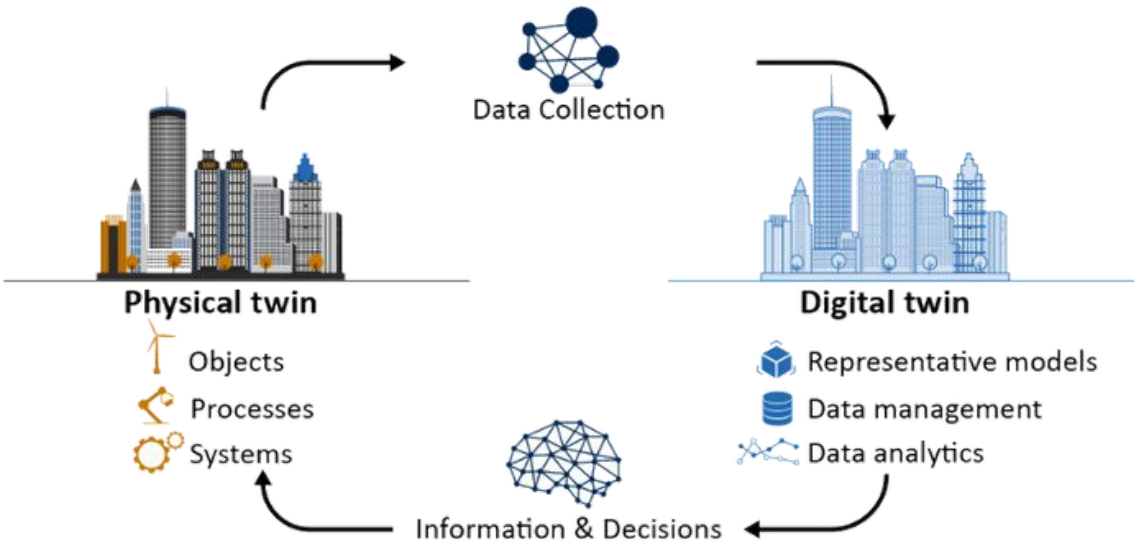
activeSENTINEL™

Digital Twin System - Security

The activeSENTINEL™ DTS uses the concept of digital twins for security in the context of fake or deceptive networks involving the creation of a digital replica of your network infrastructure and monitoring it for anomalies, potential threats, and vulnerabilities. This helps you detect and respond to unauthorized or malicious activities effectively. Most importantly, it allows customers to proactively be warned of network intrusions, giving you time to react before hackers obtain sensitive information or hold your network for ransom. Here's how you can use digital twins for network security:

DTS first creates a Digital Twin of Your Network:
DTS develops a comprehensive digital model representing your network infrastructure, including servers, routers, switches, firewalls, and endpoints. Include configurations, network traffic patterns, access controls, and network topology in your digital twin.

Step 2, DTS integrates network Data and Monitoring:
Integrating real-time data from your actual network into the DTS system digital twin engine is central to all security activities. This data should include network traffic logs, access logs, firewall logs, and other relevant information. DTS continuously synchronizes the digital twin with your live network data to ensure it accurately reflects the current state of your network.



activeSENTINEL™ and Anomaly Detection:
The DTS machine learning and artificial intelligence algorithms analyze the data from your digital twin. By looking for unusual or unexpected patterns of network traffic or behavior, DTS maintains a constant state of alert for any changes in physical and digital twin environments. The user can then establish alerts and triggers to notify security personnel when anomalies are detected. These anomalies could indicate a fake network or unauthorized activities.

DTS Threat Simulation and Testing:
Employ your DTS digital twin to simulate various threat scenarios, including the presence of fake or deceptive networks. These threats could be external or internal to the network for a holistic testing approach. Conduct penetration testing, vulnerability assessments, and red team exercises to identify weaknesses in your network and security controls.

activeSENTINEL™

Digital Twin System - Security

DTS Behavior Analysis:
DTS implements behavioral analysis algorithms to understand the expected behavior of devices and users on your network. Thereby detecting deviations from normal behavior that might indicate the presence of fake or rogue devices.

Access Control and Authentication:
Use the digital twin to model and test access control policies and authentication mechanisms. This ensures that only authorized devices and users can access critical parts of your network.

Response and Mitigation:
When the digital twin detects suspicious activity, DTS implements automated or manual response mechanisms to mitigate the threat. Isolate or quarantine suspicious devices or network segments to prevent further damage.

Legacy decoys are a security mechanism used in cybersecurity to detect, deflect, or study attempts at unauthorized use of information systems. It's essentially a trap set to detect, deflect, or study attempts at unauthorized access or information systems.

The dynamic creation of **SENTINEL AI Decoy** allows activeSENTINEL™ to evade attack with dummy data while learning an attacker's methods while itself acting, not as part of the intrusion system, but merely a component of surveillance system and can detect intrusions while also deceiving the malignant party.

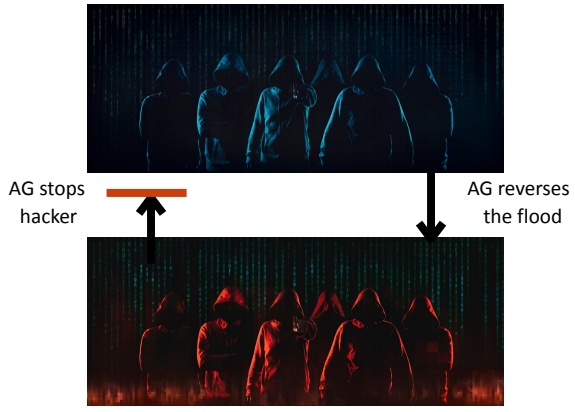
Threats never sleep and neither does activeSENTINEL™

Logging and Audit Trails:
Maintain detailed logs and audit trails within the digital twin to track all network activities. These logs can be valuable for post-incident analysis and forensic investigations.

Regular Updates and Testing:
Keep your digital twin up to date with changes in your network infrastructure and security policies. Continuously test and refine your security strategies using the insights gained from the digital twin.

Collaboration and Training:
Systems and users can share information and insights from the digital twin with your security team and network administrators. The United Sentinel Alliance is a central repository to enable such sharing of malicious activities and countermeasures used against them.

DTS includes implementations of "**Dynamic Tarpits**," where the service offers an open telnet, ssh, or HTTP port disguised as a target. Then, when an attacker connects, it does some protocol manipulation to artificially stall out the attacker -- e.g., sending an infinitely long banner message, sending the data one byte at a time just fast enough to avoid timeouts, or sending "wait" messages over and over again.



activeSENTINEL™ Digital Twin

activeSENTINEL™ WT-100
Supports up to 100 Tactical Sentinels

6 Port 10/100/1000 with 2 1G SFP and 2 10G SFP+ ports with Next-gen Firewall features for enterprise offices. Features a high-performance Intel processor, 512G SSD, 32G RAM, and Dual PSU

activeSENTINEL™-WT-1000
Supports up to 1000 Tactical Sentinels

6 Port 10/100/1000 with 2 1G SFP and 4 10G SFP+ ports with Next-gen Firewall features for enterprise offices. Features a high-performance Intel processor, 512G SSD, 32G RAM, and Dual PSU

activeSENTINEL™-WT-10000
Supports up to 10,000 Tactical Sentinels

6 Port 10/100/1000 with 2 1G SFP and 4 10G SFP+ ports with Next-gen Firewall features for enterprise offices. Features a high-performance Intel processor, 512G SSD, 32G RAM, and Dual PSU

The role of the activeSENTINEL™ Digital Twin Solutions is multifaceted, even if its primary objective is to occupy the attacker's time. Dedicated hardware focused on DTS performance is central because the actual machines that are being attacked in parallel will still fall should performance be compromised. The offensive is met by DTS's counteroffensive, as the whole network is under attack.

In certain situations, AI may need to adopt a distinct approach when dealing with specialized attacks involving varied attack models. Instead of simply delaying the attacker, the AI's response is to allow the system to accumulate sufficient evidence of an attack's existence, justifying the blockage of the source of the threat only during the initial stages of the attack. This action is taken before the attack script manages to deploy an exploit payload. The automated block requires a substantial amount of evidence due to the inherent risk of misidentification. However, the presence of numerous emulated machines on the network significantly amplifies the quantity of evidence the system can gather, even from relatively innocuous low-profile scans aimed at emulating benign auto-discovery processes.