CaspiPoT

SECURITY GUARD

Defend Your Business Against the Latest Cyber Threads

”

Technical Documentation

Product overview

- Quick Start Guide
- What's New
- Getting Started Guide

Planning

- Architecture and Deployment Guide

Installing

- Installation Guide

Configuring

- Honeypot Node Configuration Guide
- Attack Surface Monitor Configuration Guide
- Breach Data Control Configuration Guide
- Phish Data Configuration Guide
- IOC's Data Usage Guide
- O365 Integration Guide Line (Quick Start Guide Version 2.0)

Administering

- Administration Guide

Monitoring

- Attack Surface Monitoring (Quick Start Guide Version 2.0)
- Breach Data (Quick Start Guide Version 2.0)
- Honeypot (Quick Start Guide Version 2.0)

Tuning and Troubleshooting

- Troubleshooting and System Notifications Guide
- Tuning Guide(Quick Start Guide Version 2.0)

Effective Approach for Your Cyber Security with **CaspiPoT** Security Guard

Quick Start Guide
Version 1.2.2

Caspipot Security Guard is an all in one SaaS security solution where you can create your honeypot services within minutes, track the attackers and gather information with attack surface monitoring & breach data control.

This guide gets you started with a typical installation and configuration. To obtain the Quick Start Guide in other languages, print the language-specific PDF from the installation media.

WHAT's NEW

Office 365 security compliance can help to protect all parties involved, maintain public reputation, avoid fines, and ensure important data is not lost or stolen. Large companies, small and medium-sized enterprises and even smaller companies have already deployed these solutions to increase the productivity and collaboration of their teams.

Microsoft 365 solutions offer unprecedented flexibility in information sharing and collaboration, allowing employees to connect to their work environment on a variety of devices and from any location.

However, this flexibility to access documents, data and other company information via SharePoint, OneDrive, Exchange, creates many problems and opportunities for highly targeted cyber-attacks on the information system.

With the **CaspiPoT-OSeC365** module, all your risks can be monitored on an integrated screen. With machine learning-based analysis, it helps you detect and catch potential threats faster.

Getting Started Guide

CaspiPoT Security Guard Getting Started Guide introduces you to key concepts, an overview of the installation process, and basic tasks that you perform in the user interface.

Intended audience

This information is intended for use by security administrators who are responsible for investigating and managing network security. To use this guide you must have a knowledge of your corporate network infrastructure and networking technologies.

Technical documentation for information about how to access more technical documentation, technical notes, and release notes, see CaspiPoT Security Guard Security Documentation Technical Note (https://www.caspipot.com/support/1905).

Contacting customer support for information about contacting customer support, see the Support and Download Technical Note (http://caspipot.com/support/).

Statement of good security practices IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. CaspiPoT Security Guard systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. CaspiPoT DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note: Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. CaspiPoT Security Guard may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of CaspiPoT.

Architecture and Deployment Guide

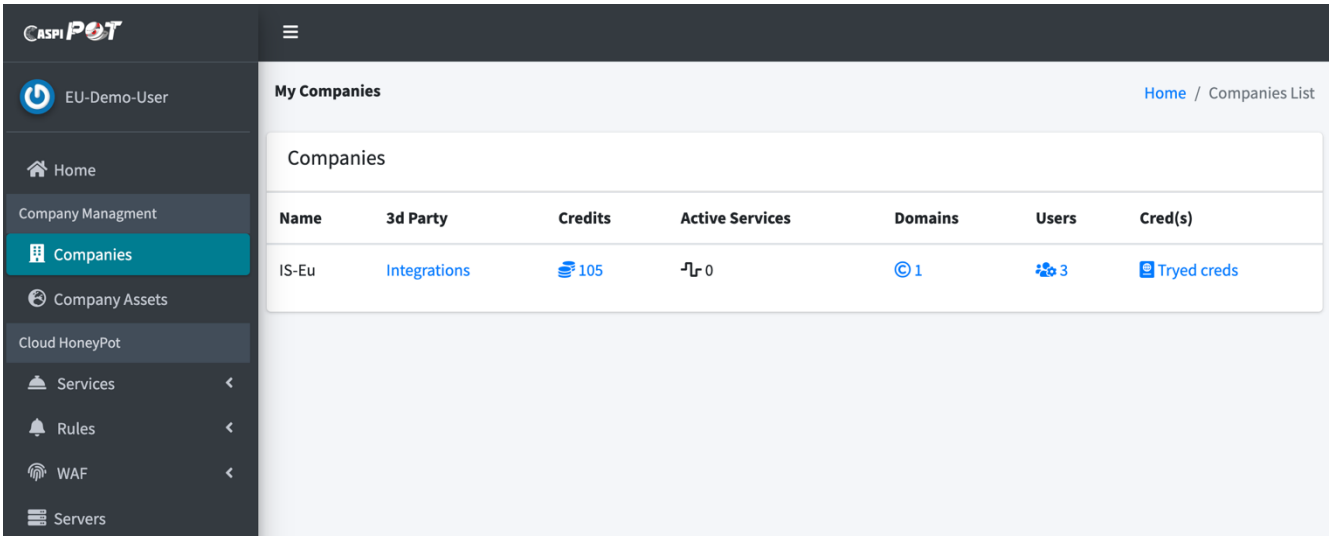
When you plan or create your CaspiPoT Security Guard deployment, it's helpful to have a good awareness of CaspiPoT architecture to assess how CaspiPoT Security Guard components might function in your network, and then to plan and create your CaspiPoT deployment. CaspiPoT processes, aggregates, and stores attack-data in real time. CaspiPoT Security Guard providing real-time information and monitoring, alerts and offenses, and responses to threats. CaspiPoT Security Guard is a modular architecture that provides real-time visibility, which you can use for threat detection and prioritization. You can scale CaspiPoT to meet your collection and WAF response. Attack Surface Monitoring systems helps to find critical issues in assets.

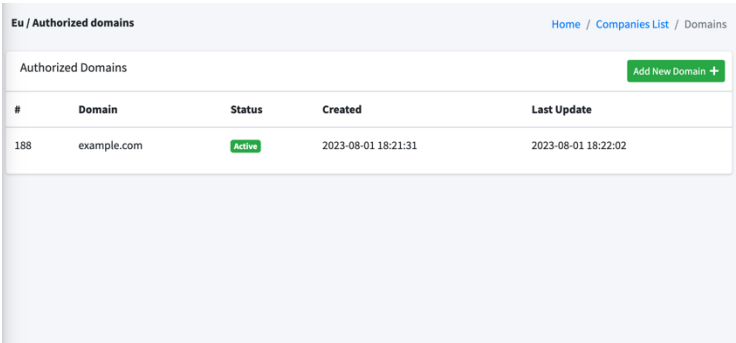
CASPIPOT COMPONENTS

CLOUD HONEYPOT Services Rules Waf	**BREACH DATA CONTROL**	**ATTACK SURFACE MONITOR** Last Scanner Activities Asset Status Control Blacklist Control
PHISH DATA	**IOC's** Bad IP Pool Proxy Pool Fqdn Pool	**O365 GUARD**

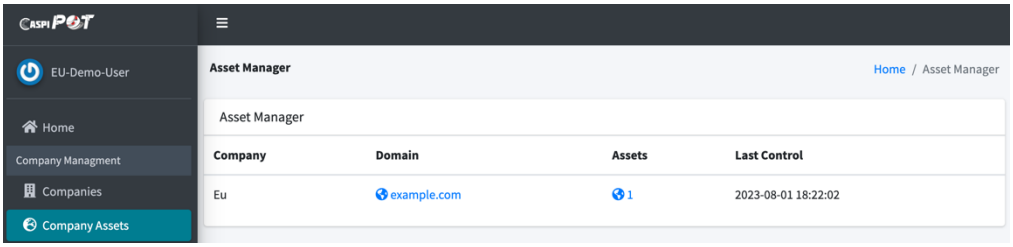
ALL-in-ONE DEPLOYMENT

Although the product consists of multiple modular structures, it is very easy and simple to install. First of all, in order to activate your services, you must register your domain name. You can access panel with https://manager.caspipot.com





After the approved registration of your domain name is completed, the domain name is automatically added to the asset list.

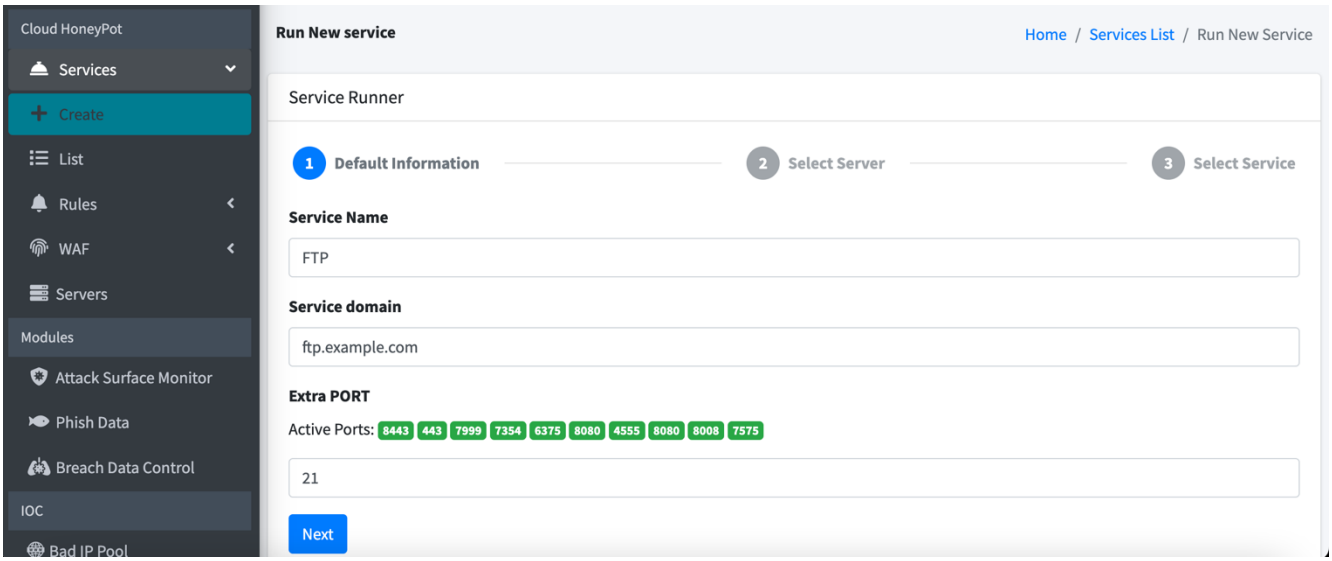


CONFIGURING

Honeypot Node Configuration Guide

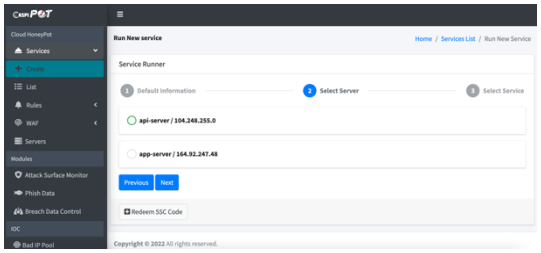
To activate honeypot services via **the manager panel || CLOUD HONEYPOT >> Services >>> Create** field should be reached.

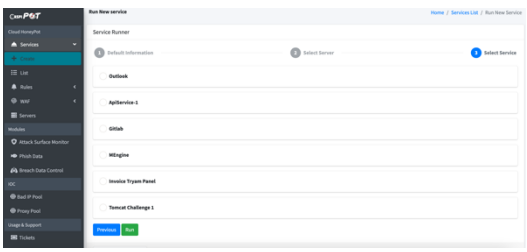
In order to define services, it is necessary to complete the **service name**, **domain name** and **port information** of your service completely.



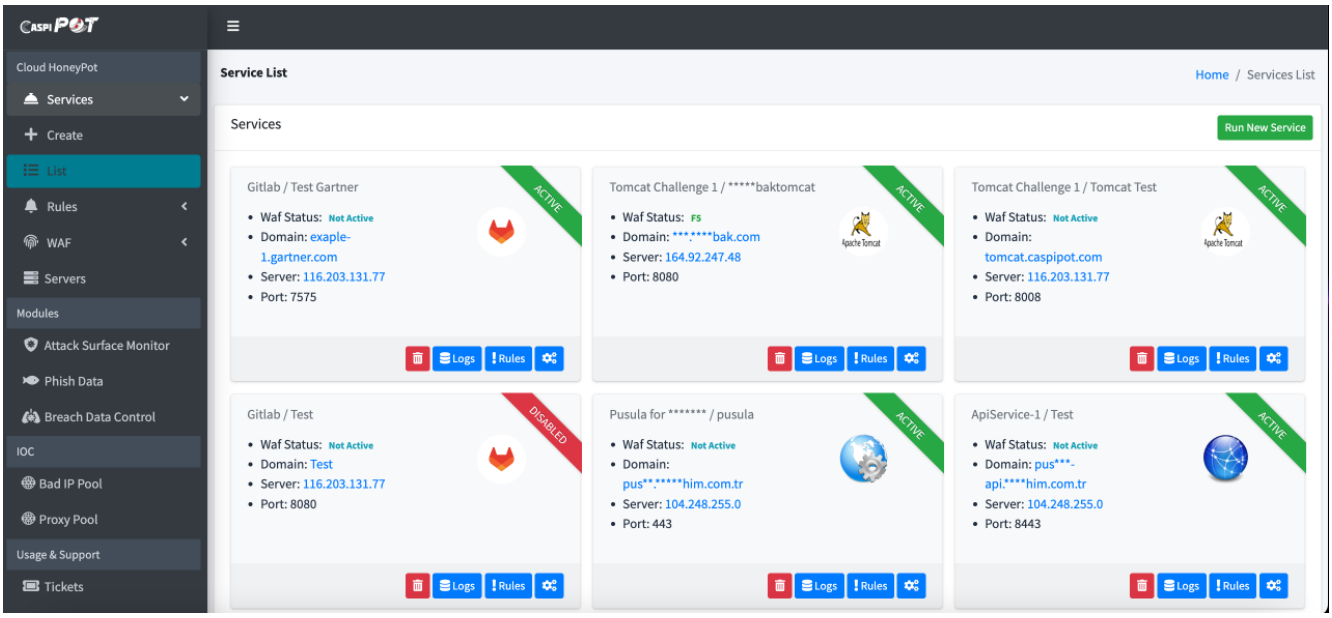
With the defined information, the area where you can choose from among the servers defined in different datacenters around the world will be displayed to within the scope of the license type.

These are the things that need to be done in order to take a service live.

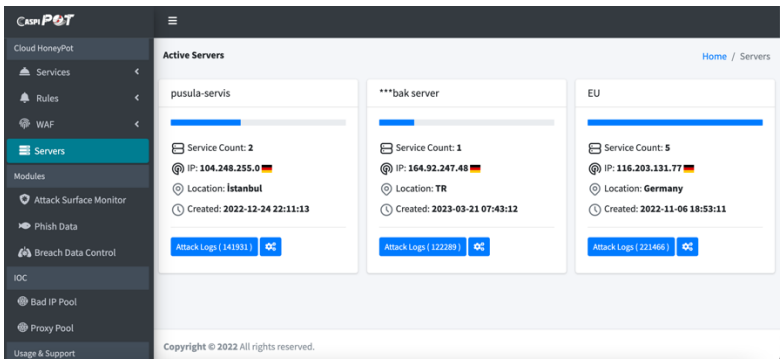




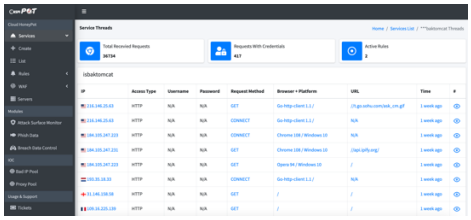
After the configurations related to the services, the manager panel shows all active and passive services. You can be viewed by following the steps of **manager panel || CLOUD HONEYPOT >> Services >>> List**



To Access your licensed servers manager **manager panel || CLOUD HONEYPOT >> Services >>> Servers**



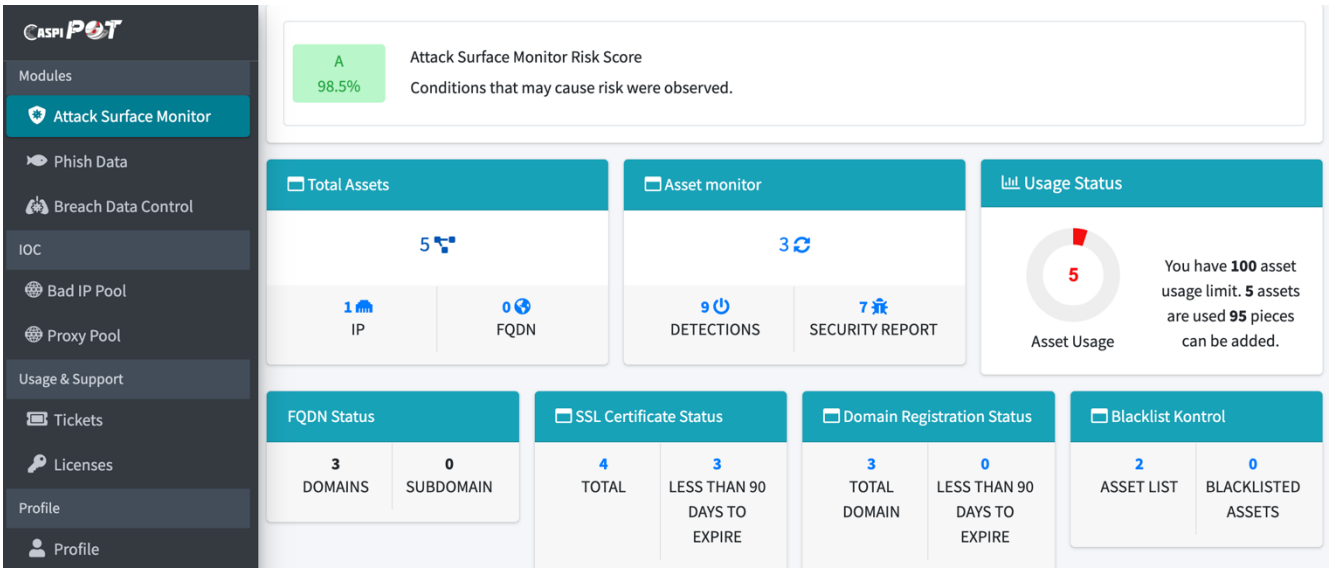
With the operations performed, attacks on services that are now defined begin to be detected. Important rules can be written for the listed attack types and critical situations. You can receive hourly, daily, monthly reports on detected attacks and automatically forward them to the relevant teams.

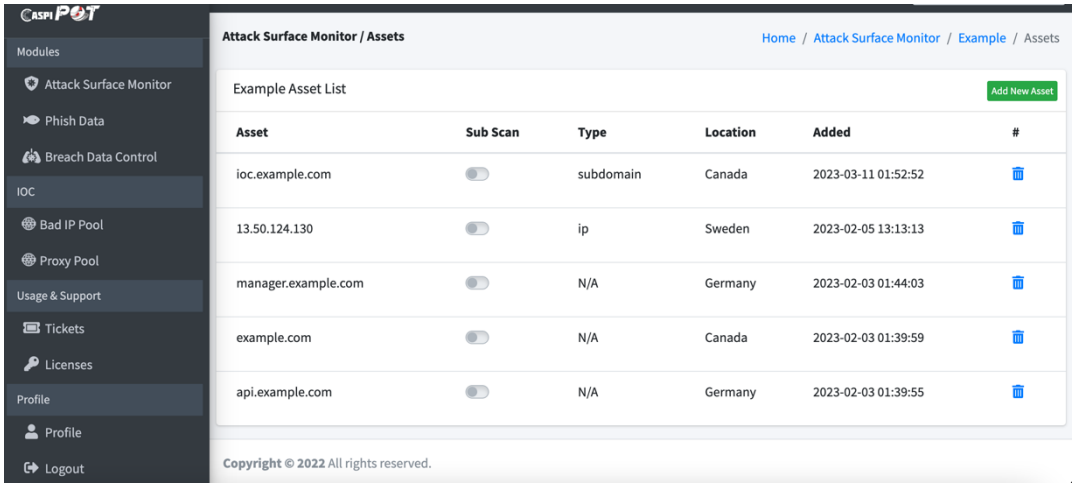


Attack Surface Monitor Configuration Guide

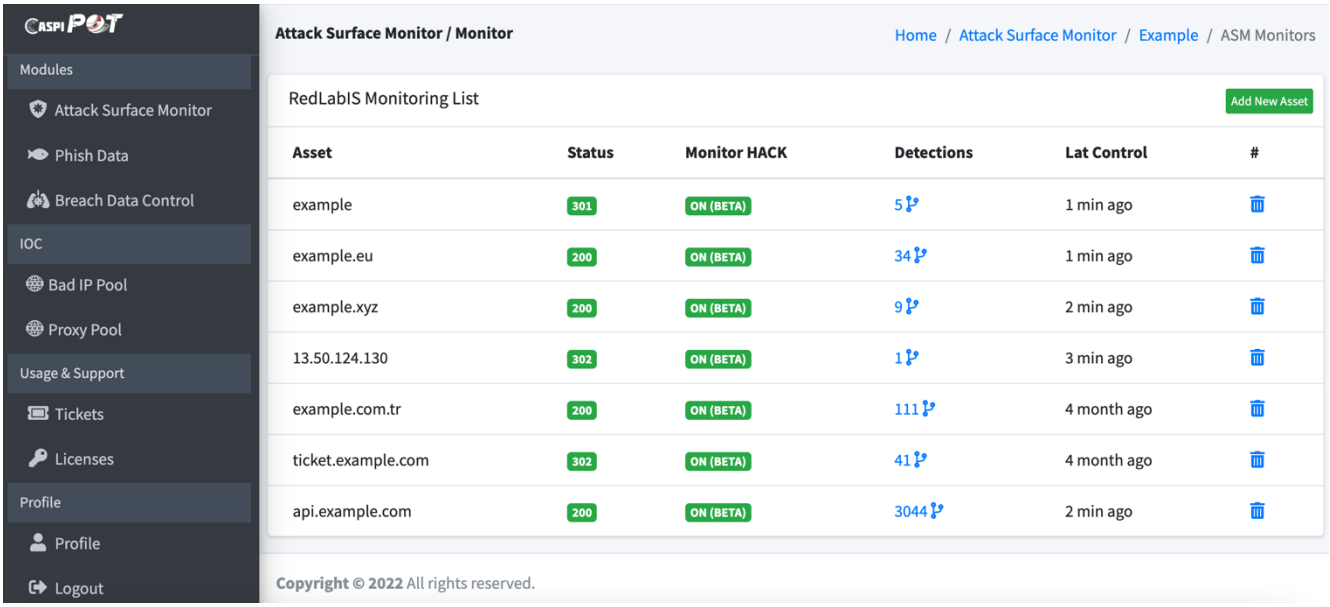
To activate attack surface management services via **the manager panel || Modules >> Attack Surface Monitor** field should be reached.

In order to define services, it is necessary to complete at the *"Total Assets "* **domain name** and **IP address** service completely. CaspiPoT security guard will automatically scan and add subdomains to the system.

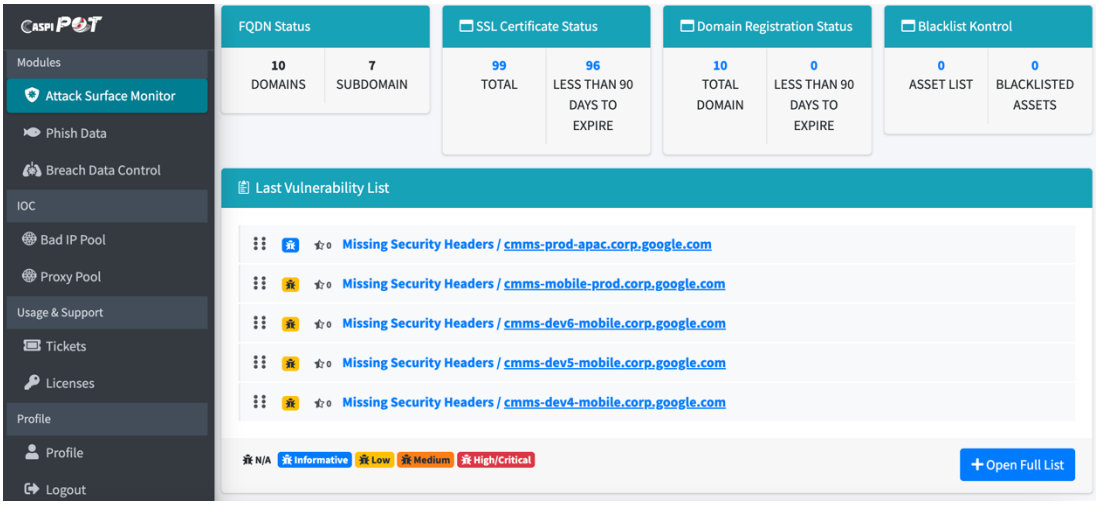




Asset Monitor allows you to monitor the health status of all your inventory that provides internet service that is open to the world. **The manager panel || Modules >> Attack Surface Monitor >> Asset Monitor** field should be reached.



With the correct entry of the information, the system will automatically scan the **Service**, **Port**, **Vulnerability** information of the added asset and display the results in a short time.

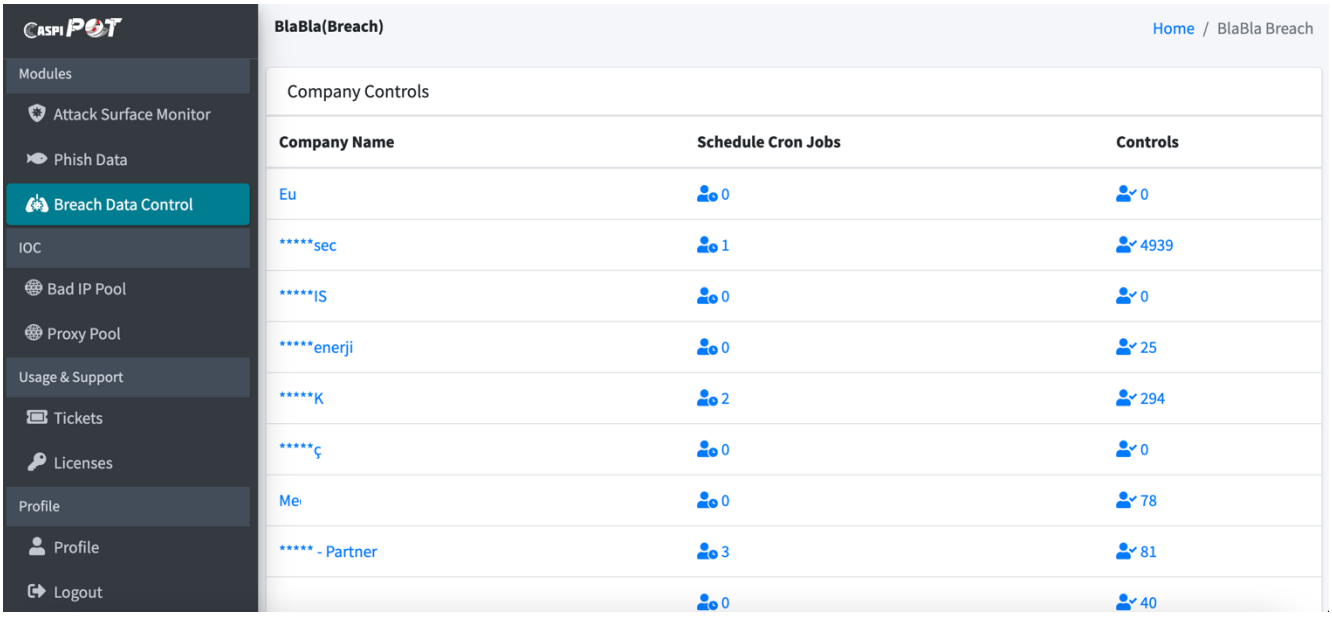


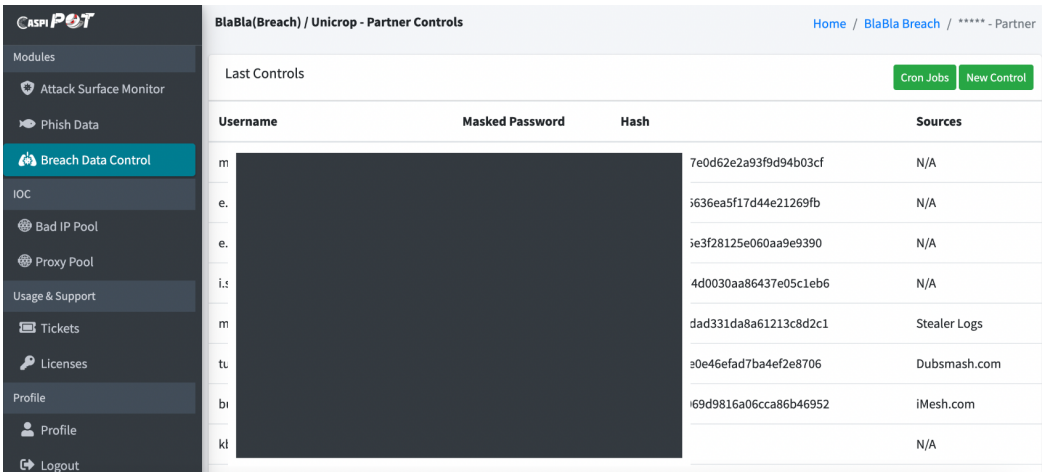
Breach Data Control Configuration Guide

To activate breach data services via **the manager panel || Modules >> Breach Data Control** field should be reached.

When the stolen data area is accessed, the company lists defined for you will be displayed automatically. While you access the company field you want to process, the **domain names** that have been given permission for the company are displayed.

You can view *existing stolen* data by creating a new **Check Leaked Password** . By defining scheduled tasks and making these searches continuous, you are aware of a potential data leak.

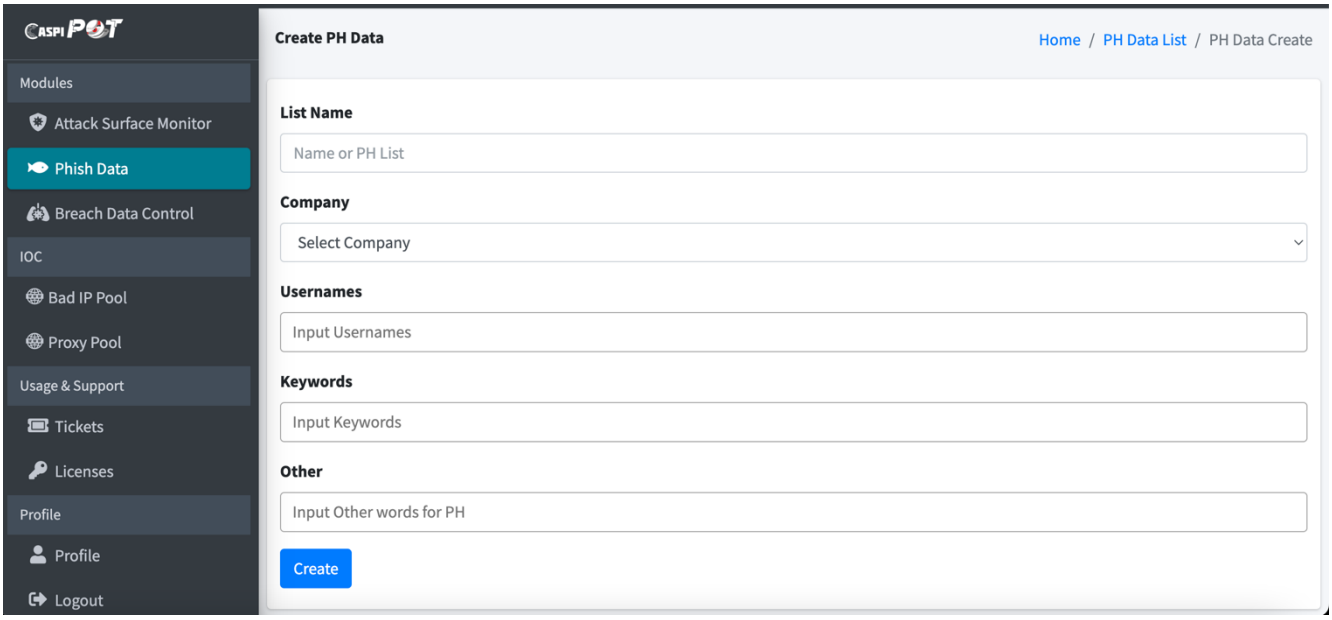




Phish Data Configuration Guide

To activate attack phish data services via **the manager panel || Modules >> Phish Data** field should be reached.

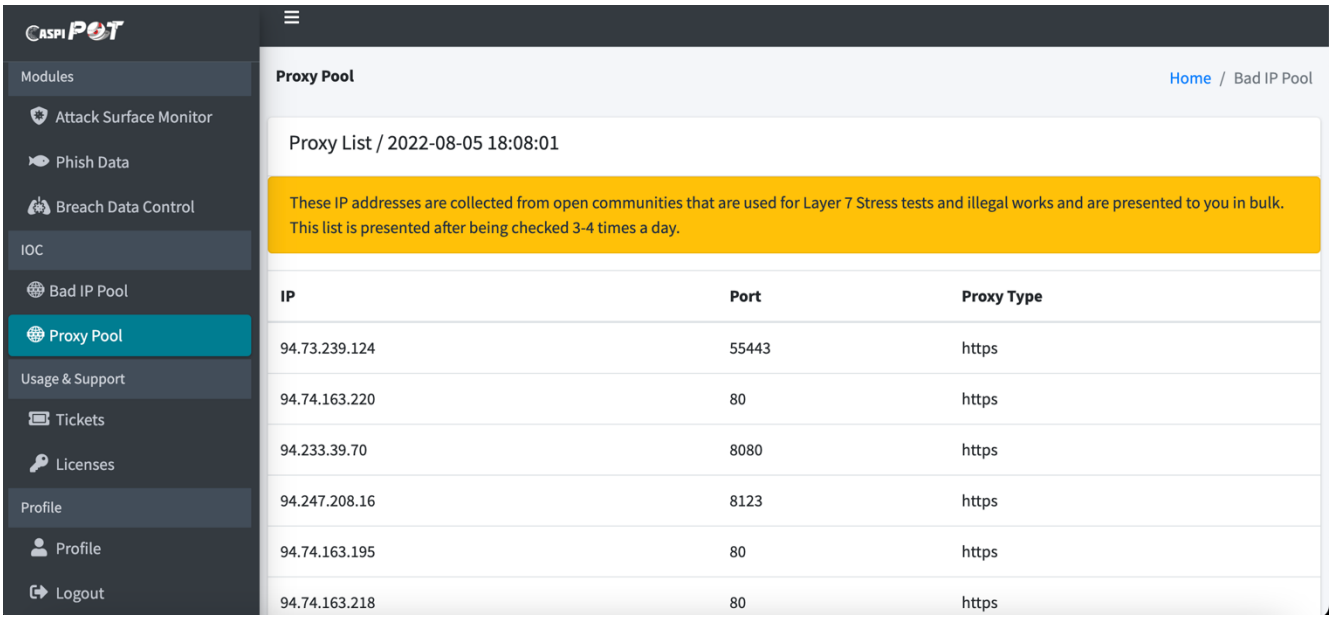
Use the *Create* tab to search for a new PH data.



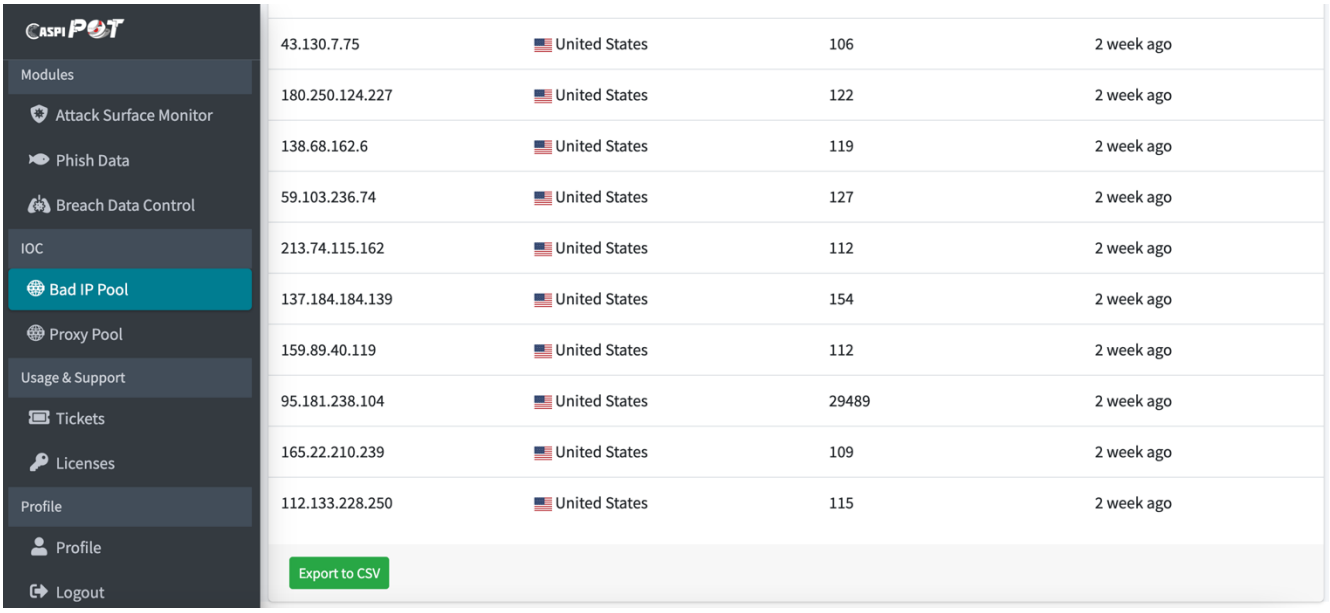
IOC's Data Usage Guide

IOC's services via **the manager panel || IOC** field should be reached.

IOC data can be accessed under the **the manager panel || IOC >> Bad Ip Pool&Proxy Pool** tab.



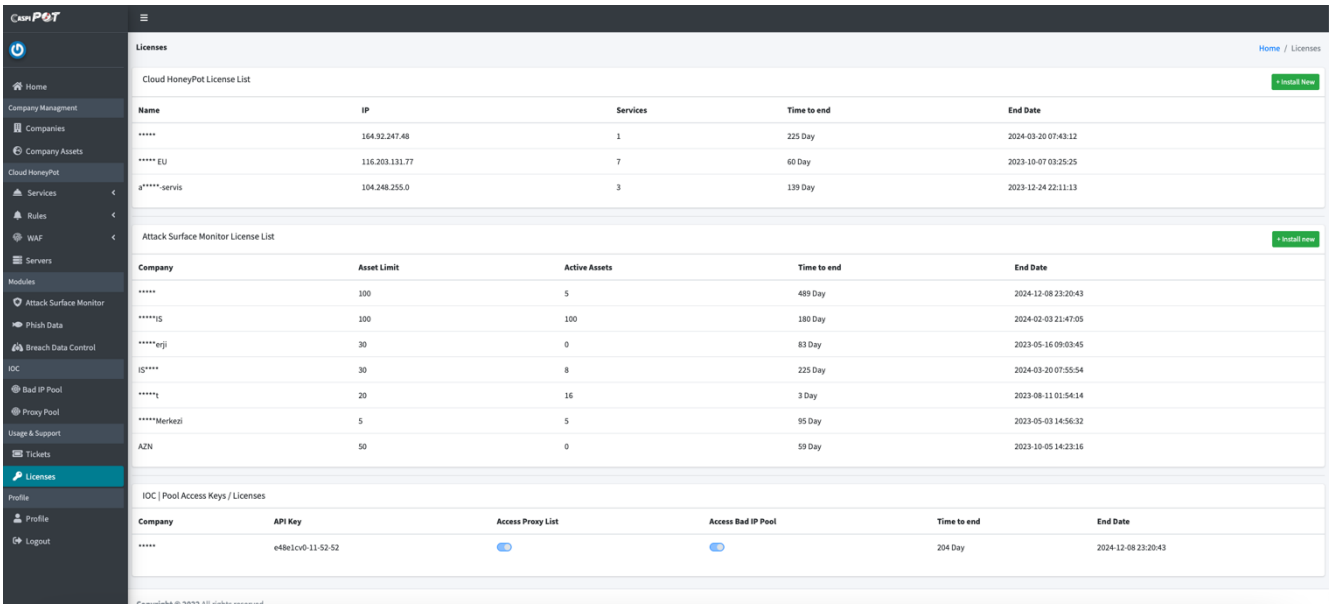
Use the *Export CSV or API integration* to collect for a new IOC's.



ADMINISTRATION GUIDE

Licences

To activate licences via **the manager panel || Usage&Support >> Licenses** field should be reached. All license management of the application is performed on this panel.



License addition, deletion, new license request and modification operations are done here.

Tickets

To send any request and information via **the manager panel || Usage&Support >> Tickets** field should be reached.

CaspiPoT