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.
- loT Systems:
  Protect loT 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

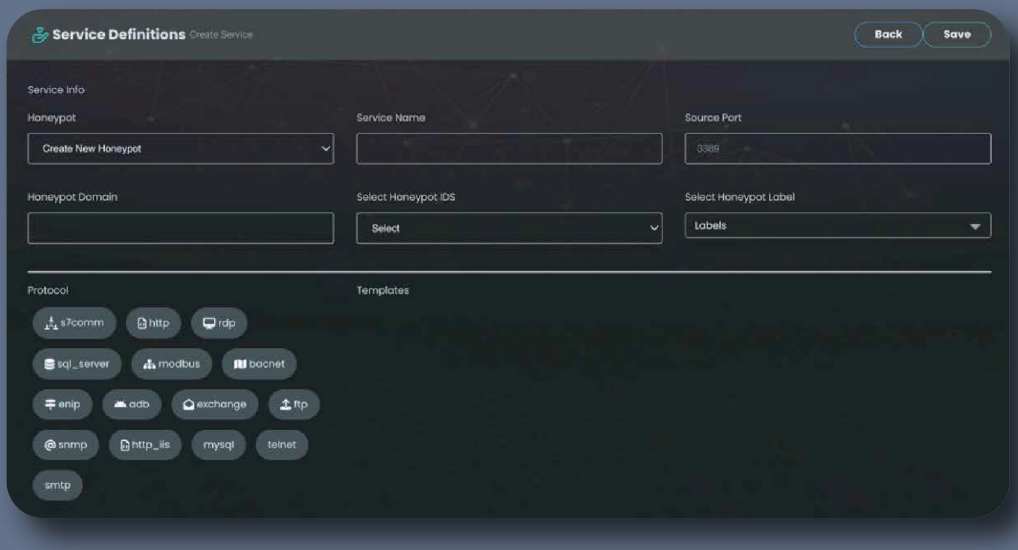
SMARTDECEPTIVE: Deception Technology for Real-Time Threat Intelligence

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.



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

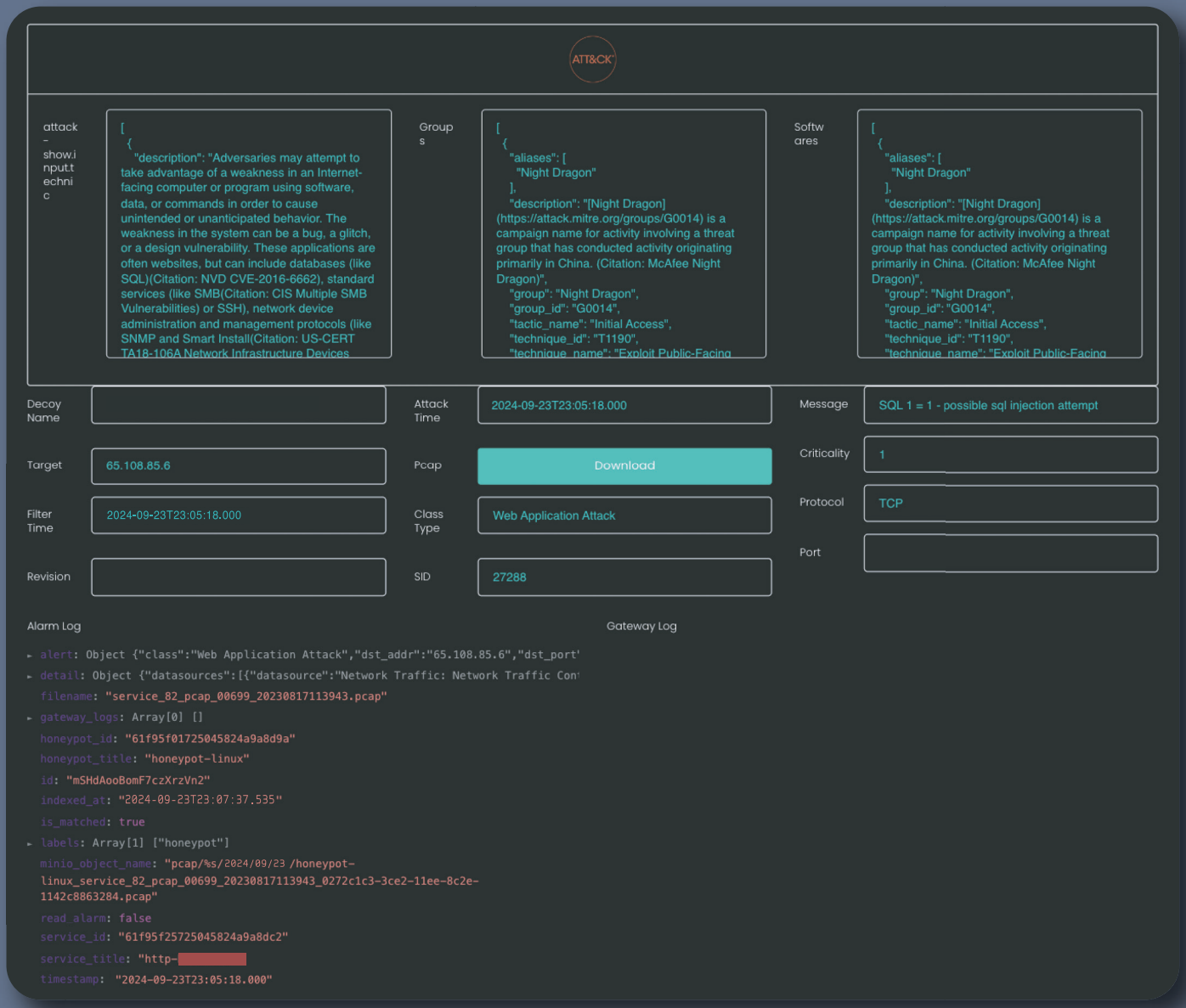
OTD BİLİŞİM GLOBAL VAD

Cost Efficiency

There are no additional licensing or hardware costs; decoys do not require extra purchases such as databases or application licenses to simulate these environments.

In-Depth Analysis

With full packet capture (PCAP) capability and Mitre ATT&CK integration, SmartDECEPTIVE provides a detailed analysis that enables a comprehensive understanding of the attacker's behavior.

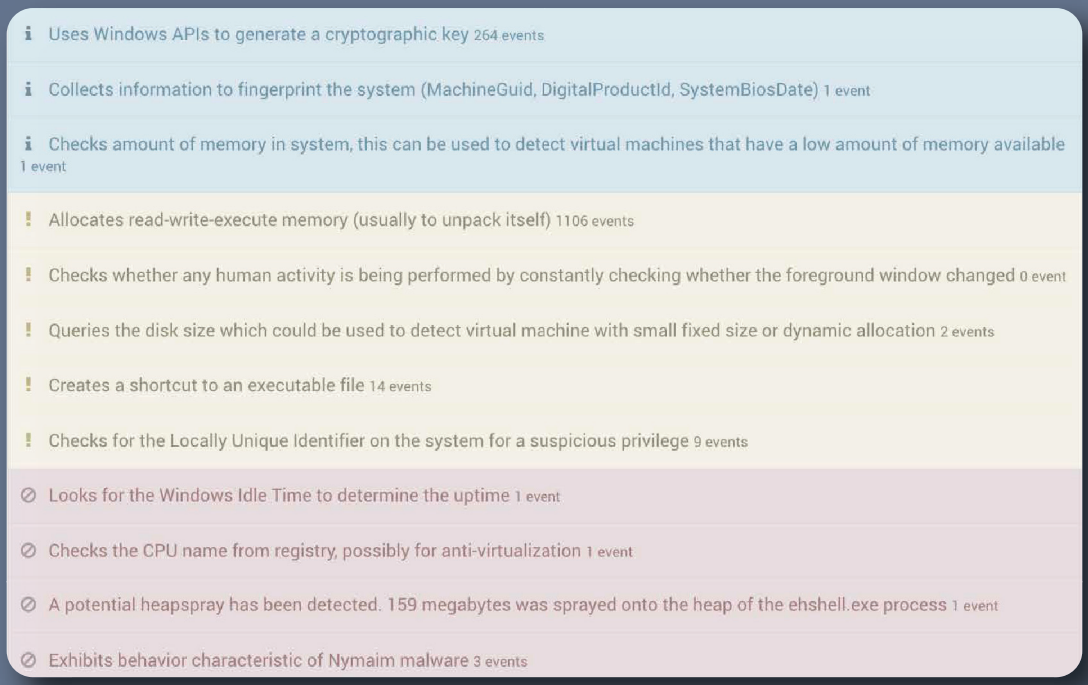


AI-Powered Reports and Recommendations

SmartDECEPTIVE delivers AI-driven reports and actionable recommendations that analyze all detected attacks, strengthen defenses, and provide actionable insights aimed at reducing future risks.

Malware Analysis

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



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

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.

SmartDECEPTIVE

CATCHPROBE™

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.