Annex 3 - Proposal for Partnership with Labirynth Security Solutions

Proposal for Partnership

Labyrinth Deception Platform is a cybersecurity solution for the detection of hacking activities and attacks on internal IT infrastructure and services. The Platform is proven to be very effective for uncovering advanced threats that have bypassed network perimeter defense. In such cases, the LDP takes a hit and gives time necessary for the reaction to the attack.

The efficiency of the Platform is achieved by simulating a broad range of real services (mail, web applications, etc.) and common vulnerabilities, that make these services attractive to adversaries. Additionally, the system mimics the user's network connectivity and all kinds of decoys (files, links, ssh keys, etc.), to increase the probability of an attacker getting into simulated services.

As a result, a security team gets notifications about abnormal events in a corporate network and detailed information about incidents, including the source and type of attack.

Benefits of using

• Detects and stops targeted and advanced cyber-attacks without requiring any prior knowledge of the form, type or behavior of the threat.

• Reduces cyber security operating costs by up to 30% - does not collect tons of data, does not generate false positives, does not require special skills to use.

• Accelerates incident response by reducing the average time to detect and respond to threats (MTTD, MTTR) by 12 times.

• No negative impact on the performance of network devices, hosts, servers, or applications.

• Fast and easy deployment, no system conflicts and no maintenance needed - no databases, signatures, or rules to constantly configure and update.

Advantages over other cyber threat detection approaches

Advanced Threat Detection

- Allows you to detect intruders on your corporate network up to 12 times faster
- Detects basic and advanced threats regardless of the methods used
- Collects data on the movements of intruders and the tools they use

Process optimization for SOC

- Significantly simplifies the process of incidents' prioritizing
- Reduces time spent on false positive notifications investigation
- Provides full visibility of the attack in real time

No deep knowledge required

- Easy installation and configuration
- No special skills required to use the solution
- Automatic detection and response to incidents when integrated with third party tools

Technical advantages over other Deception solutions

- Unlike other Deception solutions, the Labyrinth platform uses complex methods to detect and prevent human-driven attacks. This approach implements not only Deception methods, but also a wide range of other tools for detecting complex cyber threats.
- All simulations created by Labyrinth are high interaction decoys - provide interactivity at the level of at least responding to a scan, prompting for credentials, displaying a graphical and/or text interface. Each decoy is unique, with one IP address, no IP alias is used. This provides the industry's best believability for the simulations you create.
- Unique type of traps - Universal Web Points. The system scans the network and uses the collected information to automatically create emulations of local Web resources of the network with the addition of vulnerabilities and the possibility of exploiting them (scan response, requesting credentials, displaying a graphical interface).

Advanced system features:

- The system detects MiTM (man-in-the-middle) type of attacks.
- The system provides the ability to create a Windows host that periodically connects via VPN (PPTP) to remote network segments.
- The system provides the ability to create traps that periodically connect to external WEB resources (news sites, etc.).

Commercial advantages over other Deception solutions

- Industry-leading Time to Value - the entire system deployment process from start to run takes only a few hours.
- For the full functioning, the system does not require additional purchase of third-party software licenses (eg Windows).
- Does not require a lot of hardware resources for system deployment
- Supports VMWare and HyperV hypervisors, the management console has support for KVM (Proxmox, OpenStack),
- Flexible licensing based on an infrastructure size and customer needs,
- Not licensed by the number of Breadcrumbs, endpoints, etc. – licensing is based on the number of network segments (one license gives the right to connect 1 VLAN and deploy up to 15 decoys in it) or alternatively on the assumed number of decoys in the entire network (without VLAN limitation),
- Default technical support in a 12/7 model, the right to software updates, etc. - all within a single subscription price (no hidden additional fees),
- Prices for the solution are much more affordable than those of competitors.

We will be pleased to provide any additional information you may require.

Yours sincerely,

Paweł Rybczyk

Chief Channel Officer | Labyrinth Security Solutions

+48 664 300 375

info@labyrinth.tech