CATCH PROBE™

OTD BİLİŞİM
GLOBAL VAD

ABOUT US

CATCHPROBE is an internationally recognized technology company that provides actionable web intelligence, OSINT, deception systems, threat intelligence, and digital crime analytics solutions and products through the world's first AI-Driven SaaS-based centralized and autonomous intelligence platform. (Intelligency Suite, version IDA Mountain)

CATCHPROBE is an enhanced centralized actionable intelligence orchestration platform for intelligence gathering, enrichment, deception, profiling or creating targeting, semantics, and attribution solutions. It collects all the intelligence needed to prevent potential threats, enrich your data, correlate across sources, produce reports, and streamline threat prevention using the intelligence it obtains for accurate analysis.

In addition to verified threat intelligence data collected from public and private sources, deception systems (AI-Based Autonomous Deceptions), leaked data (Leak DBs) and dark/deep web resources are also used by CATCHPROBE and accessed through the centralized interface.

One Platform for All Your Needs

CATCHPROBE offers web intelligence, threat intelligence, detection, deception and leaked data profiling services, and response features deployed on the same platform, working fast and in harmony with each other.

What CatchProbe Does

Analogous to how you would monitor your home with a camera, you must do the same with your data in the digital world. The camera can't prevent a break-in, but it can help you know who did it, and what they did. While you might not have control over everything that goes on in the digital world, you can protect yourself by being aware and using a combination of tools to take precautions and, more importantly, to prevent damage. Our product provides an amazing platform for institutions, governments, and individuals because everyone needs verified intelligence.

WHAT CATCHPROBE HAS TO OFFER

Through the development of seamlessly integrated modules, each with its own specialized purpose that complements and enhances the capabilities of others, we have created a unique and unified ecosystem for verified and actionable intelligence, offering a comprehensive suite that enables what others can’t:

Effective communication between intelligence and security.

DarkMAP, our web intelligence platform powered by AI, empowers analysts with the ability to effectively identify and counteract cyber threats that specifically target their operations. Housing an extensive repository of 6.7 petabytes of raw data, DarkMAP executes keyword-based explorations across all web layers, delivering comprehensive results within a swift 48-hour timeframe.

Particularly in operational technology environments, SmartDECEPTIVE plays a pivotal role by providing sophisticated deceptions. These decoys enable the identification and profiling of threat actors, safeguarding critical infrastructure from potential attacks.

Seamlessly integrating with existing SIEM/Firewall systems, ThreatWAY automates the incident response process, minimizing response time and enhancing the overall efficiency of security operations. Moreover, ThreatWAY facilitates access to the last decade’s Indicators of Compromise (IoCs).

LeakMAP is a comprehensive solution for exploring and analyzing a vast leak database, comprising over 1 petabytes of profiled and mapped data.

RiskROUTE is our attack surface management module that performs comprehensive IP and port scans, detects phishing and proactively discovers past IP vulnerabilities and potential security threats.

DarkMAP
Web Intelligence

CatchProbe **DarkMAP** is not just a simple platform where you can feed on intelligence information. It brings you to the forefront of next-generation defense technologies with its strong analysis capabilities, data enrichment, and infrastructure driven by artificial intelligence.

One objective of **DarkMAP** is to enable exploration and indexing across all layers of the Internet: Social Media, DeepWeb, and DarkNet. DarkMap can archive the targeted pages without missing any content and has the ability for automated content tracking and discovery processes.

Another differentiating factor of **DarkMAP** from other WEBINT products is its fast setup, low cost, and the ability to escalate and delegate tasks among analysts and departments. Additionally, **DarkMAP** presents the collected content in a functional, simple, and comprehensive manner, enabling analysts to effortlessly conduct their research.

Features:

- Threat group association through keyword analysis
- Blind spot detection on the dark net using iterative link analysis
- Flow management feature for membership-requiring platforms like forums, IRC groups, and Telegram groups
- Multilingual resources translated into English.
- Real-time threat analysis
- Crime and criminal analysis with cross-case analytics insights using CrimeGround
- Low-cost and high-efficiency with SaaS infrastructure

Overview

Tree Branch Methodology

Unique Technology

SaaS Based Platform

Easy to Use

AI and Next-Gen Analysis

Proactive Defense Capabilities

IOC and threat discovery using regular expressions

Attacker analysis facilitated by WebInt platform

Event-based risk analysis for analysts

Escalation and delegation process for analysts

Detailed authorization protocols among departments and analysts

GAIN SPEED & TIME

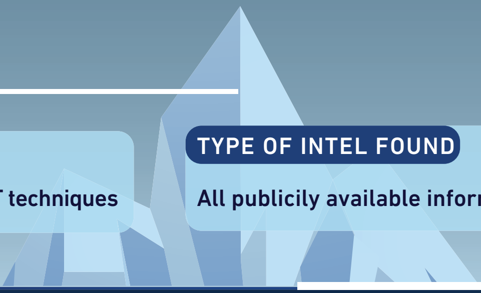
GET CRITICAL INSIGHT

FIND EMERGING THREATS

EXPLORE THE DEEP

OTD BİLİŞİM
GLOBAL VAD

DARKMAP: NAVIGATING THE DIGITAL DEPTHS



SURFACE WEB

INTEL COLLECTION EFFORT: MINIMAL

Web scraping tools, search engine API's and OSINT techniques

TYPE OF INTEL FOUND

All publicly available information

DEEP WEB

INTEL COLLECTION EFFORT: MODERATE

Data extraction from APIs, databases or password-protected environments.

TYPE OF INTEL FOUND

- Corporate and government databases
- Subscription-based research or news sites
- Intranets or organizations

VALUE

Offers valuable, exclusive information such as private discussions.

DARK WEB

INTEL COLLECTION EFFORT: HIGH

May involve social engineering, linguistics expertise and ethical hacking.

TYPE OF INTEL FOUND

- Stolen credentials and credit card numbers
- Cybercrime toolkits (malware, ransomware)
- Illicit marketplaces (drugs, weapons, counterfeit goods)

VALUE

- Essential for organizations concerned about data breaches or illicit transactions.
- Can reveal upcoming cyberattacks, vulnerabilities being sold or new criminal trends.

ANONYMOUS NETWORKS (TOR, I2P, YGGDRASIL)

INTEL COLLECTION EFFORT: VERY HIGH

Requires advanced undestanding of specific network tools. Infiltration may require building trust with communities.

TYPE OF INTEL FOUND

Highly encrypted communication channels and marketplaces that cater to illegal activities

VALUE

Useful for tracking illegal activities and securing proprietary data.

DECENTRALIZED WEB PROJECTS (FREENET, ZERONET)

INTEL COLLECTION EFFORT: VERY HIGH

Requires specializied tools.
Monitoring activities requires continuous participation.

TYPE OF INTEL FOUND

- Websites offering discussions on sensitive topics
- Censored information or communications
- Development and exchange of tools

VALUE

- Useful for tracking illegal content.

COMMUNICATION CHANNELS (ENCRYPTED MESSAGING APPS)

INTEL COLLECTION EFFORT: VERY HIGH

Often requires social engineering, access to invitation-only forums, or real-time monitoring of encrypted channels.

TYPE OF INTEL FOUND

- Discussions on cyberattack coordination or tactics
- Trading of stolen data or illegal content
- Encrypted communications between criminal actors

VALUE

Critical for real-time threat detection, cybersecurity, and tracking disinformation campaigns or illegal activity coordination.
Offers early warning for organizations or law enforcement regarding impending attacks or fraud schemes.

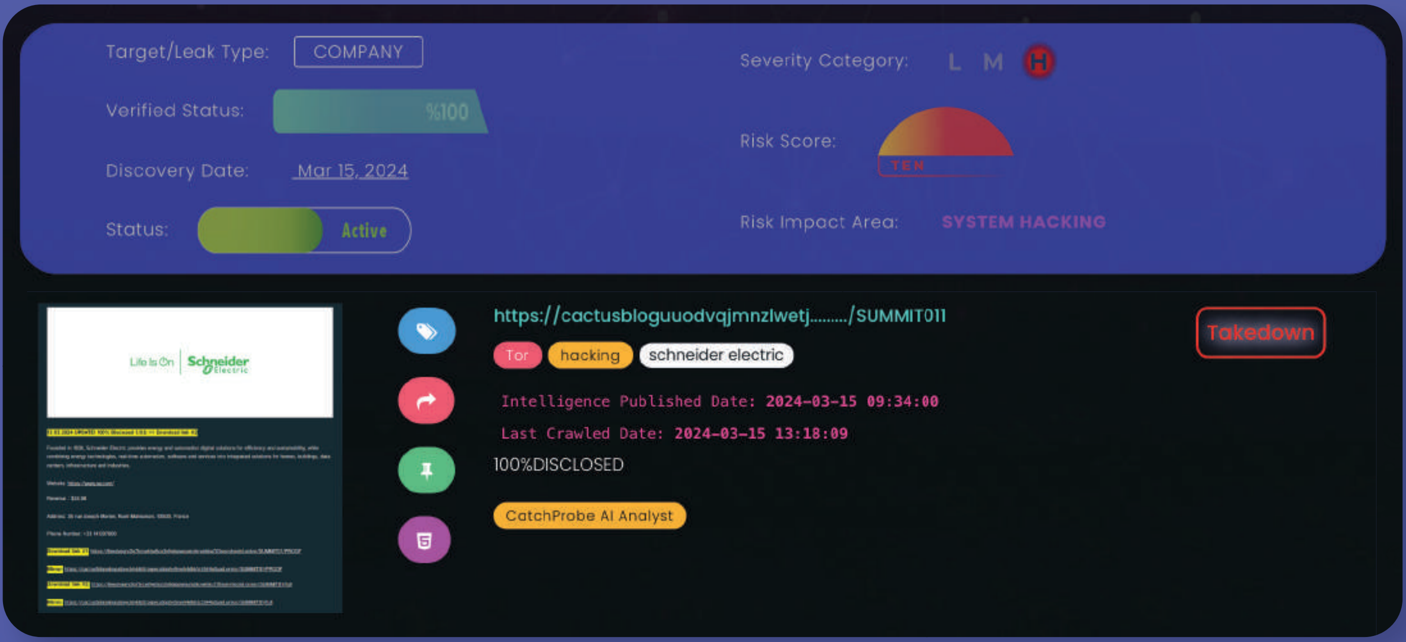
DARKMAP: Redefining Web Intelligence with Al and Next-Gen Capabilities

CatchProbe DarkMAP module enables precise. actionable intelligence across all layers of the internet facilitating advanced threat detection. analysis. and escalation for cybersecurity professionals.

Key Differentiators

Al-Based Assessment:

DarkMAP's Al infrastructure assesses nndings in real time, generating detailed insights on threat severity, allowing for immediate prioritization and action.



Target/Leak Type: COMPANY

Verified Status: %100

Discovery Date: Mar 15, 2024

Status: Active

Severity Category: L M H

Risk Score: TEN

Risk Impact Area: SYSTEM HACKING

https://cactusbloguuodvqjmnzlwetj........./SUMMIT011

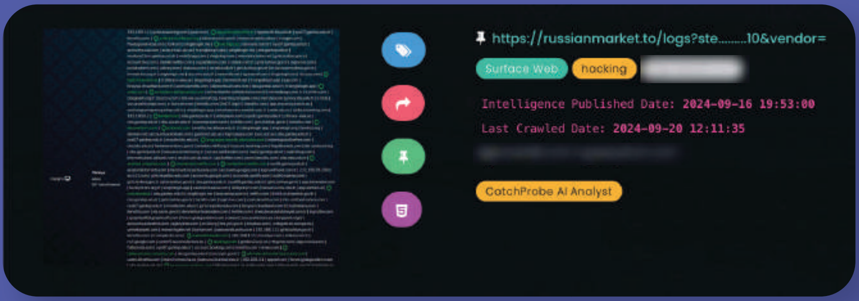
Tor hacking schneider electric

```
Intelligence Published Date: 2024-03-15 09:34:00
Last Crawled Date: 2024-03-15 13:18:09
```

100%DISCLOSED

Flow Management & Page Restriction Bypass:

Capable of handling restricted or membership-based platforms, DarkMAP bypasses restrictions to ensure full data access across all layes of the web.



https://russianmarket.to/logs?ste.........10&vendor=

Surface Web hacking [redacted]

```
Intelligence Published Date: 2024-09-16 19:53:00
Last Crawled Date: 2024-09-20 12:11:35
```

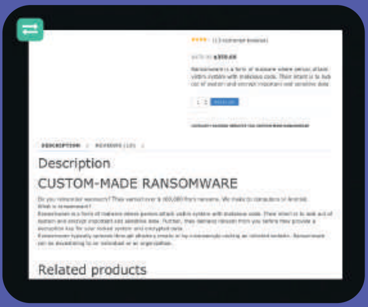
[redacted]

Additionally, DarkMAP can automatically acquire data within the pre-set budget allocated by CatchProbe.

Content Archiving

DarkMAP archives crawled data in screenshot format, ensuring future accessibility and documentation for retrospective analysis.

⇄ Additionally, if any changes are detected in the content after the initial crawl, users are alerted with a button in the top left corner.



Description

CUSTOM-MADE RANSOMWARE

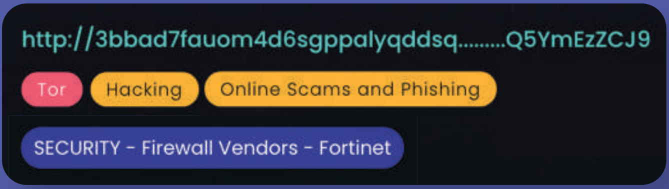
Related products

Multilingual Translation

Not all threat intelligence data is in English-many threat actors operate using languages such as Russian, Korean, and others. DarkMAP automatically translates resources from these languages, enabling comprehensive, actionable insights across language barriers.

Vendor Research Without Limits

DarkMAP allows limitless tracking of vendors to monitor vulnerabilities, without any restrictions tied to license limits.



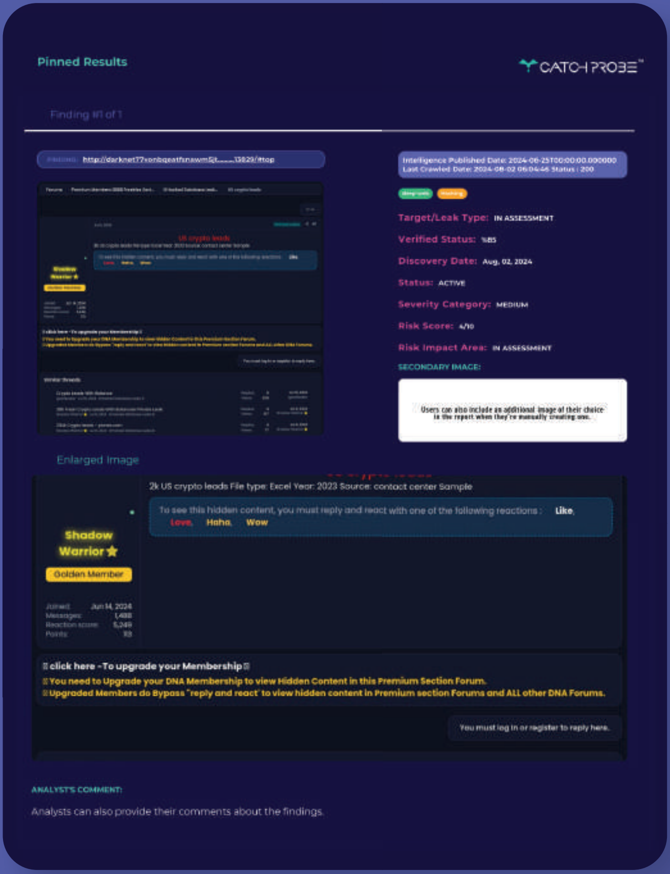
http://3bbad7fauom4d6sgppalyqddsq........Q5YmEzZCJ9

Tor
Hacking
Online Scams and Phishing
SECURITY - Firewall Vendors - Fortinet

Automated and Manual Report

Users can conhgure automated email alerts in PDF format for new hndings, specifying when, how (e.g., based on risk score). and who should receive them.

Additionally, users can manually generate detailed reports directly from the module.



http://darknet77vonbqeatfsnawm5jt......13829/#top

Intelligence Published Date: 2024-06-25T00:00:00.000000
Last Crawled Date: 2024-08-02 06:04:46 Status : 200

Target/Leak Type: IN ASSESSMENT

Verified Status: %85

Discovery Date: Aug, 02, 2024

Status: ACTIVE

Severity Category: MEDIUM

Risk Score: 4/10

Risk Impact Area: IN ASSESSMENT

SECONDARY IMAGE:

Users can also include an additional image of their choice in the report when they're manually creating one.

Enlarged Image

2k US crypto leads File type: Excel Year: 2023 Source: contact center Sample

To see this hidden content, you must reply and react with one of the following reactions : Like, Love, Haha, Wow

Shadow Warrior ★

Golden Member

Joined:	Jun 14, 2024
Messages:	1,488
Reaction score:	5,249
Points:	113

click here -To upgrade your Membership

You need to Upgrade your DNA Membership to view Hidden Content in this Premium Section Forum.

Upgraded Members do Bypass "reply and react" to view hidden content in Premium section Forums and ALL other DNA Forums.

You must log in or register to reply here.

ANALYST'S COMMENT:

Analysts can also provide their comments about the findings.

Escalation, Delegation, and Confidentiality

DarkMAP's platform architecture enables seamless delegation of tasks between teams and departments, optimizing workflow and collaboration.

Additionally, admins can set specihc information, such as subsidiary related keywords or executive names, to remain conhdential, ensuring only authorized personnel have access. Future related hndings are automatically protected, maintaining strict control over data.

LeakMAP
Open-Source Intelligence Platform

LeakMAP differs from other leak database platforms in that it correlates the relationships between leaked content by profiling and mapping the content collected in our database.

Organizations can use LeakMAP to get background information on a potential employees, to prevent any misuse of work emails and to easily search for any potential leaks. And this way organizations can prevent hackers from orchestrating sophisticated phishing campaigns or crafting convincing social engineering attacks, or worse, compromising business emails or utilizng leaks.

Overview

Breach Tracking

Exposed Corporate Credentials Tracking

Prevent Credential Stuffing Attacks

Criminal Investigation Process

Usernames & Passwords

Credit Cards

Company Documents

Photos

Audios

ID Cards

Passports

Phone Numners

Social Media Profiles

Features:

- LeakMAP seamlessly integratess with SMARTDECEPTIVE, providing you with timely alerts regarding targeted attacks. Moreover, it integrates with DARKMAP, to automatically bolster its leaked sources.
- Correlative Functional Search (for example, retrieve the information of individuals whose identification numner starts with 43, whose registered vehicle's license plate contains AB, or whose phone numner ends with 94).
- Full text search.
- GDPR-compliant data display.

FIND ECPOSED CREDENTIALS

GATHER INTELLIGENCE

PREVENT CREDENTIAL STUFFING ATTACKS

TRACK .BREACHES

OTD BiLiŞiM
GLOBAL VAD

LEAKMAP: MAPPING THE DARK WEB'S LEAK LANDSCAPE

TYPES OF LEAKS

TYPE OF LEAKS

- Credentials
  Emails
  Usernames
  Passwords
- Financial Data
  Credit Card Numbers
  Bank Info
- Personal Identifiable Information
  Phone Numbers
  ID Cards
  Social Security Numbers
- Corporate Documents
  Contracts
  Trade Secrets
  Strategic Plans

WHY IT MATTERS

WHY PROACTIVE LEAK DETECTION MATTERS

- Immediate Threat Mitigation
Identifying and addressing leaked information before attacks occur
- Risk Profiling and Damage Control
Building defensive strategies based on the nature of the leak
- Corporate Data Protection
Ensuring that internal and customer data remains secure

HOW LEAKS OCCUR

HOW LEAKS OCCUR

- Phishing Attacks
- Weak Passwords & Poor Authentication Practices
- Third-Party Vendor Breaches
- Insider Threats
- Social Engineering
- Malware & Ransomware

POTENTIAL IMPACT

POTENTIAL IMPACT ON ORGANIZATIONS

- Financial Loss
  Fraud
  Fines
  Legal Fees
- Reputation Damage
  Loss of Customer Trust
- Compliance Violations
  GDPR
  HIPAA
  PCI
  DSS
- Operational Disruptions
  Data Corruption
  System Downtime
- Targeted Attacks
  Future Exploitation Through Exposed Data

PREVENTATIVE MEASURES

PREVENTATIVE MEUSURES FOR ORGANIZATIONS

- Use of Advanced OSINT Tools like LeakMAP
- Integration of Decoy Systems to Deflect Targeted Attacks
- Regular Security Audits and Vulnerability Assessments
- Encryption of Sensitive Data
- Employee Cybersecurity Training

EMERGING TRENDS IN DATA LEAKS

EMERGING TRENDS IN DATA LEAKS

- Supply Chain Attacks: Attackers are increasingly targeting third-party vendors, service providers, or contractors to gain access to the larger organizations they serve. Recent breaches have shown how a single vendor compromise can lead to widespread exposure of sensitive information, highlighting the need for companies to not only secure their own systems but also monitor their partners.

- Double Extortion Attacks: In double extortion attacks, companies are hit with two simultaneous threats: first, encrypted data that disrupts operations, and second, the exposure of stolen information if a ransom isn't paid. Attackers use industries' vulnerability to disruption to increase the pressure to pay.

- Corporate Espionage and Insider Leaks: Insider threats remain a critical concern as employees with access to sensitive data may leak information either maliciously or accidentally. With remote work on the rise, these threats are even harder to detect.

- Leak Farming by Cybercrime Gangs: Some cybercrime groups, such as the infamous Maze ransomware group, systematically target multiple organizations to collect and release sensitive data over time.

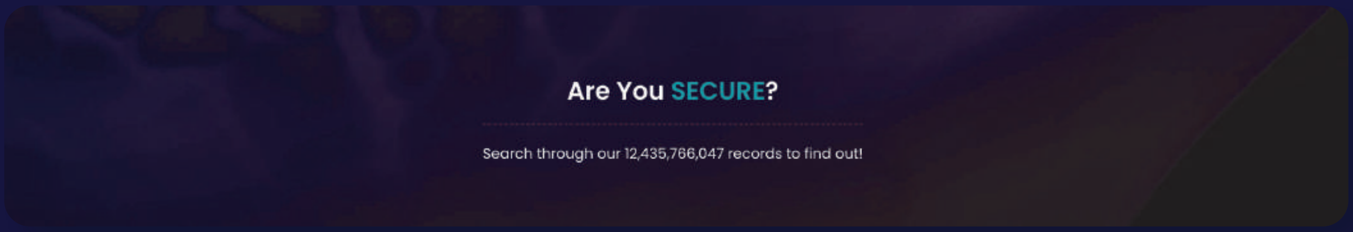
LEAKMAP: Managing Data Breaches with Precision

CatchProbe LeakMAP is the largest. continuously expanding database for identifying and analyzing leaked data. providing organizations with real-time insights and alerts. Powered by a sophisticated mapping technology and integrating with SmartDECEPTIVE decoys. it enables deep profiling and proactive defense against targeted attacks.

Key Differentiators

Comprehensive Leak Collection

Largest and continuously growing database of leaked credentials. financial data. PII. and corporate documents. Regular updates and expansions to ensure timely identification of newly leaked information.

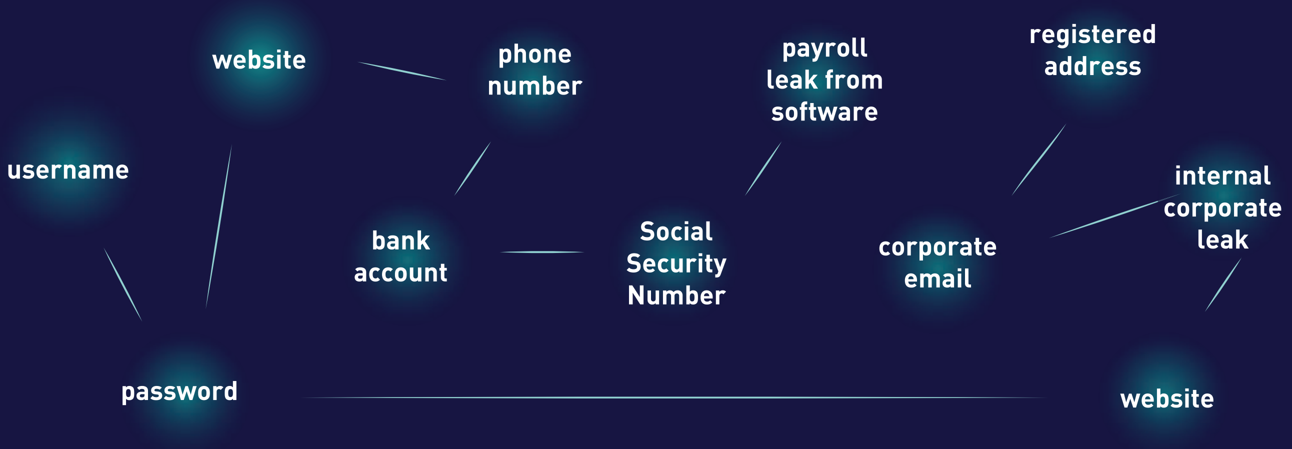


Are You SECURE?

Search through our 12,435,766,047 records to find out!

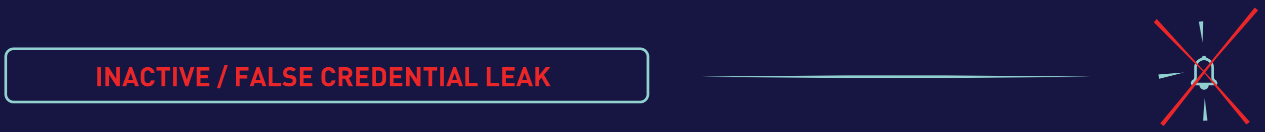
Deep Profiling and Analysis

Advanced capability to correlate leaked content. enabling comprehensive profiling of leaks and potential targets.



Automated Credential Validation

LeakMAP can automatically test leaked usernames and passwords. identifying and deleting inactive or false credentials from its database. saving your team time and effort in verification while focusing on real threats.



OTD BİLİŞİM
GLOBAL VAD

CATCH PROBE™

INTELLIGENCE TECHNOLOGIES

SMARTDECEPTIVE

OTD BİLİŞİM

GLOBAL VAD

SMARTDECEPTIVE: KEEPING ATTACKERS IN THE DARK

HOW DECEPTION TECHNOLOGIES WORK

Deception technology refers to the deployment of decoy systems and traps designed to mimic legitimate network assets, services, or data. These decoys are strategically placed to lure attackers, diverting them from real systems while gathering intelligence on their behavior. Deception solutions actively engage adversaries without jeopardizingt he actual network, capturing critical data such as IP addresses, attack methods, tools and domain names.

HOW DECEPTION TECHNOLOGIES WORK

- Decoys and Traps: These decoys can take the form of devices, servers, endpoints, or applications that appear genuine but are designed to deceive attackers.
- Engagemen otf Attackers: Once an attacker interacts with a decoy, the system collects valuable information about their tactics, techniques and procedures (TTPs).
- Real-Time Monitoring and Alerts: Security teams receive alerts the moment decoys are engaged, allowing them to analyze the threat in real time.
- Data Collection and Analysis: The system captures and logs details such as IP addresses, attack vectors, and tools used, helping organizations bolster their defenses by understanding adversary behavior.

BENEFITS OF DECEPTION TECHNOLOGIES

- Proactive Defense:
  Deception solutions allow organizations to detect attackers early in the attack lifecycle before they can cause damage to real assets.
- Accurate Threat Intelligence:
  By engaging with attackers directly, deception technology provides highly specific data that enhances threat intelligence and response efforts.
- Low False Positives:
  Because decoys are not intended for normal network traffic, any interaction with them is likely malicious, minimizing false positives.
- Increased Incident Response Efficiency:
  Deception systems work in tandem with incident response platforms, escalating confirmed threats to security teams.

WHERE CAN THEY BE IMPLEMENTED?

- Internal Networks:
  Protect critical internal assets like databases and employee credentials by deploying decoys across various devices and servers.
- Cloud Environments:
  Secure cloud infrastructures by creating decoys that mimic cloud-based applications, containers, and virtual machines.
- IoT Systems:
  Protect IoT networks by deploying traps that simulate connected devices such as cameras, printers, or industrial control systems (ICS).
- Operational Technology (OT):
  Protect OT systems and critical infrastructure (such as SCADA systems) by using deception techniques tailored for industrial environments.

OTD BİLİŞİM
GLOBAL VAD

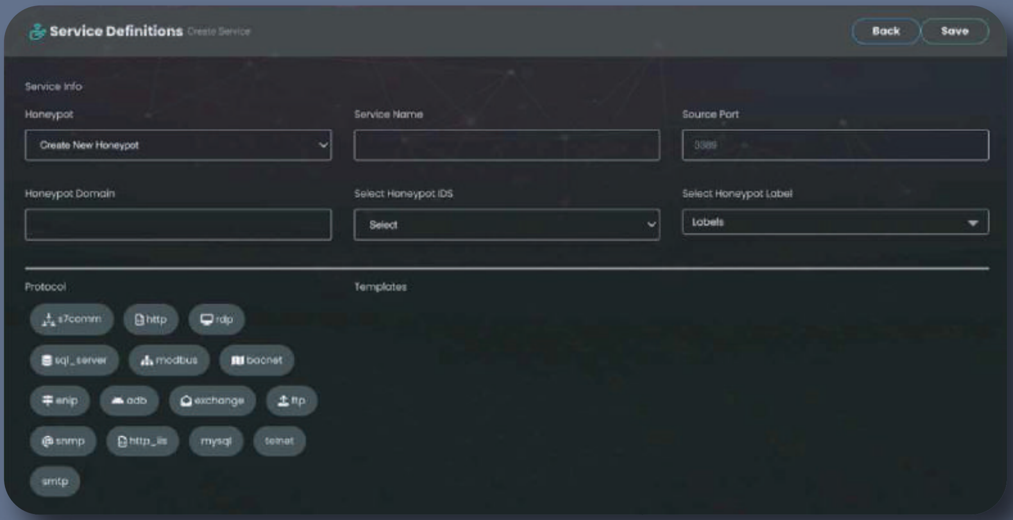
SMARTDECEPTIVE: Deception Technology for Real-Time Threat Intelligence

CatchProbe SmartDECEPTIVE is a comprehensive deception management platform designed to deploy and manage decoy traps, collect detailed cyber intelligence and monitor attacker activities in real time. It integrates seamlessly with ThreatWAY and LeakMAP to deliver actionable insights for protecting organizations.

Key Differentiators

Rapid Deployment

Decoys can be deployed in under minutes, offering quick defense without the need for complex setups or extensive configurations.



Service Info

Honeypot: Create New Honeypot

Service Name:

Source Port: 3389

Honeypot Domain:

Select Honeypot IDS: Select

Select Honeypot Label: Labels

Protocol

Cross-Platform Setup

SmartDECEPTIVE supports a wide range of protocols and services.

DECOY OPERATING SYSTEM TYPES

Windows | Linux | Android | IoTs, Printers, Camera &

APPLICATIONS | CUSTOMIZABLE TO YOUR NEEDS

Microsoft

- Microsoft Exchange Server
- Microsoft IIS Server
- Microsoft SQL Server
- Microsoft RDP Server
- Microsoft Dynamics AX
- Microsoft Dynamics NAV
- Microsoft Sharepoint

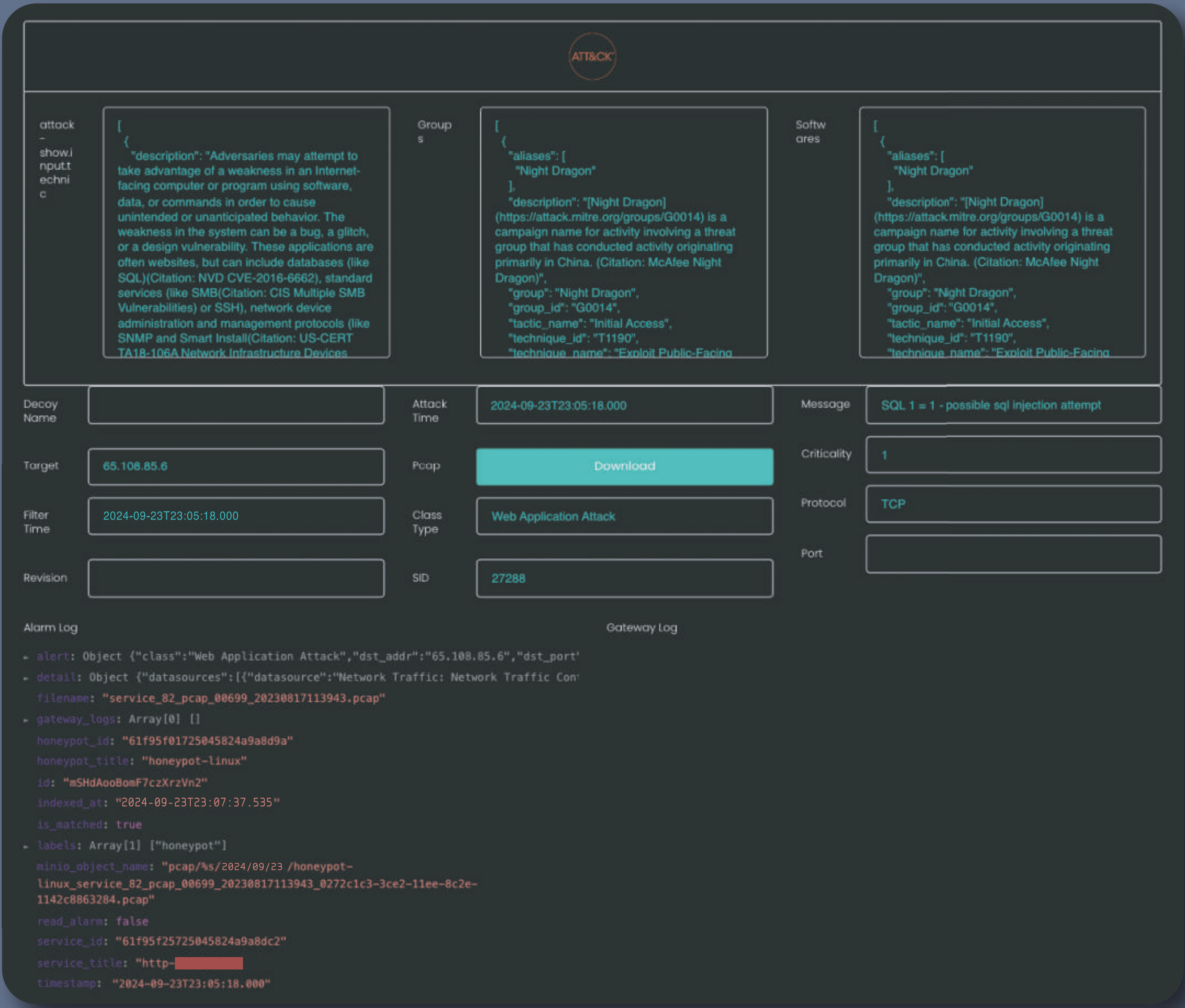
Linux

- HTTP
- SMTP
- FTP
- TELNET-DNS
- SSH
- SMB
- PhpMyAdmin

ICS/SCADA

- Modbus
- S7comm
- ENIP
- BACnet

- Mobile & Android
- Elasticsearch
- SAP
- FORTINET
- CHECKPOINT
- SOLARWINDS
- PASTEBIN
- On-Demand



attack-show.input.technic

```
[
  {
    "description": "Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL)(Citation: NVD CVE-2016-6662), standard services (like SMB(Citation: CIS Multiple SMB Vulnerabilities) or SSH), network device administration and management protocols (like SNMP and Smart Install(Citation: US-CERT TA18-106A Network Infrastructure Devices
```

Groups

```
[
  {
    "aliases": [
      "Night Dragon"
    ],
    "description": "[Night Dragon](https://attack.mitre.org/groups/G0014) is a campaign name for activity involving a threat group that has conducted activity originating primarily in China. (Citation: McAfee Night Dragon)",
    "group": "Night Dragon",
    "group_id": "G0014",
    "tactic_name": "Initial Access",
    "technique_id": "T1190",
    "technique_name": "Exploit Public-Facing
```

Softwares

```
[
  {
    "aliases": [
      "Night Dragon"
    ],
    "description": "[Night Dragon](https://attack.mitre.org/groups/G0014) is a campaign name for activity involving a threat group that has conducted activity originating primarily in China. (Citation: McAfee Night Dragon)",
    "group": "Night Dragon",
    "group_id": "G0014",
    "tactic_name": "Initial Access",
    "technique_id": "T1190",
    "technique_name": "Exploit Public-Facing
```

Decoy Name		Attack Time	2024-09-23T23:05:18.000	Message	SQL 1 = 1 - possible sql injection attempt
Target	65.108.85.6	Pcap	Download	Criticality	1
Filter Time	2024-09-23T23:05:18.000	Class Type	Web Application Attack	Protocol	TCP
Revision		SID	27288	Port	

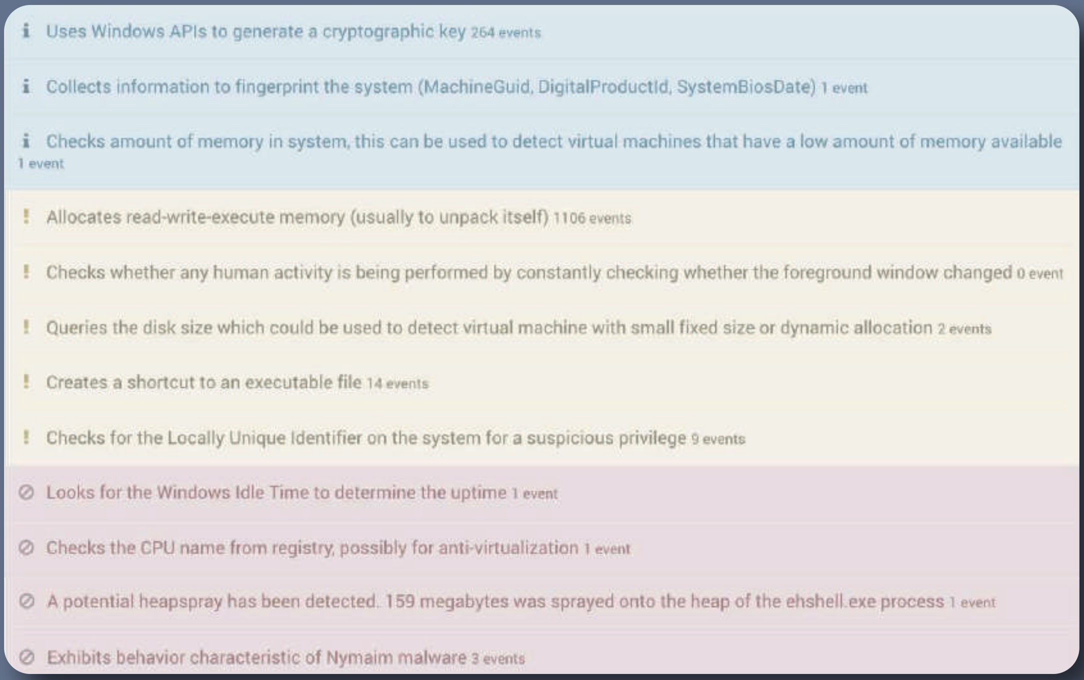
Alarm Log

Gateway Log

```
▸ alert: Object {"class":"Web Application Attack","dst_addr":"65.108.85.6","dst_port'
▸ detail: Object {"datasources":[{"datasource":"Network Traffic: Network Traffic Con'
  filename: "service_82_pcap_00699_20230817113943.pcap"
▸ gateway_logs: Array[0] []
  honeypot_id: "61f95f01725045824a9a8d9a"
  honeypot_title: "honeypot-linux"
  id: "mSHdAooBomF7czXrzVn2"
  indexed_at: "2024-09-23T23:07:37.535"
  is_matched: true
▸ labels: Array[1] ["honeypot"]
  minio_object_name: "pcap/%s/2024/09/23 /honeypot-
  linux_service_82_pcap_00699_20230817113943_0272c1c3-3ce2-11ee-8c2e-
  1142c8863284.pcap"
  read_alarm: false
  service_id: "61f95f25725045824a9a8dc2"
  service_title: "http-[redacted]
  timestamp: "2024-09-23T23:05:18.000"
```

Malware Analysis

Attackers can upload malware to these decoys, enabling customers to receive detailed analysis of the malware.



- i Uses Windows APIs to generate a cryptographic key 264 events
- i Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) 1 event
- i Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available 1 event
- ! Allocates read-write-execute memory (usually to unpack itself) 1106 events
- ! Checks whether any human activity is being performed by constantly checking whether the foreground window changed 0 event
- ! Queries the disk size which could be used to detect virtual machine with small fixed size or dynamic allocation 2 events
- ! Creates a shortcut to an executable file 14 events
- ! Checks for the Locally Unique Identifier on the system for a suspicious privilege 9 events
- ⊘ Looks for the Windows Idle Time to determine the uptime 1 event
- ⊘ Checks the CPU name from registry, possibly for anti-virtualization 1 event
- ⊘ A potential heapspray has been detected. 159 megabytes was sprayed onto the heap of the ehshell.exe process 1 event
- ⊘ Exhibits behavior characteristic of Nymaim malware 3 events

Other Key Features

Real-Time
Status Tracking

Long-Time
Unnoticed

Rich and Custom
Scenarios

Instant Setup

Full PCAP
Capability Feature

Data Enrichmet &
TTP Analysis

ICS Scenarios

Threat Profiling and
Reputation Ranking

Alerting & Reporting
Capabilities

Automated Malware
Analysis on SandBox

Exploit, Malware and
Shellcode Detection

Flexible Deployment

SmartDECEPTIVE decoys can be deployed on-premise or in the cloud.

Integration with ThreatWAY LeakMAP

SmartDECEPTIVE integrates with ThreatWAY for automated incident response and LeakMAP to detect targeted attacks, identifying any attempts to exploit leaked data for malicious purposes.

What is a Decoy System?

A decoy system is a cybersecurity mechanism designed to attract and trap potential attackers by simulating vulnerable systems or networks. Its primary purpose is to detect, deflect, or study hacking attempts, providing valuable insights into how attackers operate. Decoy systems appear as legitimate targets to cybercriminals, enticing them to engage with the deception, while allowing security experts to monitor their actions and gather critical data.

How Do Deception Systems Work?

A deception system operates by simulating a vulnerable system, network, or application environment to attract attackers and analyze their behavior. The decoy is set up to resemble a legitimate target, such as a server, application, database, or network service. It is populated with realistic but fake data, like user accounts, files, or network traffic, making it appear as a genuine system. Monitoring tools are integrated into the decoy to capture all incoming and outgoing traffic, including network packets, login attempts, and other interactions. Every action an intruder takes within the decoy is meticulously logged, including commands executed, files accessed or modified, and any malware dropped.

When an attacker engages with the decoy, the system records their methods and techniques. Low-interaction decoys may only simulate basic responses, while high-interaction decoys provide a more realistic environment. Real-time alerts can be set up to notify security personnel of suspicious activity detected within the deception system. The intelligence gathered helps identify new vulnerabilities, malware, and attack vectors, contributing to overall threat intelligence.

Benefits of Using Deception Technologies

There are several advantages to utilizing deception technologies in an enterprise network:

Early Threat Detection: Decoy systems can detect malicious activities before they reach critical systems, identifying new and emerging threats, including zero-day exploits that may bypass traditional security measures.

Threat Analysis: Deception traps provide detailed insights into attackers' tactics, techniques, and procedures (TTPs). Understanding these behaviors helps organizations develop more robust defense strategies and enhances overall threat intelligence.

Distraction and Deception: Traps can divert attackers’ attention and waste their time and resources, pulling them away from actual targets. These systems can also detect malicious insiders by enticing them to interact with decoy elements.

Efficient Resource Allocation: Deception technologies allow for a more focused allocation of security resources, concentrating efforts on genuine threats and reducing the need for broad, generalized defenses.

Types of Decoys

Research Decoys: Used to study attack patterns, malware behavior, and new exploits. These decoys gather intelligence for research, rather than direct defense.
Example: A network of decoys set up to monitor botnet activity.

Production Decoys: Deployed to enhance security by detecting intrusions early. They serve as an alert system for real threats.
Example: An email server decoy set up to catch phishing attempts.

SmartDECEPTIVE

CATCHPROBE™

ARE THERE ANY RISKS?

Aspect	Traditional Honeypots	SmartDECEPTIVE Decoys
Detection by Attackers	Can be detected by skilled attackers	Highly interactive, detection nearly impossible
Escalation of Attacks	Risk of escalation if not isolated	No interaction with actual system, no escalation risk
Resource Demand	Requires significant resources	Deployed on cloud, no resource demand
Resource Demand	Requires significant resources	Deployed on cloud, no resource demand
False Positives	Leads to false positive fatigue	AI-driven assessment of attacks
Performance Issues	Can affect network performance	Deployed on cloud, no network performance impact
Misconfiguration	Risk of introducing new vulnerabilities	No misconfiguration risks
Overreliance	May lead to overreliance on decoys	Part of a platform with four other modules for resilience

OTD BİLİŞİM
GLOBAL VAD

SmartDECEPTIVE CATCHPROBE™

UNDERSTANDING THE HACKER'S POINT OF VIEW

Initial Reconnaissance: Let me show you how I find my way in

OSINT, SIGINT, HUMINT – all the classics.

Google? It's your best buddy...and mine.
Forums? They're gold mines. From official Cisco or Oracle ones to random developer hangouts, they're packed with insights.

GitHub? Jackpot.
Compromise databases and Pastebin? Both super generous with info.

Nmap and Shodan? Absolutely your real friends, but they're my best pals when it comes to finding exposed systems.

CVE database? Always handy.

Actual threat intelligence feeds? Some are gold, some are garbage—but the good ones are game-changers.

With this arsenal (and then some), it's shockingly easy to build a complete picture of "you"—who you are, where you work, what you do, and most importantly, what will make you click on something or engage in a conversation.

Initial Compromise: Let me show you the ways I get in...

Phishing? Classic. I'll slip into your inbox with a convincing email and make you hand over everything.

Social Engineering? I'll sweet-talk my way in through your phone, chat, or even face-to-face—trust me, I know how to play the game.

Credential Stuffing? You reuse passwords? Perfect. I'll grab leaked credentials and see what else I can break into.

Brute Force? I've got automated tools ready to guess your passwords—no sleep for me.

OTD BİLİŞİM
GLOBAL VAD

Zero-Day Exploits? If there's a vulnerability nobody's found yet, I'll be the first to use it against you.

Trojans? It looks legit, but I've hidden malicious code inside, just waiting for you to install it.

Credential Stuffing? You reuse passwords? Perfect. I'll grab leaked credentials and see what else I can break into.

Brute Force? I've got automated tools ready to guess your passwords—no sleep for me.

Ransomware? I'll lock up your files and charge a fortune for their return—better pay up.

Man-in-the-Middle? If you're on public Wi-Fi, I'll intercept everything you do, without you noticing.

SQL Injection? Those insecure web forms? I'll use them to dig deep into your database.

Cross-Site Scripting (XSS)? You'll load a web page, and boom—I've injected malicious scripts to steal your info.

Remote Code Execution? Found a hole in your system? Great, I'll run my malicious code remotely and take over.

Exploit Kits? I've got a toolkit ready to scan for weaknesses and exploit them automatically—easy peasy.

Oh, come on, do I really need to list them all?...

Here's what I'd do after I get in: I'll intercept antivirus requests by pretending to be the OS, modify my code every time I infect a new machine, and encrypt myself inside executable files to stay hidden. With a polymorphic engine, I rewrite key parts of my code during each infection, and if I'm feeling ambitious, I'll go full metamorphic and completely rewrite myself for every target. Next, I'll scan your network, map out DNS, DHCP, and servers, trace routes between hosts, and check out MAC addresses. I'll also dig into Netstat for connections and NBTStat for names and IPs. Once I've got that, I'll enumerate DNS names, NetBIOS names, user accounts, MAC addresses, network adapters, shares, and services to see exactly what I'm dealing with. Now that I know the landscape, I can use all this intel to make my next move.

Post-Compromise: What Could You Have Done to Stop Us?

Firewalls? Sure, those are great—unless you're bombarded with IoCs. (Hey... you, yes you, my dear customer, they don't know ThreatWAY filters irrelevant IoCs and scores risks, so your firewall isn't overwhelmed!)

IDS/IPS? Bypassed. We know how to slip past without setting off alarms.

DLP? Left a port open, didn't you? We'll just slip data right through. (If only they knew RiskRoute would've flagged those open ports instantly!)

Deep Packet Inspection? Yeah, we've been dodging that since 2012.

Patches? Keeping up with all your vendors' vulnerabilities? I don't think you do... (Shhh... DarkMAP has you covered for that.)

Antivirus? Congrats on the 3-7% effectiveness—oh, and half the time it's already disabled.

SIEM? You've got it installed? Cool. Too bad your team's drowning in alerts. (Yeah... not with ThreatWAY—let's keep it our little secret.)

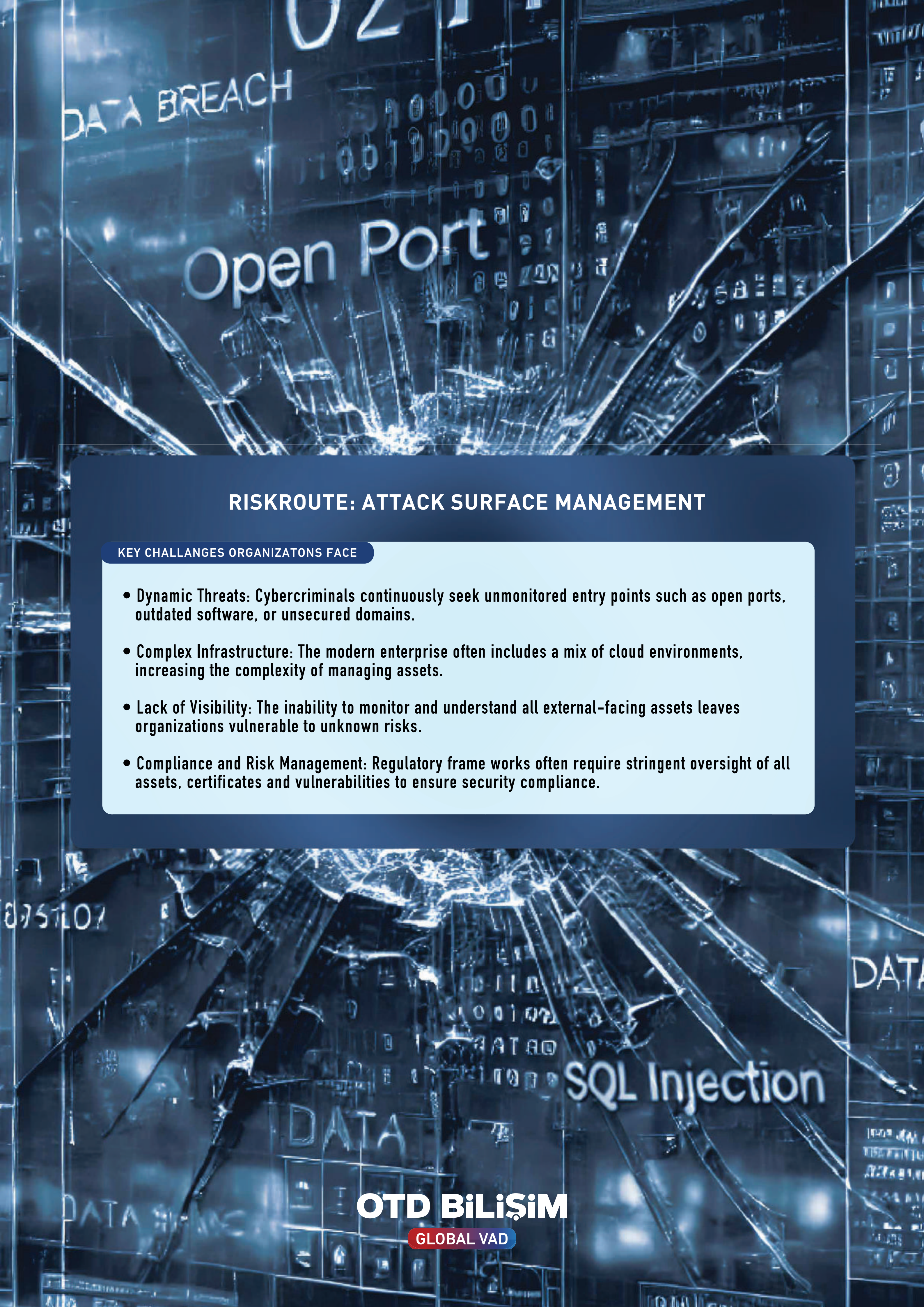
Policies and Procedures? Maybe, if you could all agree on them and not bicker over implementation.

The truth? You have to win 100% of the time. We just need to get lucky once.

This isn't about saying your security technologies are outdated. They're sophisticated, but they're only part of the solution. For the last 20 years, security's been focused on prevention—and you haven't won the cyber-war. Now, with SaaS, IoT, BYOD, Cloud, V2V, V2X, your perimeter is practically designed to be porous. You need smart, by-design solutions that adapt to this evolving environment.

Solutions that predict attacks by sniffing out threat patterns and intent—using tools like decoys, web intelligence, OSINT, and actionable insights to figure out the attackers before they even get close to figuring you out.

Prevention alone won't cut it anymore.



RISKROUTE: ATTACK SURFACE MANAGEMENT

KEY CHALLANGES ORGANIZATONS FACE

- Dynamic Threats: Cybercriminals continuously seek unmonitored entry points such as open ports, outdated software, or unsecured domains.

- Complex Infrastructure: The modern enterprise often includes a mix of cloud environments, increasing the complexity of managing assets.

- Lack of Visibility: The inability to monitor and understand all external-facing assets leaves organizations vulnerable to unknown risks.

- Compliance and Risk Management: Regulatory frame works often require stringent oversight of all assets, certificates and vulnerabilities to ensure security compliance.

OTD BiLiŞiM
GLOBAL VAD

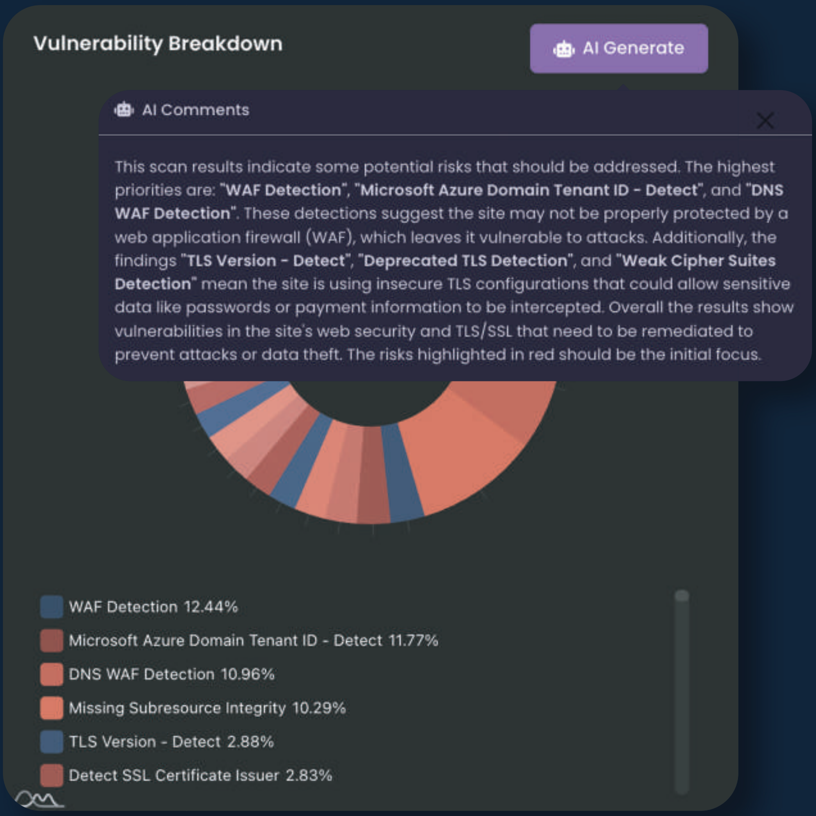
RiskROUTE: Proactive Security for Every Corner of Your Digital Landscape

CatchProbe RiskRoute offers a robust suite of tools designed to protect your organizations digital assets by providing continuous visibility and control over your entire digital environment. Its advanced capabilities empower security teams to monitor, manage and secure critical systems, identify vulnerabilities, track asset health and proactively defend against potential threats, reducing the risk of data breaches and cyber attacks.

Key Differentiators

AI-Powered Analysis and Remidiation Suggestions

RiskRoute goes beyond detection by leveraging AI to analyze each finding, providing detailed insihts into the nature of the issue and recommending tailored remediation steps.



This scan results indicate some potential risks that should be addressed. The highest priorities are: "**WAF Detection**", "**Microsoft Azure Domain Tenant ID - Detect**", and "**DNS WAF Detection**". These detections suggest the site may not be properly protected by a web application firewall (WAF), which leaves it vulnerable to attacks. Additionally, the findings "**TLS Version - Detect**", "**Deprecated TLS Detection**", and "**Weak Cipher Suites Detection**" mean the site is using insecure TLS configurations that could allow sensitive data like passwords or payment information to be intercepted. Overall the results show vulnerabilities in the site's web security and TLS/SSL that need to be remediated to prevent attacks or data theft. The risks highlighted in red should be the initial focus.

- 🟦 WAF Detection 12.44%
- 🟥 Microsoft Azure Domain Tenant ID - Detect 11.77%
- 🟥 DNS WAF Detection 10.96%
- 🟧 Missing Subresource Integrity 10.29%
- 🟦 TLS Version - Detect 2.88%
- 🟥 Detect SSL Certificate Issuer 2.83%

Real-Time Threat Detection & Management

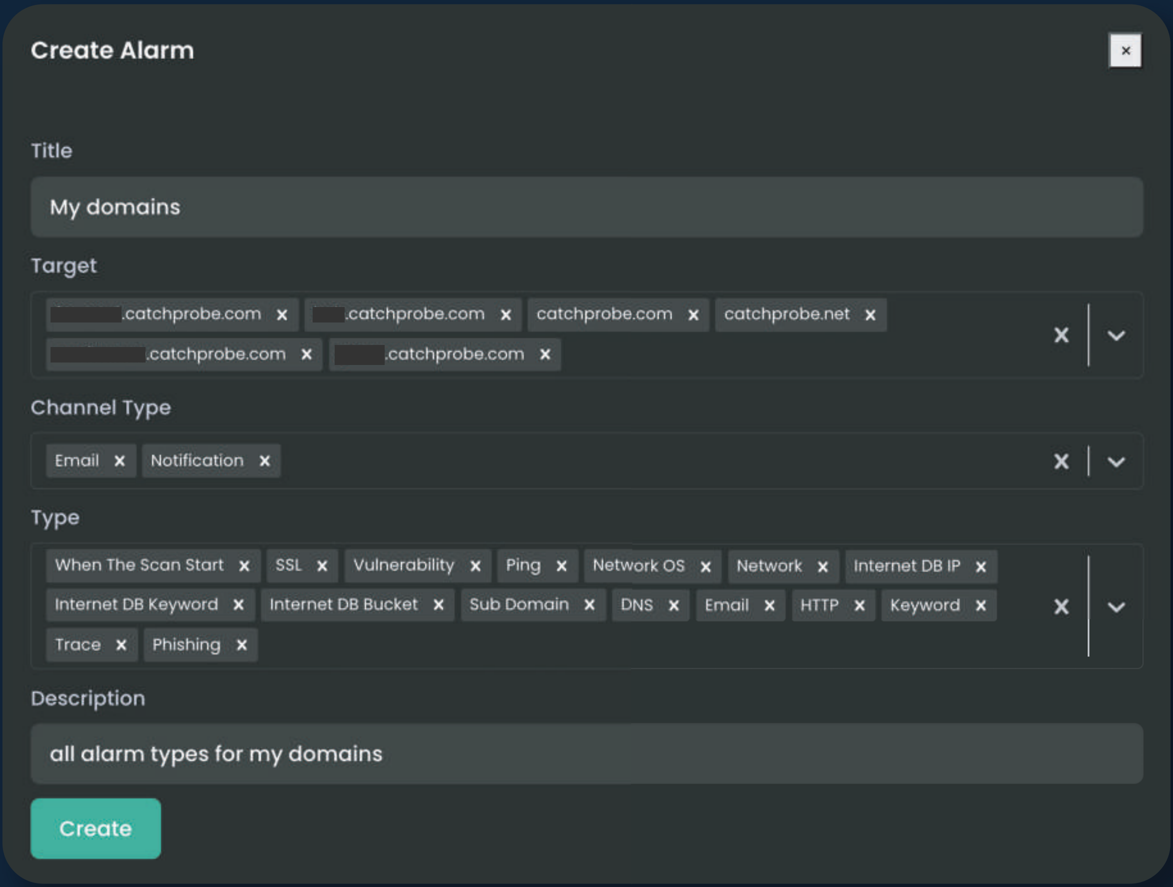
Continuously monitor for vulnerabilities, certicicate details, misconfigurations, phishing websites, HTTP details, DNS informatipn, subdomain discovery and details, port scanner results, operating system detals, network data, ping results, traceroute details and more, with real-time alerts.

Comprehensive Asset Visibility

Gain full visibility into your digital assets, from ports and domains to certicicates and historical data. RiskRoute ensures that no asset or potential vulnerability is overlooked.

Efficient Incident Response

When vulnerabilities are found, the faster you respond, the better. RiskRoute enables automatic alerts through integraions with Jira and Webhook and email, ensuring teams can quickly address threats and reduce response time.



Create Alarm

Title

My domains

Target

[redacted].catchprobe.com × [redacted].catchprobe.com × catchprobe.com × catchprobe.net × [redacted].catchprobe.com × [redacted].catchprobe.com ×

Channel Type

Email × Notification ×

Type

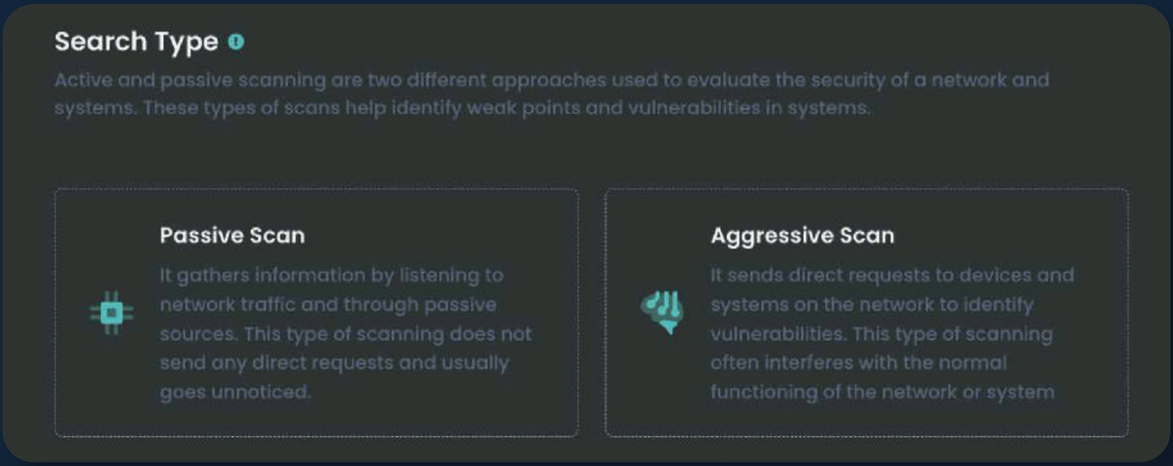
When The Scan Start × SSL × Vulnerability × Ping × Network OS × Network × Internet DB IP × Internet DB Keyword × Internet DB Bucket × Sub Domain × DNS × Email × HTTP × Keyword × Trace × Phishing ×

Description

all alarm types for my domains

Efficient Incident Response

Passive scan does not send direct requests to systems, allowing it to go unnoticed and minimizing the risk of interference with regular network operations whereas aggressive scan sends direct requests to devices and systems to identify vulnerabilities. While more intrusive, it provides in-depth analysis of potential weaknesses.



Search Type

Active and passive scanning are two different approaches used to evaluate the security of a network and systems. These types of scans help identify weak points and vulnerabilities in systems.

Passive Scan

It gathers information by listening to network traffic and through passive sources. This type of scanning does not send any direct requests and usually goes unnoticed.

Aggressive Scan

It sends direct requests to devices and systems on the network to identify vulnerabilities. This type of scanning often interferes with the normal functioning of the network or system

THREATWAY; MAXIMIZING THREAT INTELLIGENCE

TRADITIONAL CTI GATHERING

Multiple Data Sources: Collected from OSINT, proprietary feeds, closed forums, and government databases.

High Costs: Organizations often pay for multiple feeds, leading to redundant or unnecessary expenses.

Analysis: Time-consuming processes to filter out false positives and prioritize real threats.

INFRASTRUCTURE MANAGEMENT CHALLANGES

Firewall Overload: Large volumes of raw data can cause firewalls to hit capacity limits, increasing operational costs.

Infrastructure Strain: Processing unrefined loCs strains resources, causing slowdowns or requiring costly upgrades.

Generic Threat Lists: Many traditional solutions provide generic loCs, leading to irrelevant alerts and fatigue.

TRADITIONAL CTI SOLUTIONS LIMITATIONS

Data Overload: Floods systems with irrelevant or low-priority alerts, leading to inefficiency.

Fragmented Tools: Requires integration of disparate systems, complicating data normalization and sharing.

Slow Incident Response: Manual processing delays threat response, increasing the potential impact of attacks.

OTD BİLİŞİM
GLOBAL VAD

ThreatWAY
Threat Intelligence Exchange

ThreatWAY serves as an early warning system, enabling businesses to proactively identify and block malicious activity, while also facilitating real-time threat sharing.

Features:

- Offrers proactive insights by investigating attacks and facilitating automatic incident response capabilities.
- Gathers and disseminates data acquired from CatchProbe's decoys and exposed attacks, sourced from both API integration with open closed sources and crawling operations, in real-time.
- Distributes the obtained data and enables users to share them with their-inter-an intra-organizations within milliseconds.

MANAGE THREATS

ENABLE PROTECTION

DIGITAL FORENSICS

REAL-TIME INTELLIGENCE

Overview

Dynamic Channel and Collection Management

Targeted attack data incoming from thousands of honeypots

API integration with open and closed platforms

Collection of newly registered domain addresses

Automated Data Normalization

Real-Time Alerts: Receive real-time alerts on potential threats

Customizable Data Sources: Add an remove data sources as needed.

API Support: Easilşy integrate it with your existing Firewalls and SIEMs.

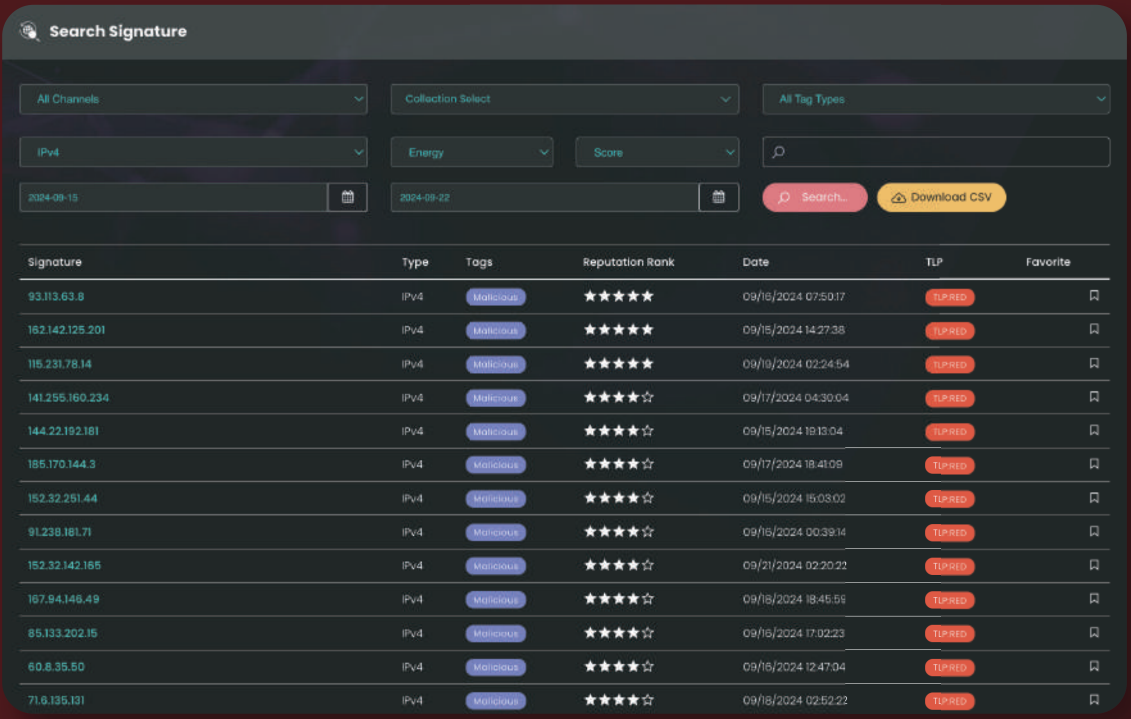
Threat Intelligence Reputation Ranking

ThreatWAY: Real-Time CTI Fites Seamslessly into Your Ecosystem

Key Differentiators

Critical Threats First: Focused Protection Where It Matters Most

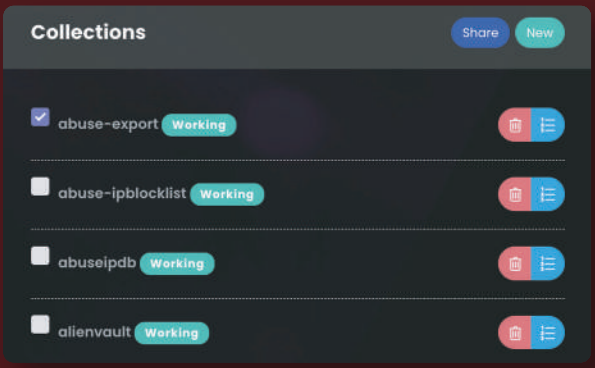
ThreatWAY analuzes and prioritizes threats, ensuring that your organization is focused on the most critical risks. By ranking IoCs based on their relevance and potential impact, ThreatWAY helps you identify which threats pose the greatest danger to your specific environment, reducing noise and minimizing distractions from low-risk or irrelevant data.



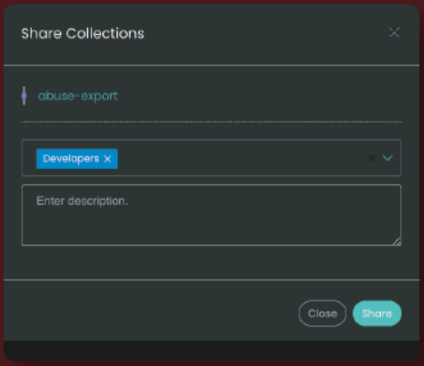
Signature	Type	Tags	Reputation Rank	Date	TLP	Favorite
93.113.63.8	IPv4	Malicious	★★★★★	09/16/2024 07:50:17	TLP:RED	🔖
162.142.125.201	IPv4	Malicious	★★★★★	09/15/2024 14:27:38	TLP:RED	🔖
115.231.78.14	IPv4	Malicious	★★★★★	09/19/2024 02:24:54	TLP:RED	🔖
141.255.160.234	IPv4	Malicious	★★★★☆	09/17/2024 04:30:04	TLP:RED	🔖
144.22.192.181	IPv4	Malicious	★★★★☆	09/15/2024 19:13:04	TLP:RED	🔖
185.170.144.3	IPv4	Malicious	★★★★☆	09/17/2024 18:41:09	TLP:RED	🔖
152.32.251.44	IPv4	Malicious	★★★★☆	09/15/2024 15:03:02	TLP:RED	🔖
91.238.181.71	IPv4	Malicious	★★★★☆	09/16/2024 00:39:14	TLP:RED	🔖
152.32.142.165	IPv4	Malicious	★★★★☆	09/21/2024 02:20:22	TLP:RED	🔖
167.94.146.49	IPv4	Malicious	★★★★☆	09/18/2024 18:45:59	TLP:RED	🔖
85.133.202.15	IPv4	Malicious	★★★★☆	09/16/2024 17:02:23	TLP:RED	🔖
60.8.35.50	IPv4	Malicious	★★★★☆	09/16/2024 12:47:04	TLP:RED	🔖
71.6.135.131	IPv4	Malicious	★★★★☆	09/18/2024 02:52:22	TLP:RED	🔖

Automated Data Collection and Sharing

ThreatWAY's infrastructure enables businesses to not only clooect but also share refined intelligence accross intra-and inter-organizational channels in milliseconds.



- ☑ abuse-export Working
- □ abuse-ipblocklist Working
- □ abuseipdb Working
- □ alienvault Working

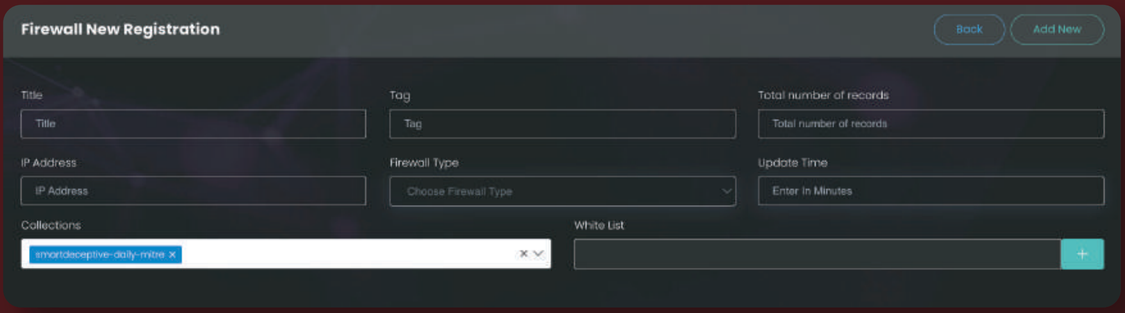


OTD BİLİŞİM
GLOBAL VAD

Effortless Integration, Real-Time Action

ThreatWAY empowers businesses by seamlessly delivering verified indicators of Compromise (loCs) directly to your firewalss, SIEMs and SOAR platforms. Whether through a REST API or direct integration using custom rules, ThreatWAY ensures that threat intelligence is rapidly actionable within your existing security infrastructure.

Option #1



Firewall New Registration

Title: Title

Tag: Tag

Total number of records: Total number of records

IP Address: IP Address

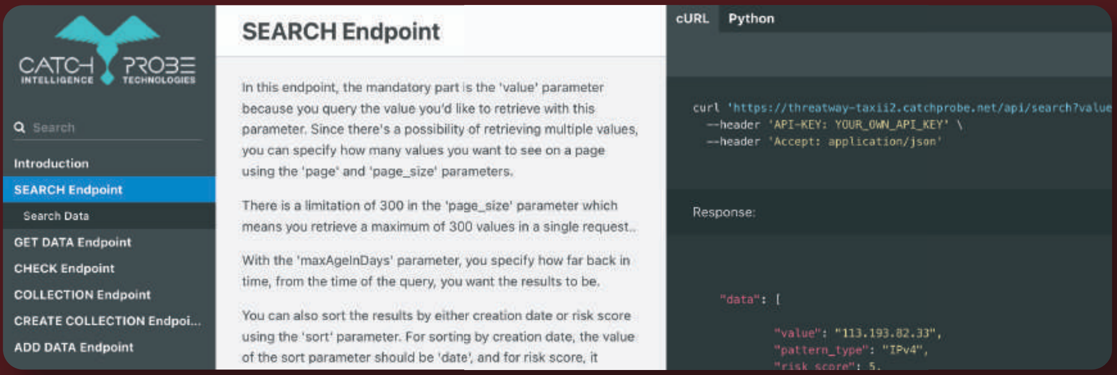
Firewall Type: Choose Firewall Type

Update Time: Enter In Minutes

Collections: smartdeceptive-daily-mitre ×

White List:

Option #2



SEARCH Endpoint

In this endpoint, the mandatory part is the 'value' parameter because you query the value you'd like to retrieve with this parameter. Since there's a possibility of retrieving multiple values, you can specify how many values you want to see on a page using the 'page' and 'page_size' parameters.

There is a limitation of 300 in the 'page_size' parameter which means you retrieve a maximum of 300 values in a single request..

With the 'maxAgeInDays' parameter, you specify how far back in time, from the time of the query, you want the results to be.

You can also sort the results by either creation date or risk score using the 'sort' parameter. For sorting by creation date, the value of the sort parameter should be 'date', and for risk score, it

```
curl 'https://threatway-taxii2.catchprobe.net/api/search?value
  --header 'API-KEY: YOUR_OWN_API_KEY' \
  --header 'Accept: application/json'
```

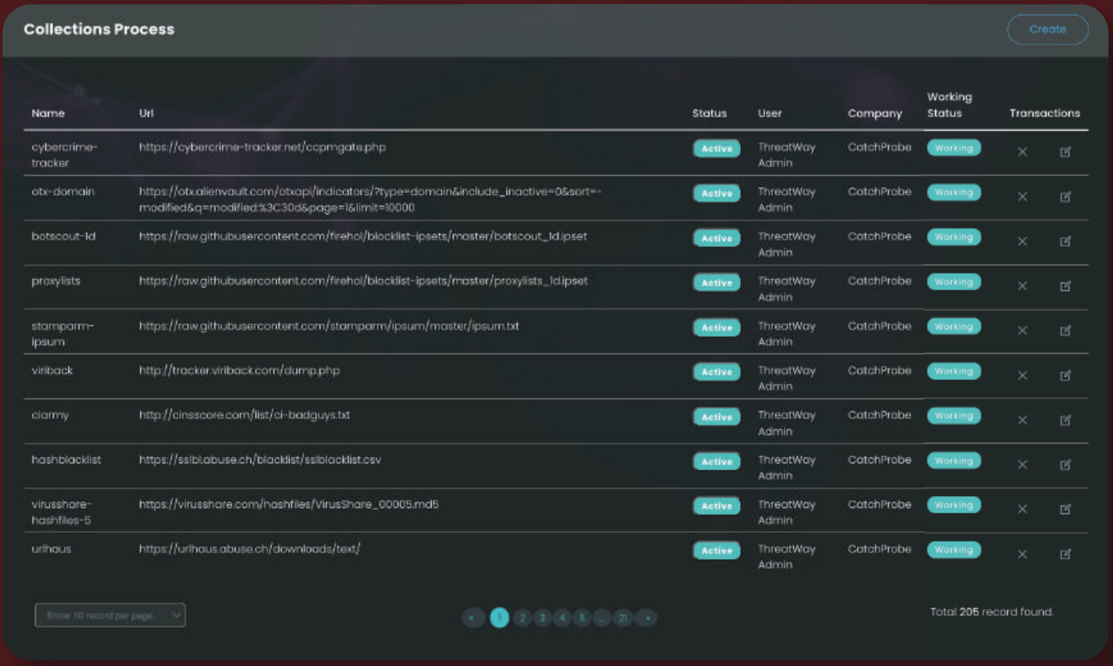
Response:

```
    "data": [

            "value": "113.193.82.33",
            "pattern_type": "IPv4",
            "risk_score": 5,
```

Customizable Data Sources

ThreatWAY offer seamless integration of over 200 platforms throygh API, alongside DarkMAP's advanced crawling operations and SmartDECEPTIVE's decoys and exposed attacks, while also allowing you to easily add or remove customized data sources to ensure only most relevant intelligence is available for your specific needs in real-time.



Collections Process

Name	Url	Status	User	Company	Working Status	Transactions
cybercrime-tracker	https://cybercrime-tracker.net/ccpmgate.php	Active	ThreatWay Admin	CatchProbe	Working	× ✎
otx-domain	https://otx.alienvault.com/otxapi/indicators/?type=domain&include_inactive=0&sort=-modified&q=modified:%3C30d&page=1&limit=10000	Active	ThreatWay Admin	CatchProbe	Working	× ✎
botscout-1d	https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/botscout_1d.ipset	Active	ThreatWay Admin	CatchProbe	Working	× ✎
proxylists	https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/proxylists_1d.ipset	Active	ThreatWay Admin	CatchProbe	Working	× ✎
stamparm-ipsum	https://raw.githubusercontent.com/stamparm/ipsum/master/ipsum.txt	Active	ThreatWay Admin	CatchProbe	Working	× ✎
viriback	http://tracker.viriback.com/dump.php	Active	ThreatWay Admin	CatchProbe	Working	× ✎
ciarmy	http://cinsscore.com/list/ci-badguys.txt	Active	ThreatWay Admin	CatchProbe	Working	× ✎
hashblacklist	https://sslbl.abuse.ch/blacklist/sslblacklist.csv	Active	ThreatWay Admin	CatchProbe	Working	× ✎
virusshare-hashfiles-5	https://virusshare.com/hashfiles/VirusShare_00005.md5	Active	ThreatWay Admin	CatchProbe	Working	× ✎
urlhaus	https://urlhaus.abuse.ch/downloads/text/	Active	ThreatWay Admin	CatchProbe	Working	× ✎

Total 205 record found.

CATCHPROBE'S INTEGRATION-ENABLED FEATURES

THREAT ACTOR

Through the development of seamlessly integrated modules, we have built a unique and unified ecosystem. This enables us to provide a comprehensive suite of interconnected modules, each with its own specialized purpose that complements and enhances the capabilities of the others.

1 Deceive attackers with SmartDECEPTIVE

By producing authentic responses that effectively deceive attackers, SMARTDECEPTIVE protects your systems while providing insights into attackers and ensures the secure monitoring of their actions.

SMARTDECEPTIVE

DECEPTION MANAGEMENT & ANALYSIS

2 Analyze & Profile with LeakMAP

SMARTDECEPTIVE integrates with LeakMAP to detect structured attacks. This refers to instances where an attacker attempts to gain access to a system using leaked credentials. Because in most cases, these attacks are not specifically directed at a particular individual port scanning. So although the structured attacks may occur less frequently, they are potentially more dangerous.

LEAKMAP

F Block attackers with ThreatWAY

ThreatWAY ensures that every organization receives a customized and refined coolection of loCs (Indicators of Compromise) that present real threats to their specific environment. Additionally, ThreatWAY seamlessly integrates with Firewalls and SIEMs to enable automated incident response.

THREATWAY

THREAT INTELLIGENCE EXCHANGE PLATFORM

1 DarkMAP sends loCs to ThreatWAY

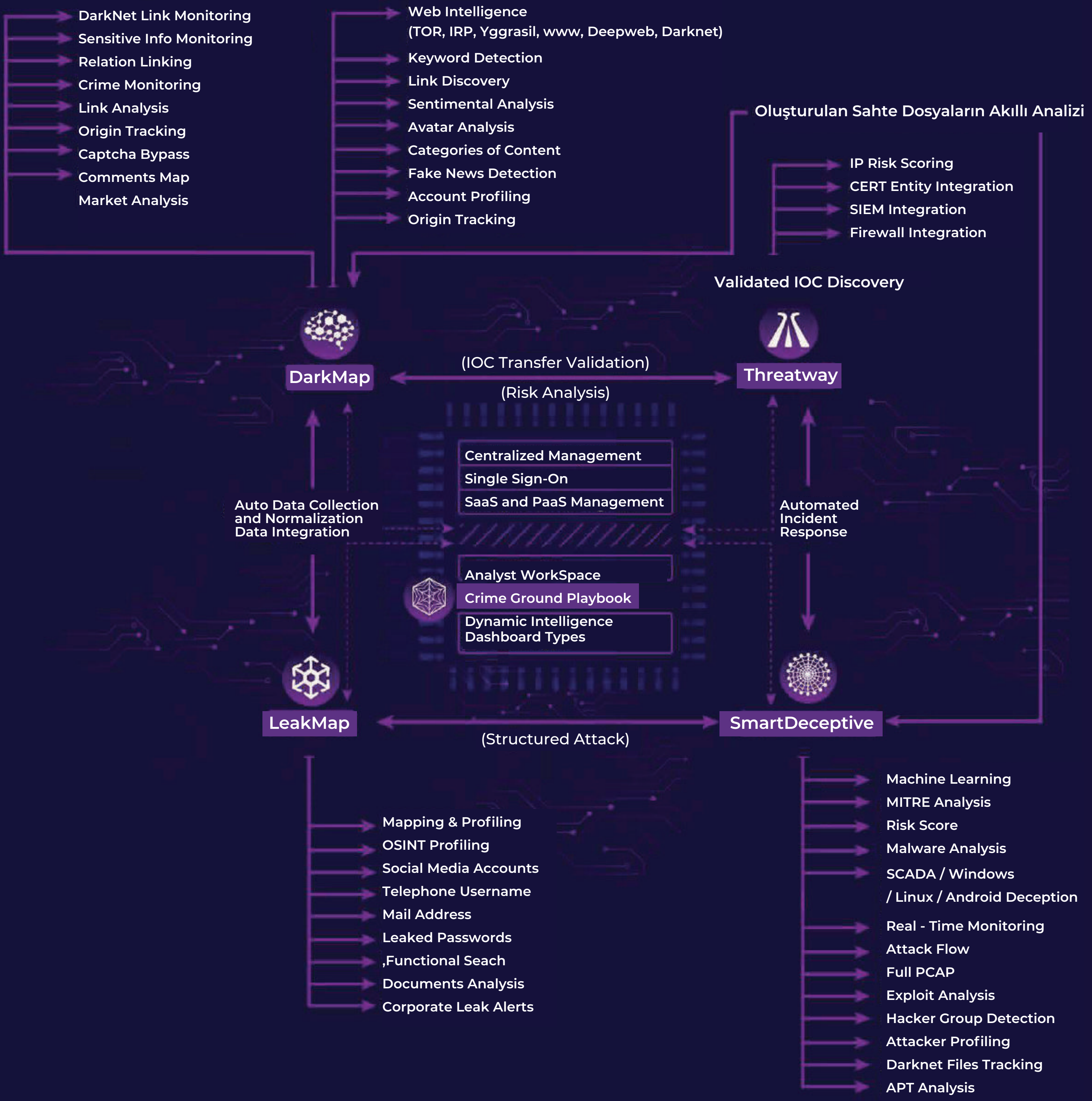
Alongside capturing data from SmartDECEPTIVE' exposed attacks and from API integrations with open and closed sources, ThreatWAY leverages real-time loC's (Indicators of Compromise) information obtained through DarkMAP's crawling operations.

DARKMAP

WEB INTELLIGENCE

CATCHPROBE ACTIONABLE INTELLIGENCE ORCHESTRATION ARCHITECTURE

Centralized All-in-One Cyber and Digital Intelligence Suite



- DarkNet Link Monitoring
- Sensitive Info Monitoring
- Relation Linking
- Crime Monitoring
- Link Analysis
- Origin Tracking
- Captcha Bypass
- Comments Map
- Market Analysis

- Web Intelligence (TOR, IRP, Yggrasil, www, Deepweb, Darknet)
- Keyword Detection
- Link Discovery
- Sentimental Analysis
- Avatar Analysis
- Categories of Content
- Fake News Detection
- Account Profiling
- Origin Tracking

Oluşturulan Sahte Dosyaların Akıllı Analizi

- IP Risk Scoring
- CERT Entity Integration
- SIEM Integration
- Firewall Integration

Validated IOC Discovery

DarkMap

(IOC Transfer Validation)

(Risk Analysis)

Threatway

Auto Data Collection
and Normalization
Data Integration

Centralized Management

Single Sign-On

SaaS and PaaS Management

Automated
Incident
Response

Analyst WorkSpace

Crime Ground Playbook

Dynamic Intelligence Dashboard Types

LeakMap

(Structured Attack)

SmartDeceptive

- Mapping & Profiling
- OSINT Profiling
- Social Media Accounts
- Telephone Username
- Mail Address
- Leaked Passwords
- ,Functional Seach
- Documents Analysis
- Corporate Leak Alerts

- Machine Learning
- MITRE Analysis
- Risk Score
- Malware Analysis
- SCADA / Windows / Linux / Android Deception
- Real - Time Monitoring
- Attack Flow
- Full PCAP
- Exploit Analysis
- Hacker Group Detection
- Attacker Profiling
- Darknet Files Tracking
- APT Analysis

CATCH PROBE™

OTD BİLİŞİM
GLOBAL VAD

CATCH PROBE™

CATCH PROBE™
INTELLIGENCE TECHNOLOGIES
OTD BİLİŞİM
GLOBAL VAD