DATA SHEET

ClearSkies™ Active Defense

“Post-Breach Detection”

ClearSkies™

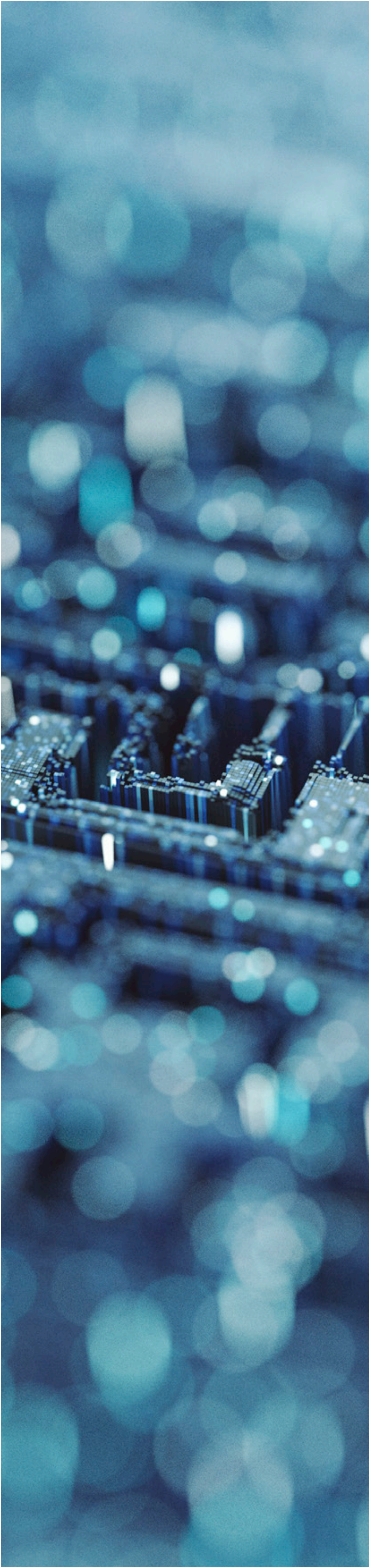

Table of Contents

Introduction

It is no longer a question of whether your network will be breached... It is a question of when.

You are then inclined to ask:

- **How quickly can I find them before they start inflicting real damage?**
- **What are their intensions?**
- **How quickly can we contain the impact of a data breach?**

> **"Prevent threat-actors who have managed to infiltrate your network from moving unimpeded for months, stealing data and intellectual property."**

The information-threat landscape is expanding. The newest generation of remotely controlled network attacks is challenging the effectiveness of traditional detection and **prevention tools, making prevention-based approaches less effective**.

Thus, it is just a matter of time before determined threat-actors penetrate your corporate network and systems. And while prevention-based security approaches remain relevant, they are no longer enough.

This paradigm shift dictates that organizations change their information risk management strategies from **prevention-based** to **post-breach detection** security approaches, if they are to maintain and safeguard their Information Security posture.

What is Deception technology?

Deception technology is an emerging **post-breach detection** classification. Its goal is to help organizations defend themselves by gathering intelligence against malware and threat-actors that have penetrated their network and strategically and progressively make their way in, **(Counter-Intelligence)**, searching for sensitive-confidential information and high-value assets, which are ultimately the target of their attack campaigns.

Deception technology can be used to mimic a broad range of legitimate technology assets, including legacy environments, industry-specific environments, like OT, and even IoT devices.

Why Deception technology is important

Once threat-actors manage to infiltrate the corporate network, they initiate reconnaissance to understand the network topology in order to laterally map other parts of the network and identify key value digital assets.

The aim of Deception technology is to deceive/delay threat-actors in order organizations have time to defend themselves, by distributing across the corporate network a collection of **Decoys and Beacon Traps** that imitate genuine key-value digital assets, as well as misinformation as baits.

> **"By occupying threat-actors for as long as possible with Decoys and Traps, organizations can delay them from achieving their real purpose, thus gaining valuable time to take necessary defensive actions."**

Thus, by delaying threat-actors in reaching **"real digital assets"**, organizations can, through this **deceive-delay** tactic, take defensive actions earlier in the attack chain to effectively minimize **"Dwell Time"**[1].

[1] **Dwell Time** is the length of **time** a **threat-actors** is inside the corporate network undetected. Dwell Time is determined by adding Mean **Time** to Detect (MTTD) and **Mean Time to Repair/Remediate (MTTR)** and is usually measured in days.

Detection by Deception

Threat-actors have different motives when focusing on gaining access to different key-value digital assets. Deploying a diverse range of Decoys and Traps, strategically positioned within the corporate network and systems, provides you with deep visibility into malicious activity, which can drastically minimize the time between breach and discovery (dwell time).

“M-TRENDS 2020 Reports states that, in **2019, 40%** of the data compromises investigated by Mandiant experts were characterized by dwell times of **30 days or fewer**, compared to **31% of the previous year**, while **12% of investigations** were characterized by dwell times greater than **700 days**, which is consistent with the previous year.”

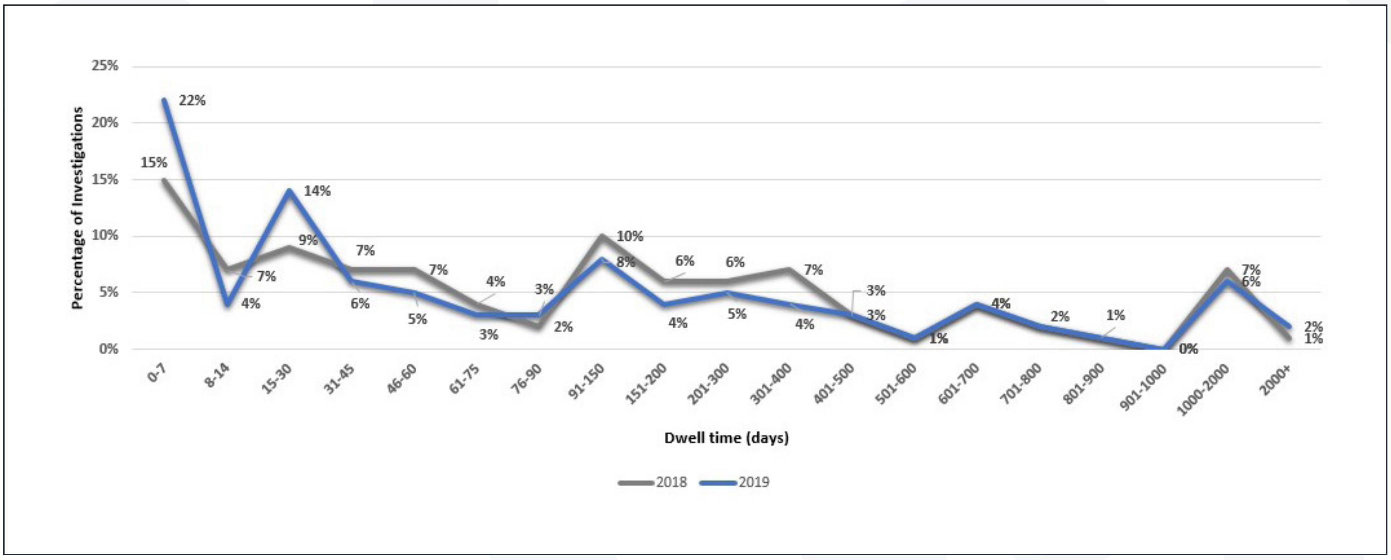

Figure 1: Global Dwell Time Distribution

How it works

ClearSkies™ Active Defense both compliments and capitalizes on the early detection and response capabilities of **ClearSkies™ Cloud SIEM**.

Deception **ClearSkies™ Active Defense** 'Decoys and Beacon Traps' are deployed across the corporate network and systems infrastructure as shown in **Figure 2**, in order to lure, trap and engage the attacker.

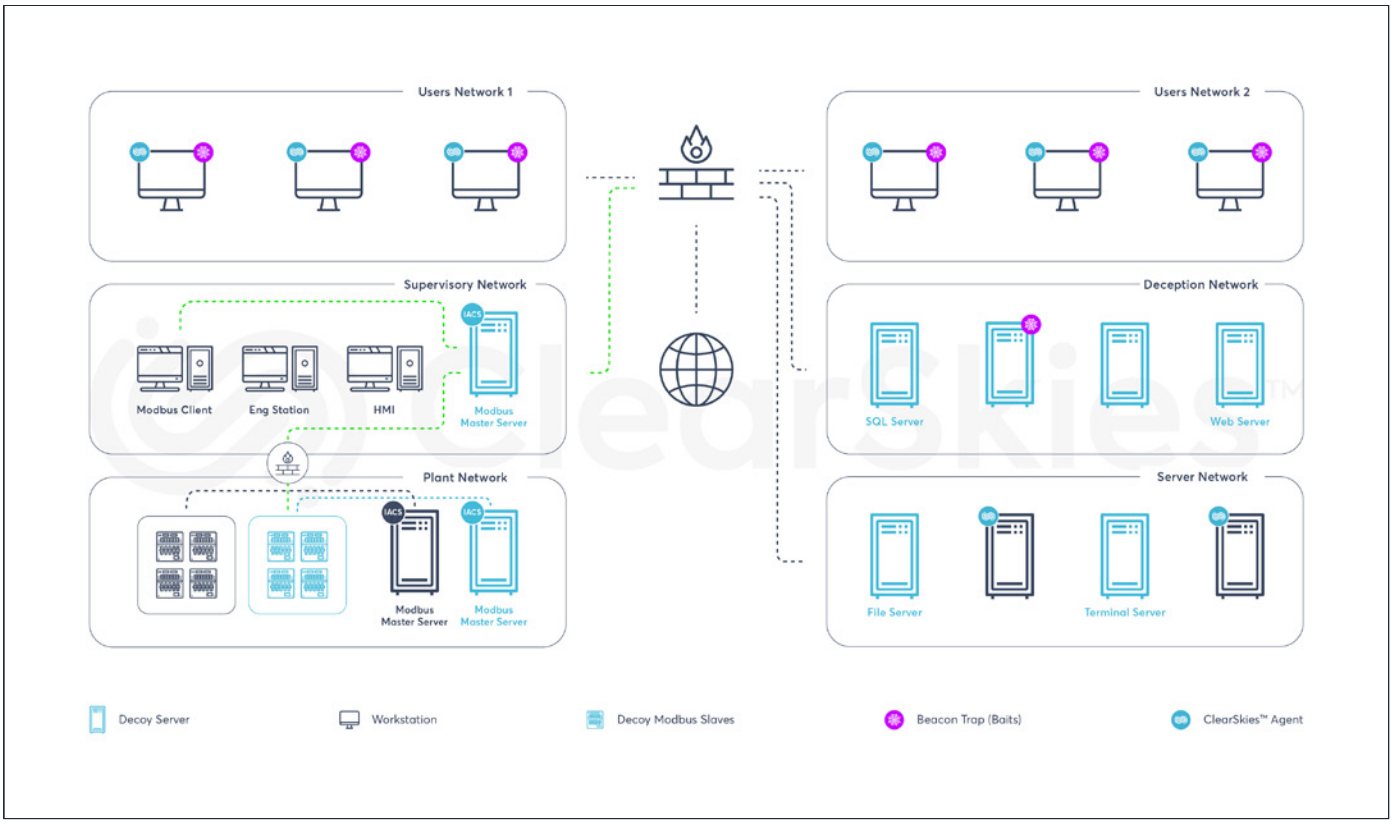

Figure 2: Sample deployment of ClearSkies™ Active Defense 'Decoys and Beacon Traps'

ClearSkies™ Active Defense 'Decoys and Beacon Traps' are designed not only to detect reconnaissance and malware related activity, but also to access and/or use planned fake information, which may include user access credentials, database connections and network shares, in order to deceive threat-actors into thinking they have discovered a way to escalate their privileges, perform lateral movement, and/or access sensitive information/data towards achieving their goals.

If any probing is attempted, or any fake information is accessed and/or used, an alert notification is triggered and sent, along with attack-vector information, to **ClearSkies™ Cloud SIEM** for further analysis before an incident is escalated, as shown in **Figure 3**.

“Organization’s visibility into suspicious activity within internal networks and systems is critical.”

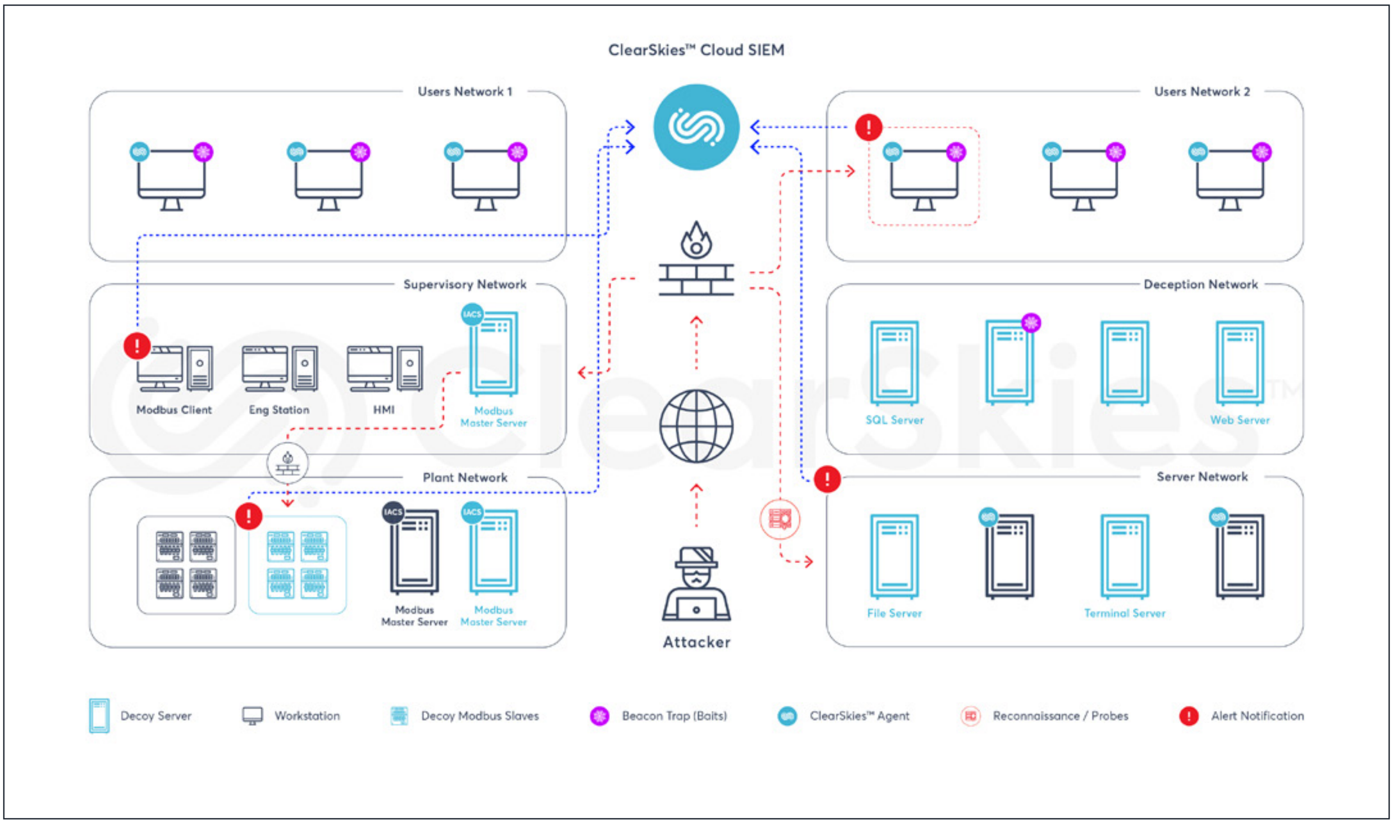

Figure 3: ClearSkies™ Alert notification and Incident escalation

Attack-Vector information provides the organization with valuable intelligence as to how threat-actors interact with assets, including their methods, purpose and source.

“The difference between ‘Decoys and Beacon Traps’ and the real assets is that legitimate users of the network have no reason to access them, so any access is an indication of suspicious and/or malicious activity.”

Incident escalation can be automated, so security personnel can be informed even as the attack is taking place. Incidents can be sent via email, SMS and/or push notification on smartphones and tablets with ClearSkies™ Mobile App (for iOS and Android) installed. For more detailed information related to incident escalation, refer to the ClearSkies™ Secure Web Portal (SWP) **“Event Management”** ServiceModule.

ClearSkies™ Active Defense ‘Decoys and Beacon Traps’ are fully deployed, managed and monitored through the ClearSkies™ Secure Web Portal (SWP).

ClearSkies™ Active Defense can be deployed and managed by organizations with their own Security Operations Center (SOC) or by **Odyssey's 24/7 Managed Security/Detection & Response (MDR) Services.**

Building blocks

Decoys

ClearSkies™ Active Defense high/medium-interaction 'Decoys' are designed to look and behave exactly like a real information asset, impersonating real OS, business applications, and possessing open ports using the same protocols (TCP, UDP, SMB, HTTP, ICMP, RDP, FTP, TFTP, MYSQL, MSSQL, TELNET, MODBUS, SSH and SNMP). This makes it virtually impossible for threat-actors to distinguish between a real or a fake asset, thus increasing the probability of engagement, luring them to the wrong path, and inadvertently revealing their presence and intentions, as shown in **Figure 4**.

Beacon Traps

ClearSkies™ Active Defense 'Beacon Traps' use fake information and **"poisoned data"**[2] as bait to lure threat-actors. This information consists of different file formats and is placed strategically amongst real information to aid in the early detection of suspicious activities related to unauthorized use and/or access.

Fake information may have the form of email accounts, user credentials, financial spreadsheets and document files related to intellectual property or any other valuable information.

Any attempt to **copy, access, modify** or use this information by threat actors automatically triggers an Alert/Incident, as shown in **Figure 4**, while a similar action involving **"real"** information/data would have gone unnoticed, allowing the attacker to continue their silent perpetration through the organizational infrastructure.

[2] Poisoned Data: Fake information such as user credentials that, if used by threat-actors towards escalating their access, will reveal lateral-movement attempts.

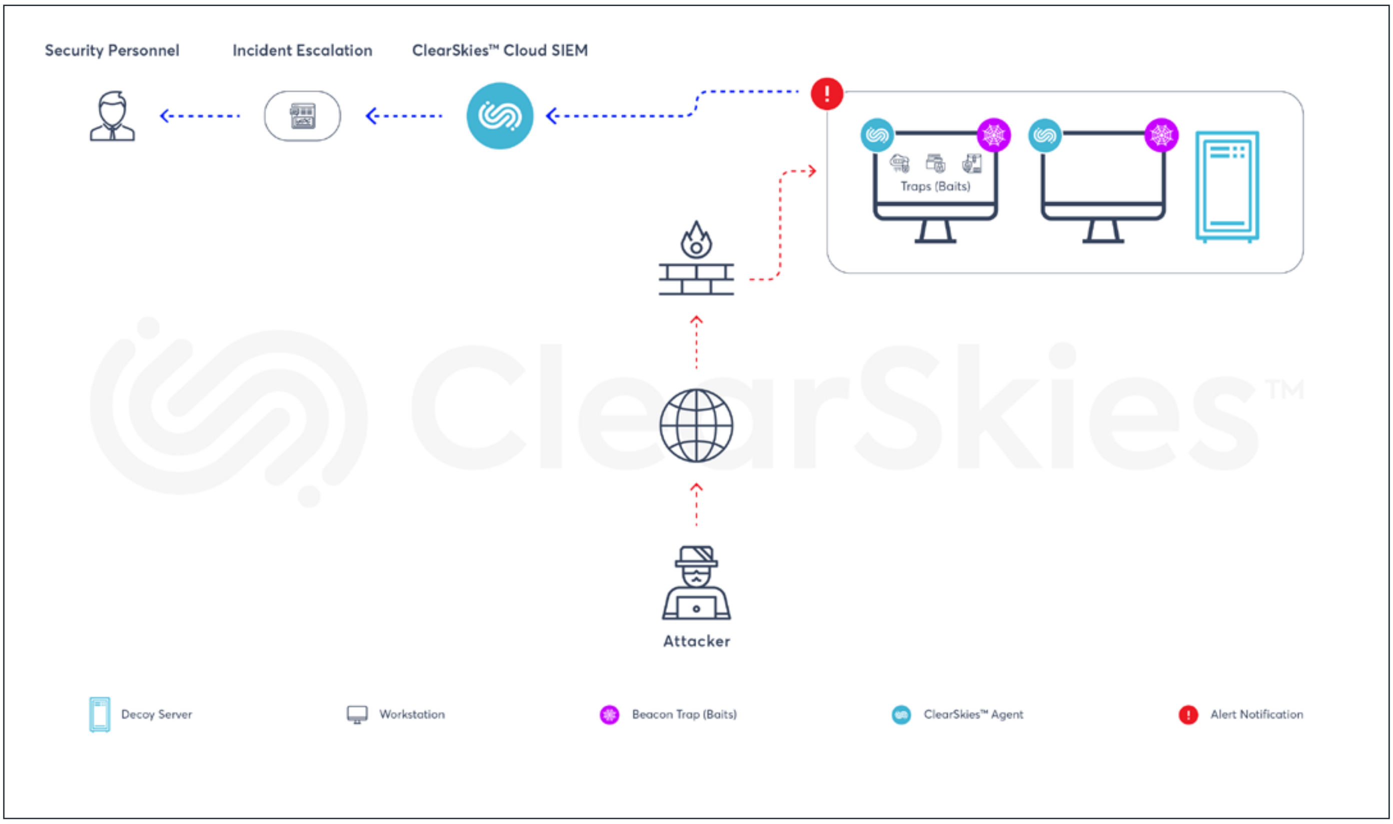

Figure 4: ClearSkies™ Active Defense Decoys and Beacon Traps at work

Industrial Automation and Control Systems (IACS)

The malware attack on Stuxnet and the Iranian uranium enrichment facility was designed specifically for IACS and was an eye-opener for the Information Security community.

Nowadays, Operational Technology (OT) systems, including IASC/SCADA, are intergraded with enterprise management systems, which are connected to the corporate network for crucially important management purposes. However, these Supervisory Control and Data Acquisition (SCADA) and IACS devices such as PLCs, DCS controllers, IEDs, and RTUs, are **DESIGNED** with a focus on reliability and real-time I/O, not **Secure**.

Since then, a number of new-breed malware targeting IACS, including SCADA, such us **'Black Energy, FrostyURL, Havex, Triton, Crash Override/Industroyer'**, have all continued to pose high risk to manufacturing, process, and pipeline control operators throughout the world.

The evolving information-threat landscape demonstrated that prevention-based security and audit control, including air-gapped technologies proved to be a false hope.

Successful cyberattacks on IASC/SCADA that manage critical national infrastructures, such as electrical and water supply, can last for a long time and can result in devastating social and economic outcomes.

Thus, the implementation of ClearSkies™ Active Defense Modbus ‘Decoys’ is a critical element for any organization working toward building **“Defense-In-Depth”** layered security for real-time visibility into threats targeting your enterprise network, systems and OT environments.

Modbus

Modbus is a client-server[3] data communication protocol originally developed by Modicon (now Schneider Electric) which is widely being used by IACS/SCADA’, which allows communication with Programmable Logic Controllers (PLC). The Modbus-Master controls the communication with all Modbus-Slaves. Modbus-Slaves respond to the Modbus-Master’s requests to read from or write data to.

The ClearSkies™ Active Defense TCP-Modbus high-interaction ‘Decoy’ emulates Modbus ‘Master/Slave’ communication in real time for command and control purposes, as shown in **Figure 5**.

Any attempt to communicate with the Master-Modbus will trigger an alert and send to the ClearSkies™ Cloud SIEM.

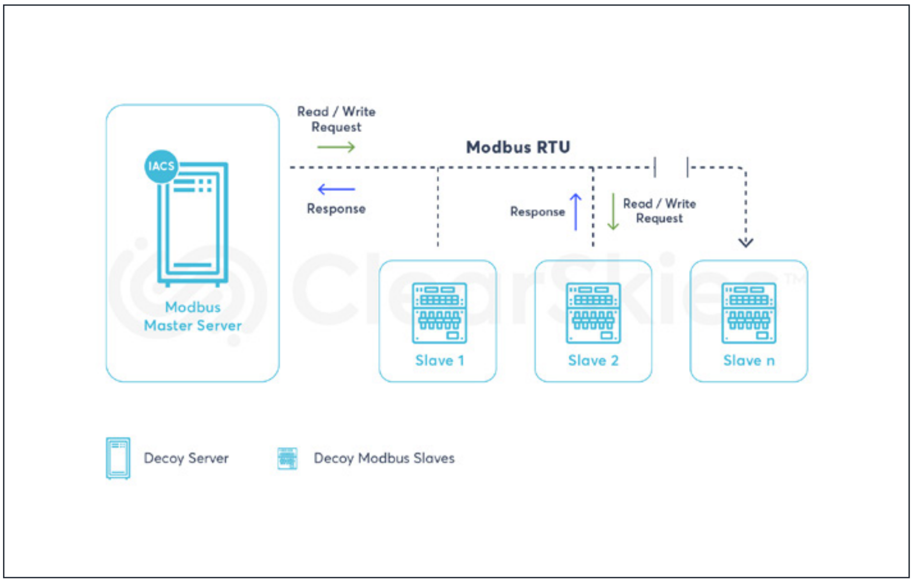

Figure 5: ClearSkies™ Active Defense Decoys and Beacon Traps at work

ClearSkies™ Active Defense Modbus-Master Decoy accepts the following configuration attributes:

- “Number of Slaves”,
- “Vendor Name”,
- “Product Code”,
- “Vendor URL”,
- “ProductName & Version”,
- “Model Name”,
- “Major Minor Revision”.

[3] The device requesting the information is called the Modbus-Master and the devices supplying information are Modbus-Slaves.

Deployment

ClearSkies™ Active Defense ‘Decoys and Beacon Traps’ are strategically deployed on different network segments where key-value assets reside, thus creating a **“Deception Defense Layer”**, which complements your organization’s “**Defense-In-Depth”**[4] multilayered approach, as shown in **Figure 6**. The whole approach contributes to the early detection of malware and threat actors as they strategically and progressively make their way in to move throughout corporate networks and systems unnoticed.

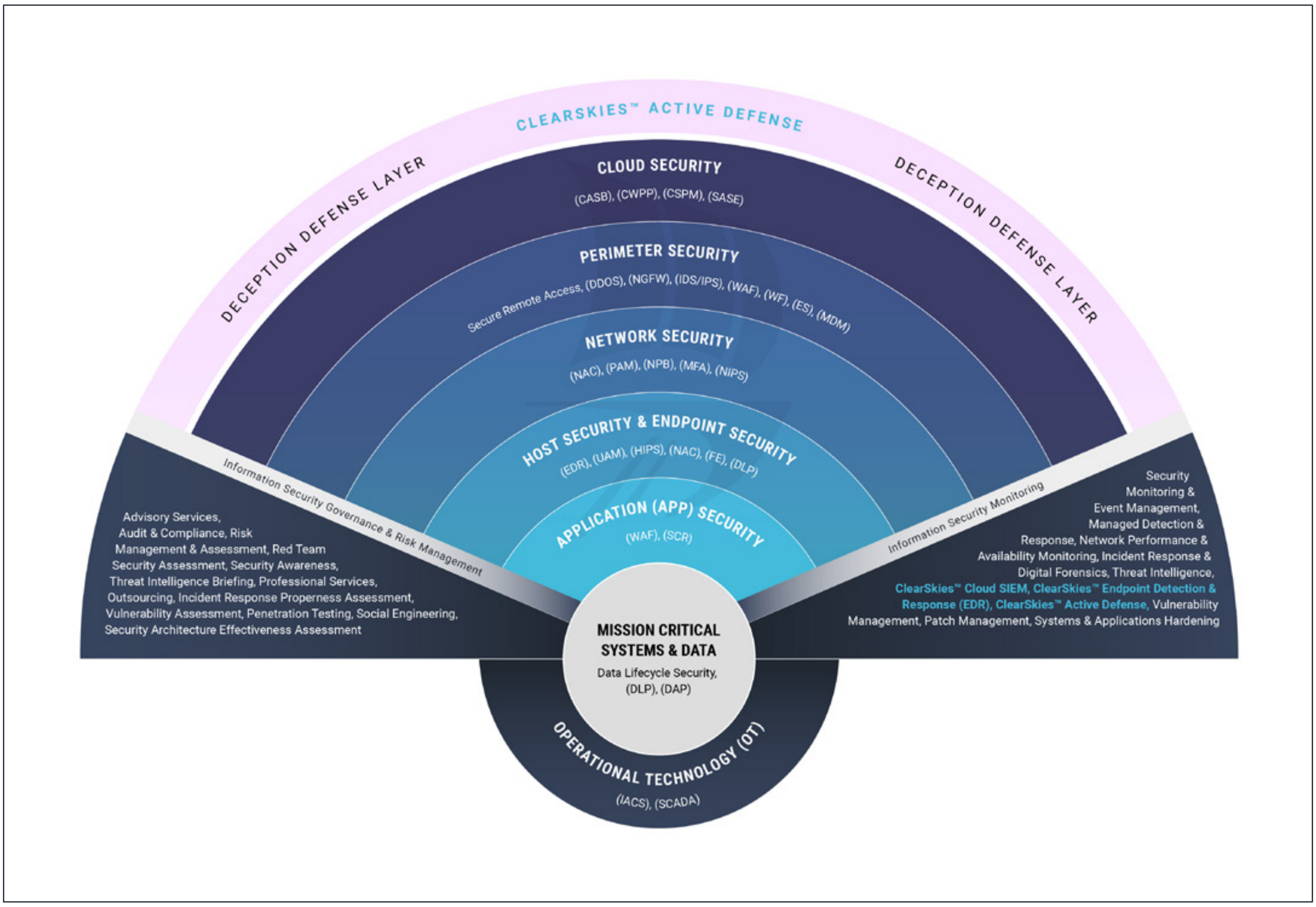
CLEARSKIES™ ACTIVE DEFENSE
DECEPTION DEFENSE LAYER
DECEPTION DEFENSE LAYER
CLOUD SECURITY
(CASB), (CWPP), (CSPM), (SASE)
PERIMETER SECURITY
Secure Remote Access, (DDOS), (NGFW), (IDS/IPS), (WAF), (WF), (ES), (MDM)
NETWORK SECURITY
(NAC), (PAM), (NPB), (MFA), (NIPS)
HOST SECURITY & ENDPOINT SECURITY
(EDR), (UAM), (HIPS), (NAC), (FE), (DLP)
APPLICATION (APP) SECURITY
(WAF), (SCR)
MISSION CRITICAL SYSTEMS & DATA
Data Lifecycle Security, (DLP), (DAP)
OPERATIONAL TECHNOLOGY (OT)
(IACS), (SCADA)
Information Security Governance & Risk Management
Advisory Services, Audit & Compliance, Risk Management & Assessment, Red Team Security Assessment, Security Awareness, Threat Intelligence Briefing, Professional Services, Outsourcing, Incident Response Properness Assessment, Vulnerability Assessment, Penetration Testing, Social Engineering, Security Architecture Effectiveness Assessment
Information Security Monitoring
Security Monitoring & Event Management, Managed Detection & Response, Network Performance & Availability Monitoring, Incident Response & Digital Forensics, Threat Intelligence, ClearSkies™ Cloud SIEM, ClearSkies™ Endpoint Detection & Response (EDR), ClearSkies™ Active Defense, Vulnerability Management, Patch Management, Systems & Applications Hardening

Figure 6: Defense-In-Depth layered security

[4] “Defense-In-Depth” follows the military principle that it is much more difficult for an enemy to defeat a multi-layered defense system than to penetrate a single barrier.

This strategic deployment ensures that threat actors attracted to different types of information/data, or use a variety of techniques and attack tactics, can be caught on this **“Deception Defense Layer”**.

The effectiveness of the **“Deception Defense Layer”** depends on the following key characteristics:

- Diversity and location of ‘Decoys and Beacon Traps’ deployed
- Fabrication and planting of convincing fake **“Poisoned Data”**

Deception Defense Layer (The Art of Deception)

The aim of the **“Deception Defense Layer”**, as shown in **Figure 7**, is to assist organizations for the early detection of and response to targeted attacks and data breaches by creating confusion and by luring the attackers to the wrong path, and as a result, reveal their presence and intentions before is too late.

Any interaction with any **‘Decoys and Traps’** indicates a suspicious/malicious activity in progress.

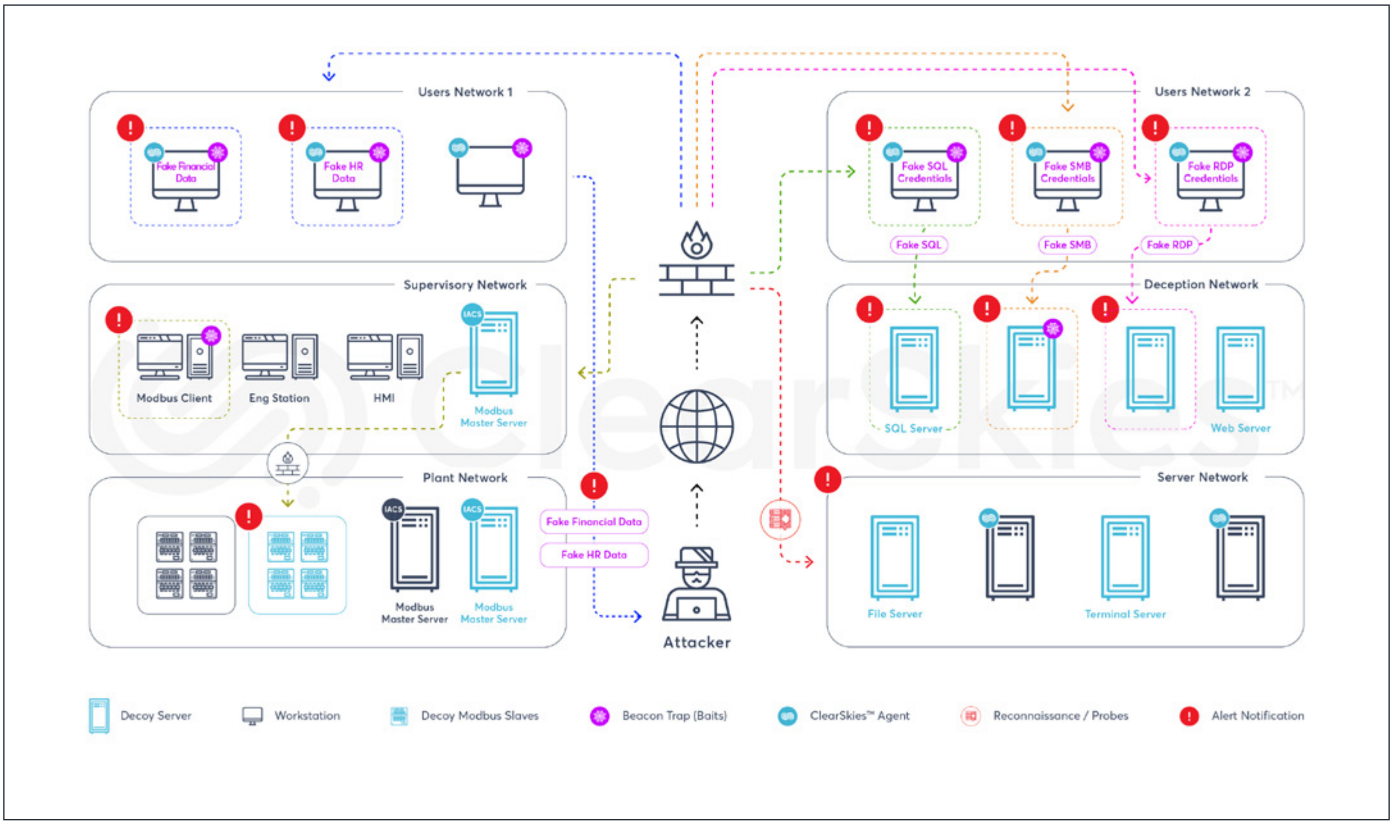

Figure 7: “Deception Defense Layer” complementing the “Defense-In-Depth” layered security by utilizing

Key Features & Benefits

- **Post-Breach Detection:** Minimizes the time between the initiation of a cyberattack and its detection.
- **Decrease attacker dwell time:** Drastically reduces the time a successful attacker spends scouting unnoticed within the corporate network and systems.
- **Comprehensive visibility:** Provides com¬prehensive visibility of the attacker’s intentions in your corporate network.
- **Reduced False Positives:** Focuses on real threats, thus accelerating your organization’s response and overall cyber defense capability, effectively improving your security posture.
- **Intelligence Gathering:** Helps you gather valuable intelligence and collect valuable forensic information about a cyberattack, including methods used, purpose and source, which can be used to both improve your network and system defenses, as well as to construct and support relevant legal cases against the attacker.
- **Regulatory compliance:** Helps you obtain evidence to meet regulatory compliance requirements.
- **Scalable:** Can be easily scaled at any given time, depending on organizational needs and/or on the information-threat activity level.
- **No risk:** Poses no risk whatsoever to data exchanged/stored and has no impact on the availability/integrity of resources.

Decoy License Bundles

The following Key Technology Decoy Bundles are available. Bundles could include one or more decoys, which imitate specific functionality and/or behavior. On access, Decoys trigger alert notifications and send along with related attack-vector information, to **ClearSkies™ Cloud SIEM** for further analysis as shown below.

Decoy Bundles	Event	Action Triggers	Attack Vector Information
Reconnaissance	Port Scanning	NMAP scans: NULL, OS, XMAS, FIN & SYN	• Source IP address • Destination IP address • Ports scanned
Web Access	HTTP get request	HTTP access attempt	• Source IP address • Web path requested • Browser User Agent
	HTTP login	Login access attempt	• Source IP address • User submitted credentials • User Agent
Database Access	MySQL Database Authentication	Authentication access attempt.	• Source IP address • User submitted credentials
	MSSQL Database Authentication	MSSQL authentication access attempt. **Note**: Both Windows and mixed mode authentication methods are supported.	• Source IP address • User submitted credentials
Remote Access	Remote Desktop Protocol (RDP)	Remote Desktop Protocol (RDP) access attempt.	• Source IP address
File Access	Shared directory or folder	Access a file within share directory	• Username submitted credentials including domain name or workgroup • File Name access • Client hostname • Directory path • Source IP address • Client SMB protocol version

File Transfer	FTP login	FTP login access attempt.	• Source IP address • User submitted credentials
	TFTP access	TFTP file access attempt.	• Source IP address • File Name access • File 'READ/WRITE' actions
Network Access	TELNET login	Telnet login access attempt.	• Source IP address • User submitted credentials
	SSH login	SSH login access attempt. **Note**: Both password-based and key-based authentication are supported	• User submitted credentials • SSH server string supplied • SSH client string supplied • SSH key used • SSH key monitored
	SNMP Request	SNMP request attempt.	• SNMP community string • SNMP OID requested
Industrial Control System - Modbus	Modbus Master/Slave request/response	Modbus client access attempt on Modbus-Master Can be configured with the following attributes (values returned during reconnaissance): • Number of Slaves • Vendor Name • Product Code • Major/Minor revision • Vendor URL • Model Name	• Source IP Address • Protocol used tcp/udp • Timestamp • Modbus-Master data received: includes binary commands Operations/ Functions such as: - Read Coils, - Read Discrete Inputs, - Read Holding, - Registers, - Read Input Registers, - Write Single Coil, - Write Single Register, - Write Multiple Coils, - Write Multiple Registers, - Report Slave ID • Returned data to adversary: binary output based on the above Operations/Functions called

Beacon Traps

The following Key Beacon Traps are available. One or more Beacon Traps can be enabled on the same workstation/server. On access, Beacon Traps trigger alert notifications and send along with related attack-vector information, to **ClearSkies™ Cloud SIEM** for further analysis as shown below.

Beacon Traps	Baits "poisoned data"	Action Triggers	Attack Vector Information
Files of different file formats which contain fake information/ data placed strategically amongst real information/ data.	Network design, systems Information, IPs in use, business applications, critical systems	• Access, • Edit, • Read, • Delete, • Rename, • Use the information found on files • Directory listing (File Explorer or CMD)	• Trap Type • Event Type Triggered • Host IP address • Username • Service Timestamp
	HTTP, FTP, SSH, SNMP, RDP, TFTP, Telnet user login credentials		
	MySQL, MSSQL Database user login credentials		
	Shared directory or folder access		
	TFTP access		
	SNMP Request		
	Financial Data, PII, Intellectual property, etc.		

System requirements

Below you will find the minimum system resource requirements for running ClearSkies™ Active Defense Decoys and Beacon Traps.

ClearSkies™ Active Defense virtual appliance

The ClearSkies™ Active Defense virtual appliance can be installed on a virtual system environment and, depending on the model configuration, can emulate up to 40 simultaneous Decoys.

Appliance Characteristics	ClearSkies™ Active Defense 10	ClearSkies™ Active Defense 20	ClearSkies™ Active Defense 40
Number of supported Decoys	up to 10 Decoys	up to 20 Decoys	up to 40 Decoys
Hypervisor type & version	VMware / Hyper-V	VMware / Hyper-V	VMware / Hyper-V
Supported version	5.1 or later/ 5.0 or later	6.0 or later/ 5.0 or later	6.0 or later/ 5.0 or later
Virtual CPUs	2 (6 cores)	4 (6 cores)	4 (8 cores)
Virtual Network Management Interface	1	1	1
Virtual Memory	8GB	12GB	24GB
Virtual Storage	150GB	250GB	400GB

ClearSkies™ Active Defense “Beacon Traps”

The minimum system requirements for activating ClearSkies™ Active Defense “Beacon Traps” on ClearSkies™ Endpoint Detection & Response (EDR) Agent are as follows:

System Requirements	Resources
CPU	Intel i5 3.0 GHz quad core or equivalent processor
Memory	8 GB
Disk Space	20 GB

Contact Us

Cyprus (Headquarters)

1 Lefkos Anastasiades Str. 2012
Strovolos, Nicosia

T +357 22 463600
E info@clearskiessa.com

www.clearskiessa.com

OFFICES CYPRUS | GREECE | USA | UK | KSA