CASE STUDY

Summary

SoftServe is a global IT company of Ukrainian origin. The portfolio includes a wide variety of services provided to our customers – software engineering, big data & analytics, AI & ML, the Internet of things, cybersecurity, experience platforms, extended reality, robotics, research & development.

SoftServe delivers open innovation, from generating compelling new ideas to developing and implementing transformational products and services.

SoftServe had successfully completed over 20 000+ projects globally and provides services to market leader entities such as Cisco, IBM, Allscripts, Atlassian, Coupa, Panasonic, Logitech, and many others.

Challenge

SoftServe employs more than 13,000 associates in 55 development centers, offices, and client locations globally, with our most significant operations in Central and Eastern Europe. SoftServe does not rely on one specific office location or country for its operations. SoftServe's IT and security infrastructure is cloud-centric with services delivered from distributed data centers in CEE, the EU, and the US.

softserve

With growing cyber threats around the globe, we should keep our security standards at the highest level to protect our assets, associate's and customers' data. The challenge for us is to lower the risks of potential breaches and unsolicited access.

It is also required to provide and establish a valid response toolset for the internal Cybersecurity Operation Center to deal with potential violators who may have already entered the network (e.g. via a compromised VM installed on the corporate user endpoint).

Realization

The deception functionality was selected for implementation as an additional protection toolset. The configuration of traps should be similar to the existing corporate assets available in the corporate network.

Labyrinth Admin VM and Labyrinth Worker VM were deployed on hundreds SoftServe server LAN and DMZ segments with thousands of LAN hosts in it.

Solution

Implementation of the deception system was done in several steps:

1. Identified a corresponding number of traps based on the number of active hosts at each network.
2. Identified and investigated all types of services in each network segment.
3. Deployed and configured honeypots in accordance with analysis results.
4. Established proper 24/7 incident detection and response. Configured required detection events and developed playbooks for the internal CSOC team to provide reactions to potential incidents.
5. Reduced false positive detections in our SIEM. We built a behavioral model of services and users within the network to finetune our response procedures.

Results

The major validated outcome was external penetration testing with purple and blue team activities. Professional pentesters from one of the top security consulting company wasn't able to detect network traps and our CSOC had an appropriate security event demonstrating a successful trap for "hackers".

Additionally, Labyrinth deception deployment has proved itself as a viable addition to the existing SoftServe security toolset:

- We have significantly improved our visibility in isolated network segments.
- It helped us to identify existing "Network usage policy" violations and improve our security posture.
- Improved our detection of network configuration errors.
- Speeded up CSOC team reaction and response to malicious actors' unauthorized access to corporate resources. This was confirmed based on the results of independent third-party penetration testing activities.
- Provided us with a toolset to build up a typical behavioral and access model of the various services within our network.
- Improved our tradecraft analysis capabilities.

Based on the data gathered by the Labyrinth Deception Platform, we have significantly enriched our incident response capabilities. The gathered information by Labyrinth was a viable addition to our CSOC team in the field of detection and prevention of cybersecurity incidents. It became easier to make viable decisions during incident management reduce false positives.

Labyrinth is a team of experienced cybersecurity engineers and penetration testers, which specializes in the development of solutions for early cyber threat detection and prevention.