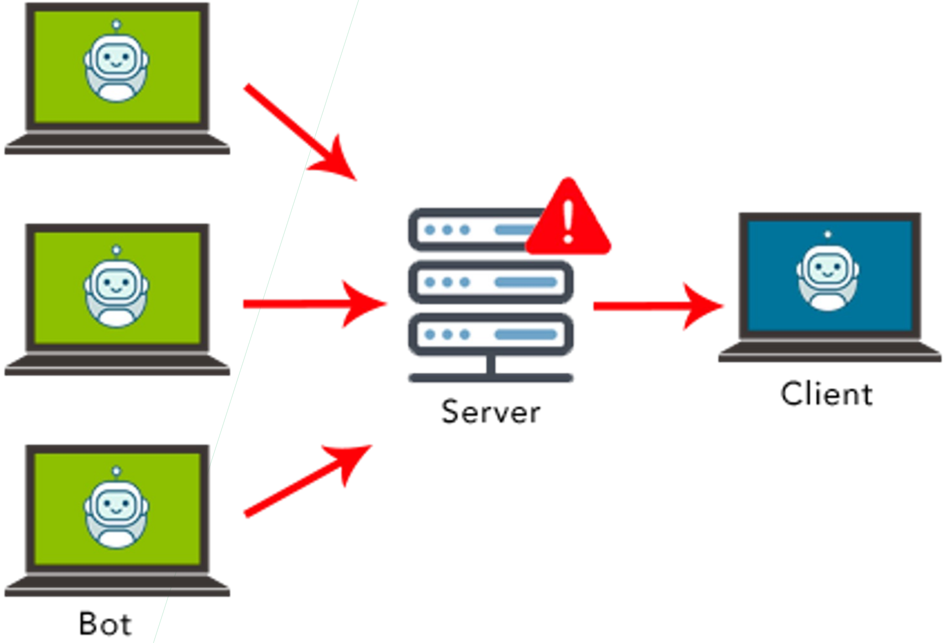
Stress Tester

Load Stress Tests

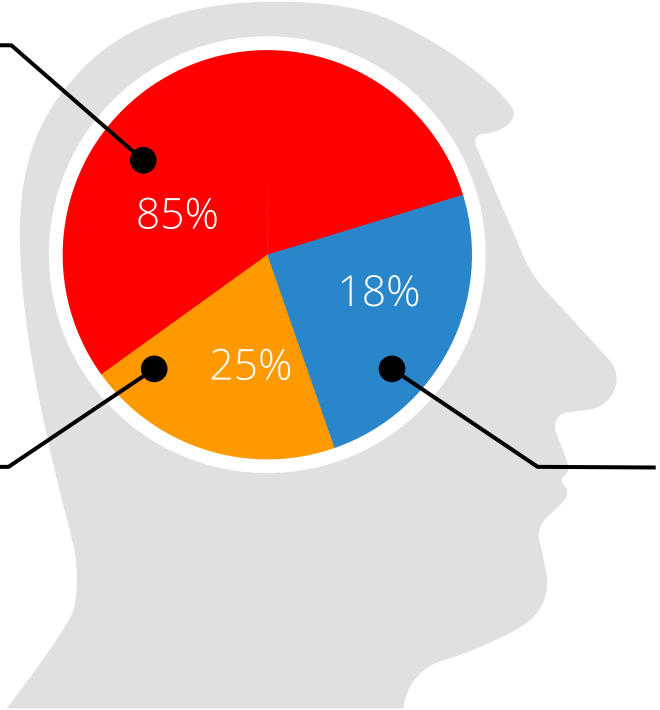
Subjecting systems to denial of service tests with distributed HTTP requests to designated targets (L4,L7)

Detailed Report

See detailed reporting and analysis data through the dashboard. Sharing and direct download of reports.



Breach Data



Password Reuse

It has been determined that 85% of the company employees use the passwords they use within the company in their private lives.

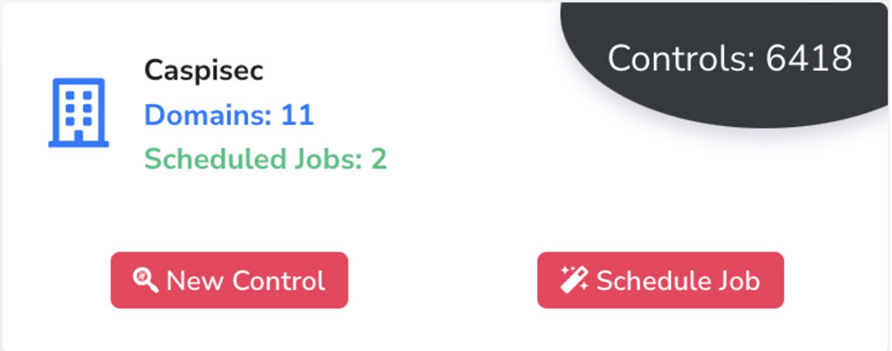
Memorable Changes

It was found that password changes were generally made over the old password.

Multiple Verification

A very small proportion of company employees use dual verification in their private lives.

Breach Data



Controls: 6418

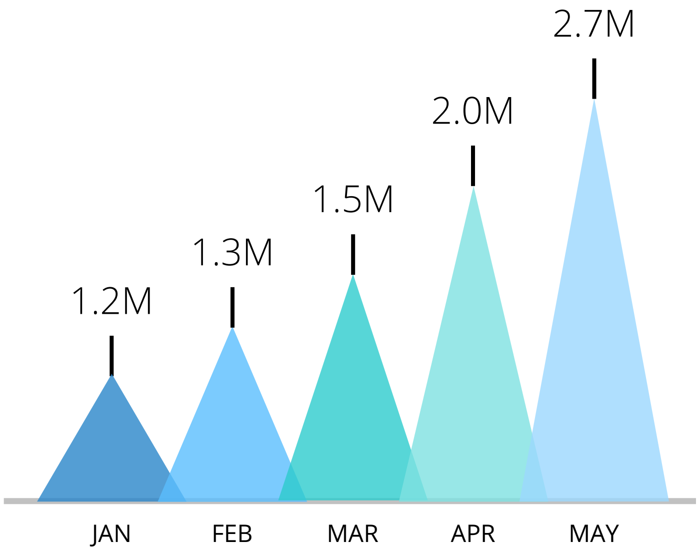
Caspisec

Domains: 11

Scheduled Jobs: 2

Password Leak Check

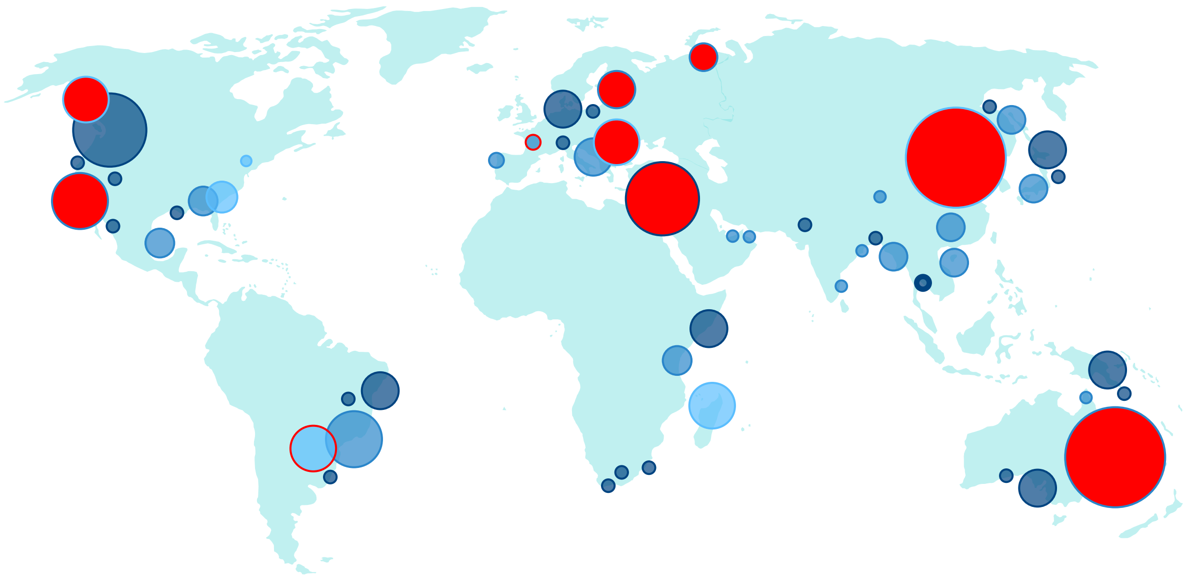
Monitoring the accounts used by company and institutional employees on external services and reporting data leakage in case of data leakage



2023 Active Password Detection Data

What Companies Are Missing

In 2023, independent research showed that more than 70% of hacked systems were hacked through FQDN and sub-services.

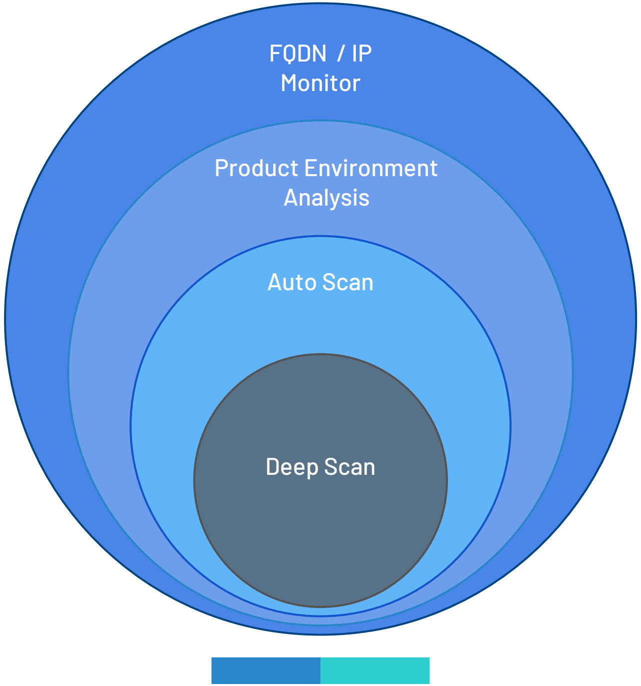


Most of the hacking is done through sub-services and legacy services.

70%

Host system and user factor.

30%



Caspipot ASM

CASPIPOT ASM - Actively monitors and scans subdomains, services and servers of institutions and organizations.

Scans are each managed and reported separately.

- **Black List / Malware Scan**

  Checks whether the identified assets are in global black lists.

- **Subdomain / PORT Scan**

  Scanning the subdomains of the corporate services defined in the system and the active ports of the servers, informing the organization and updating the inventory.

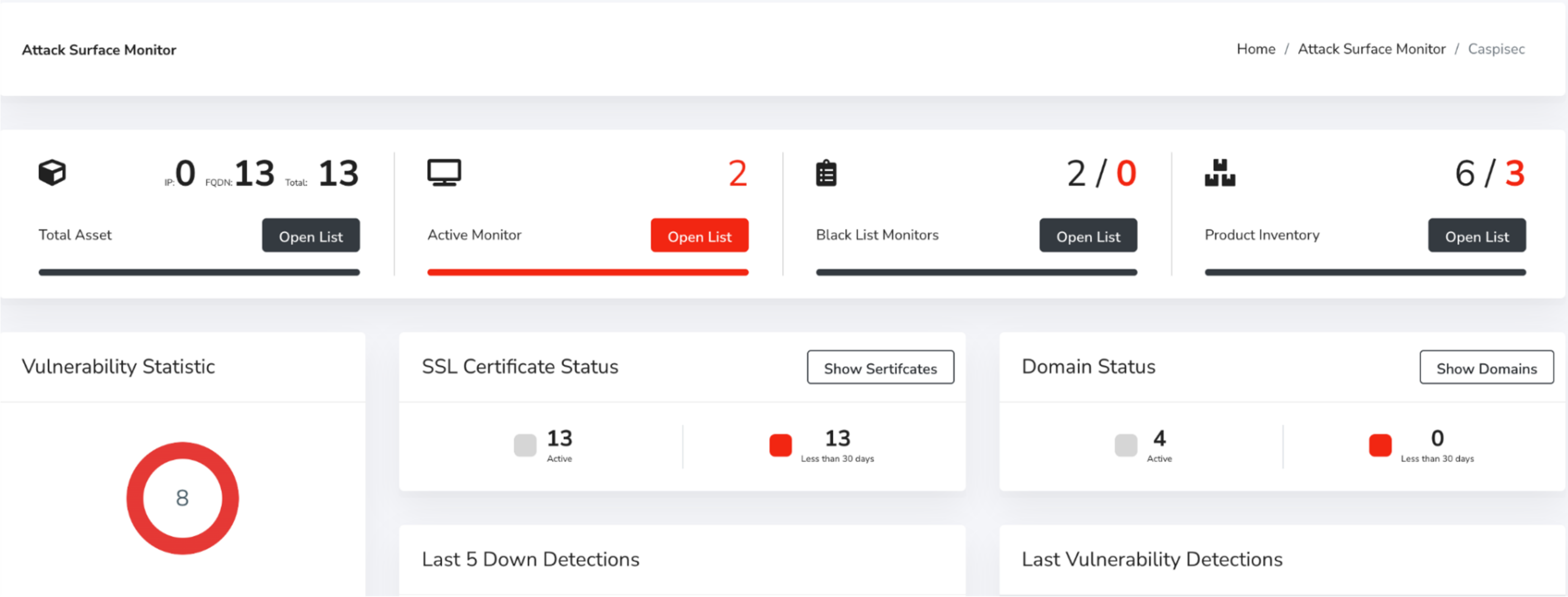
- **CVE / Vulnerability Scan**

  It performs vulnerability scans on the detected active services directly approved by the CASPIPOT team.

- **Active Scan**

  SSL, DOMAIN, Status, Hacklink monitor on systems

ASM Dashboard



Attack Surface Monitor

Home / Attack Surface Monitor / Caspisec

IP: 0 FQDN: 13 Total: 13

Total Asset

2

Active Monitor

2 / 0

Black List Monitors

6 / 3

Product Inventory

Vulnerability Statistic

8

SSL Certificate Status

13 Active

13 Less than 30 days

Domain Status

4 Active

0 Less than 30 days

Last 5 Down Detections

Last Vulnerability Detections

Support

WAF / Firewall Monitoring

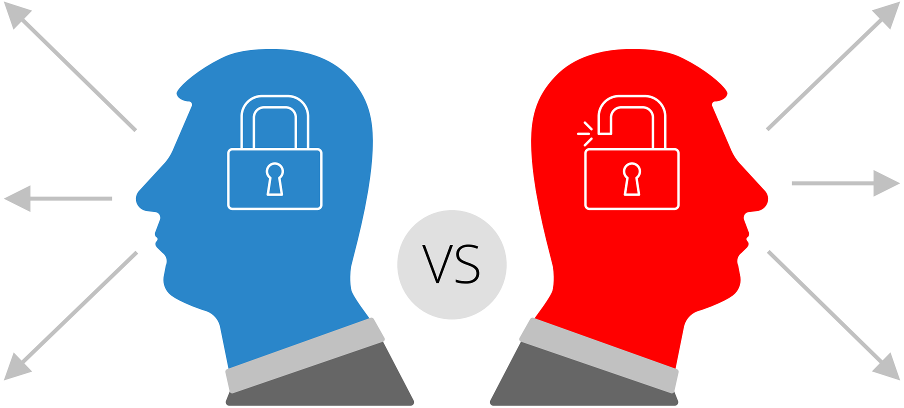
When CASPIPOT is integrated, it updates WAF / Firewall products directly and keeps the runes database up-to-date against current threats

Advanced Alarm Mechanism

By minimizing the F/P Situations, you can create detailed analyzed reports in the most accurate way.

3. Eye

Continuous scanning and analysis on scanned and detected services



WAF / Firewall

Security teams should constantly update for current threats and use specialized tools or resources for bypass methods

External Service Analysis

Continuously scan services, check inventory and keep up to date

Data Flow Monitoring

Thank You