Defensys Threat Deception Platform

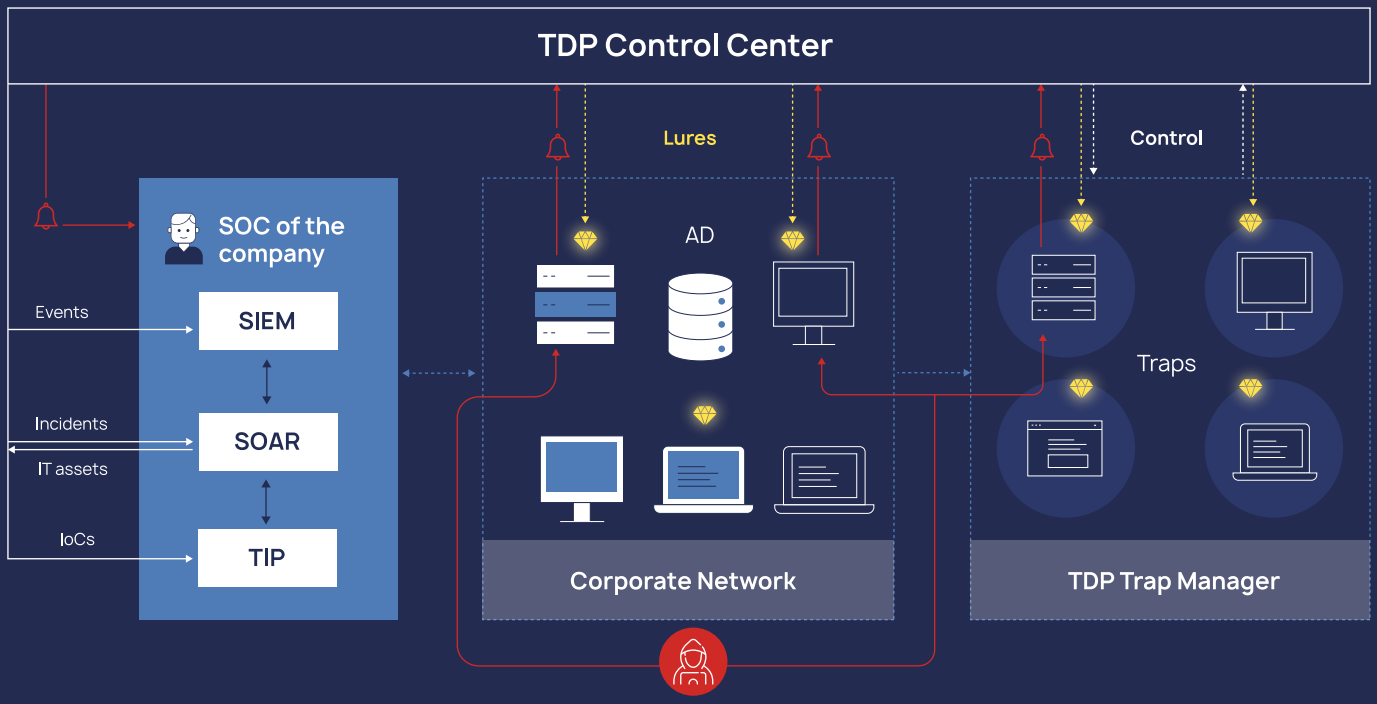
Solution for unknown threats detection
via IT & OT infrastructure parts simulation

Defensys

Defensys Threat Deception Platform is a comprehensive all-in-one tool for digital infrastructure simulation designed to proactively detect and prevent cyberattacks. With a complex combination of lures and traps, Defensys TDP detects intruders, delays their progress within the network, and ensures the cyberattack mitigation.

Defensys TDP key benefits

- Detects attacks that other tools fail to detect (targeted attacks, zero-day threats, and more)
- Reduces the intruders' progression within the network by creating an additional emulated elements layer
- Prevents attacks earlier to limit the impact of a threat
- Identifies security vulnerabilities to understand intruders' tools and behavior against the company's infrastructure



Platform Components:

Trap Manager is a trap management server

Control Center is a platform management server

System Benefits

- **Flexible traps and lures configuration** to better adapt and respond to changing company's real infrastructure dynamics
- **Maze-like tools to lure attackers** by mimicking a live system with all the typical users and services activity
- **High deployment and scalability** through automatic deployment of traps and lures
- **Clear detection of compromised systems** and automated response when deployed with other Defensys products

Centralized management of the trap system

Defensys Threat Deception Platform delivers an automated traps system that naturally emulates your company's IT assets and manage them from a single center.

With out-of-the-box trap system templates, you can quickly recreate organizational branches and imitate specific systems. To be more appealing and realistic, emulated elements combine groups of interacting hosts, services, or applications working together to better imitate a computer network.

Generating and deploying lures automatically

To raise the attacker's profile, Defensys TDP automatically sets its traps and lures in the real infrastructure. You can generate traps and lures automatically according to the company-specific parameters.

Intruder and malware detection

Defensys TDP collects events when logging interaction with lures and traps, processes them, and sends a detection alert to the cybersecurity expert. Afterwards, these events enrich with additional context and can be automatically sent to external systems such as SOAR and SIEM to respond and prevent the attack progress.

Low rate of false positives

Traps and lures are strictly designed to get an attacker's attention and are not used in regular workflows, so any interaction with them is highly likely to reveal an incident.

Identifying compromised systems

Using the Defensys Threat Deception Platform together with the Defensys SOAR enables you to quickly assess the scale of the attack, its targets, identify other compromised systems within your company, automate the response, and mitigate the attack.

Collecting attacker's attributes

While analyzing the attacker's activity, Defensys TDP collects attributes and IoCs that can be immediately exported to the Defensys Threat Intelligence Platform. The close integration of the two platforms provides:

- Further data enrichment
- Correlation with further available information
- Configuring automatic monitoring in SIEM events
- Mitigation with security tools

A trap is a point of interest to attackers. The traps are:

- Windows/Linux virtual machines
- Interactive emulation: SMB, SSH, HTTP(s)
- Basic emulation: SSH, HTTP(s), FTP, Telnet, POP3, IMAP, SMTP, SOCKS5, VNC, RDP, PostgreSQL, MySQL
- OT components

A lure is potentially valuable information. The lures are:

- Configuration files of popular administration tools
- Data files (Word / Excel / PDF)
- User accounts
- Browsing history
- SSH keys

Defensys

About Defensys

Defensys is an award-bearing and nationally acknowledged vendor of cybersecurity solutions. Since 2011, we have been fostering government agencies and private-sector companies to confidently withstand modern cyber threats and ensure reliable security management worldwide.

Defensys technologies are embedded in financial, public, oil and gas, energy, metal industry, and other sectors.

sales@defensys.com

Cybersecurity Digest:
defensys.com/blog/