Cyber Deception Platform.

Overview.

Illicium is a fully customizable Cyber-Deception Platform that allows you to deploy deception capabilities throughout your entire infrastructure, while increasing security against unknown threats and passive attacks, without compromising the current infrastructure resources. It provides an easy to use interface to create baits that can then be deployed with a single click to assets such as networks, systems, files, data, or even applications. The baits lure the attacker away from your real assets and into an isolated environment, the DeepMaze, where you can keep the attacker and record his actions.

Components.

Agents

The agents allow the deployment of deception functionality in the targeted assets. Agent installation can be done either remotely, or locally. Agents are fully managed through the Illicium Server. All communication between agents and the appliance is encrypted with TLS encryption. Agents are extremely lightweight as their activity is minimal when there is no attack to the asset, and their operation is transparent to the users (no pop-ups, no messages, no warnings. All information is gathered on the server).

Baits

Baits are the deception elements that are deployed throughout the target infrastructure. Baits are configured at the Illicium server and are implemented mainly through the agents.

Illicium incorporates baits for every deception layer and of all deception types. But if for specific scenarios the currently

Top Benefits.

- Detect threats that have bypassed all your active defensive mechanisms.
- Increase your chances to identify internal threats, 0-days, APTs, targeted and passive attacks.
- Deceive and delay the attacker.
- Calculate Attacking Trends.
- With the information gathered from the operation of Illicium you can design more effective Defensive Measures.
- As there are almost no false positives, you reduce detection and response times.
- Through Illicium you can have deception either as a Platform or as a Managed Service.

available baits are not enough, Illicium allows the implementation of fully customized baits. This allows you to implement any deception scenario, no matter the complexity.

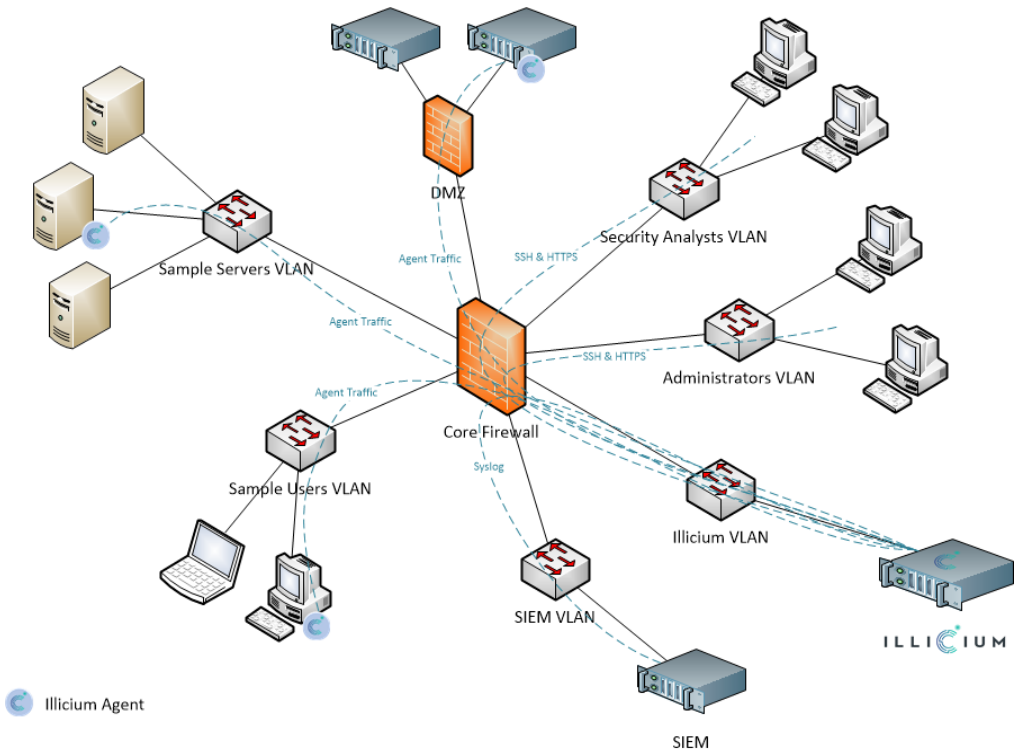
DeepMaze

DeepMaze is an isolated simulation of the organization's production environment. It consists of virtual systems that resemble the live production systems but have no real data on. Those systems are NOT clones of the original systems, but instead they are created from scratch and integrate only non-critical information from the original systems, in order to deceive the attacker into thinking they are the actual production systems. Although DeepMaze is not always essential for deception to work, its development increases greatly the realism of the deception deployment and provides the capability of secure attacker isolation.

Use Cases.

- Internal threat lateral movement detection.
- Passive attacks detection (attacks that the attacker does not take direct action on the asset).
- Increase attack detection accuracy.
- Detect unauthorized operations.

HIGH-LEVEL PHYSICAL CONNECTIVITY



Availability.

Illicium is available either in Software, Virtual Appliance, Physical Appliance, Platform as a Service (Cloud) or Deception as a Service form. In Software, Physical and Virtual Appliance form you get everything you need to install and deploy Illicium in your premises. The PaaS offering gives you the flexibility to add deception to your environment without the need to install an appliance, as the appliance is in the cloud. If you don't want to operate the deception deployment yourself, you can get Illicium in the Deception as a Service format, offered from Neurosoft's SOC. In this case you will have the minimum involvement in the whole deception deployment and management process.

Key Features and Specifications.

Feature / Spec	Value
Deception Layers	All (Network, Endpoint, Application, Data)
Number of Baits	Unlimited (subject to license)
Integration with real assets	Yes
Supported operating systems	• Debian-based (Debian, Arch, Ubuntu, CentOS) • RedHat-based (RedHat, CentOS, Fedora) • Microsoft Windows 7 or newer • Microsoft Windows 2012R2 or newer • Raspberry Pi Linux In addition to the operating systems mentioned in this list, any POSIX compliant operating system is supported (eg IBM AIX)
Attacker Isolation	Yes
Deception Customization	Ability to fully customize: • Honeypots (decoys / lures) • Baits (traps / breadcrumbs) • Deception Scenarios
Attack Traffic Analysis / Capture	Yes (export to pcap file)
Users and User Roles Management	Yes
Rules	Illicium gives you the ability to create fully customized rules for: • Attack Detection • Emergency Response (through scripts) • Alerting (on console, via logs, via e-mail)
Reporting & Statistics	Integrated reporting mechanism available for predefined reports. Grafana interface available for customised reporting.
Deployment Monitoring	Ability to customize the interface per user role
Backups Management	Yes
Northbound API	REST
Multitenancy	Yes (subject to license)
Connectivity with SIEM or other logging systems	via syslog
Distribution Options	Software Virtual Appliance Physical Appliance Platform as a Service (Cloud) Deception as a Service

Requirements.

Component	Requirements
Illicium Server	For the Physical Appliance option, the requirements are: Rack Space: 1U Network: 1x RJ45 Ethernet connection Power Supply: 450W For the Virtual Appliance option, the requirements are: CPU: minimum 2-Cores recommended 8-Cores* RAM: minimum 4 GB recommended 32 GB* HDD: minimum 50 GB recommended 1 TB* Enabled Nested Virtualization For the Software Installation option, the requirements are similar to the Virtual Appliance, with the addition of a CentOS 7 or newer operating system. * The minimum requirements cover only the operation of Illicium without the deployment of an extended DeepMaze network. Each installation's requirements depend on the size and operation of the systems in the DeepMaze.
Microsoft Windows Agents	Min. Microsoft Windows 7
Microsoft Windows Server Agents	Min. Microsoft Windows 2012R2
Linux Agents	Debian 8.0 or CentOS 6.9 or newer based linux distributions.

Physical Appliance Specifications.

	Physical Appliance
Format	rack-mounted server
Dimensions	19" (1U)
Processor	Intel Xeon
Installed Memory	32GB (2x16GB 2Rx8 DDR4-2400 U ECC)
Storage	1TB (2x 1TB Hot Plug in RAID1 configuration)
Networking Interfaces	2x 1 Gbit Ethernet LAN
Power Supply	1x hot plug modular power supply module Ability to install an additional module for redundancy 450 W Active Power, 380 W Rest
Working Temperature	5°C - 25°C / 41°F - 77°F
Warranty	Standard warranty: 1 year, On-Site Service
OS Software	Illicium Server Software (pre-installed)

About Us.

Founded in 1994, Neurosoft began as an in-house software development company with the vision of providing quality solutions and services to its clients both in Greece and abroad. Since then, Neurosoft has evolved into a fully integrated ICT company with Software Development, System Integration and Information Security capabilities, offering its products and services in SEE and MENA. The staff headcount currently exceeds 200 highly skilled employees with in-depth experience in their fields. Our projects are governed by our Certified Management Systems for Quality (ISO 9001), Information Security (ISO 27001) and Occupational Health & Safety (OHSAS 18001) and a series of strict procedures according to international standards. Neurosoft is listed in the AIM Italia exchange since 2009.

NeuroSoft S.A.
466 Irakliou Ave. & Kiprou
141 22 Iraklio Attikis, Athens, Greece
T.: +30.210.6855061
F.: +30.210.6855033
E-mail: info@neurosoft.gr
Website: www.neurosoft.gr

Learn more at: www.deceivewithillicium.com