ILLICIUM

KNOW THE ATTACKER

Today's information technology landscape is threatened by modern advanced security attacks, including 0-day exploits, polymorphic malware, and APTs. These threats cannot be identified and mitigated using classic detection and prevention technologies; they can mimic valid user activity, do not have a signature, and do not occur in patterns. In response to attackers' evolution, defenders now have a new kind of weapon in their arsenal: Deception.

NEUROsoft

EXISTING SECURITY MECHANISMS ARE NOT CAPABLE OF PROTECTING ORGANIZATIONS FROM UNKNOWN OR CAREFULLY EXECUTED ATTACKS.

Common defensive security solutions, such as anti-malware, UTM, IDS/IPS, anti-spam, content filtering, Security Policies, even DLP and SIEM, are unable to detect advanced attacks or face unknown threats. At the same time they generate large amounts of false positives that consume time and direct administrators away from the actual danger. Attackers are now very careful in order to avoid getting caught, and by using modern attack methods they avoid being detected.

To solve this problem a new defence method emerged: Deception Technologies; a category of defensive methods that can detect, identify, analyse, and defend against unknown and advanced attacks. They allow immediate identification of the attack, have a high degree of accuracy and give the defender the ability to monitor the attack. By deceiving the attackers, they detect and manage the attack in its full development.

YOUR SECURITY SYSTEMS CAN IDENTIFY KNOWN THREATS, BUT ILLICIUM CAN IDENTIFY EVERYTHING ELSE.

Illicium is an innovative deception platform that enables organizations detect and identify information security attacks, including - but not limited to - unknown threats such as 0-days, custom or new malware, even APTs. It has a unique architecture that integrates all deception techniques in one product, and a powerful interface that gives full power to the defender. By deploying a large number of baits throughout the organization, it deceives the attacker and makes him believe he is hacking the real assets, while at the same time his actions are fully monitored in an isolated environment. This way it allows the organization to identify and close the attack path in order to prevent future attacks.

INNOVATIONS

Illicium, through its state-of-the-art architecture:

- Covers all currently available deception techniques
- Gives full attack visibility
- Applies deception on any platform, even custom ones
- Integrates with other security solutions (i.e. SIEM)
- Minimizes the load of the current infrastructure

KEY FEATURES

Illicium's key features include:

- Support of multiple Users and User Roles
- Graphical representation of attacker info
- Graphical representation of target info
- Ability to create rules for detecting attacks
- Ability to create rules for emergency response
- Alerting via e-mail, SMS or other channels
- Reporting & Statistics
- Customizable deployment monitoring per User
- Backup management
- Northbound API to connect with external applications
- Integration with SIEM or other security systems

EFFICIENCY

Illicium's deceptive technology offers an efficient way to:

- Detect valid attacks with very high confidence.
- Deceive and delay the attacker by making him believe that he is hacking the right systems while he is actually hacking something fake.
- Gain enough time for reaction by isolating the attacker in a fake infrastructure, recording his tactics and properly adapting the security systems to his attack pattern.

T: +30 210 6855061 • F: +30 210 6855033
E: info@neurosoft.gr • W: www.neurosoft.gr

ILLICIUM

www.deceivewithillicium.com