Digital Forensics and Incident Response

DIGITAL FORENSICS AND INCIDENT RESPONSE

Early detection and rapid investigation are critical to repelling attackers and responding to threats. But countless warnings, insufficient information, and lack of visibility can keep you from doing these important things. This is where we come in. We provide continuous 24-hour monitoring of IT resources, both in terms of cybersecurity (threat information and threat hunting) and rapid incident response (DFIR). We invite you to familiarize yourself with the SOC service as a service provided by the Security Operations Center (SOC) team.

CONTACT

Phone:
026 368 06249

Website:
unk9vvn.com

Email:
info@unk9vvn.com

INCIDENT RESPONSE

The most important aspect of SOC / CERT services is the competence of the technical team, because the level of knowledge of the experts determines the cyber security of the organization. The network, on the other hand, is covered directly using NIDS / IDS software to uniquely detect attacks on the local network. Malicious domains, IP addresses, and hash information (IoCs) are provided by our Cyber Threat Intelligence Information System, which receives information in collaboration with other international incident response teams.

THREAT HUNTING

Threat hunting and threat information have been introduced for more than a decade. Their achievements include hunting world-class threats, namely APTs, and responding to incidents. Advanced APT attacks are monitored by IoCs and their technical and tactical pattern of behavior is plotted in hunting techniques, which is called TTP. The ability to detect zero-day vulnerabilities (software vulnerabilities for which there are no security fixes) is a feature of threat hunting.

DIGITAL FORENSIC

We offer specialized digital forensic services called DFIR (Digital Forensic Accident Response). We use highly specialized commercial equipment and tools to perform forensic analysis.

Our digital forensic lab, which conducts dozens of data mining and data extraction monthly, consists of a number of professional and reputable software, including the FTK Forensic Toolkit and X-Ways Forensics, which allow you to get evidence from Analyze through documentation.

SECURITY INCIDENT

Proper security of digital tracking allows in-depth analysis of the incident and allows you to determine in detail how the attacker performed the operation. Over time, if the evidence is not properly secured, the system scripts will be lost, even if the user is working on it and the system is simply running.

On the other hand, shutting down a computer without the necessary prior protection, results in the irreparable loss of digital data stored in the operating system memory and reserved for the attacker. This data may contain important information for incident analysis.

IT ENVIRONMENT MONITORING

Today, digital security is a requirement of every company, so the most important issue is response speed. at SOC, we use dynamic defense technologies to identify new types of never-before-seen threats (unique examples in targeted attacks).

Each new instance is automatically analyzed in a sandbox to simulate behavior and identify malicious methods. Using products such as Splunk and ELK, all behaviors within the network will be collected and behavioralized.

SECURITY OPERATIONS CENTER

The experts of SOC (threat hunter) and CERT team are always trying to be active in the fields of defensive (blue team) and offensive (red team) in cyber security, as well as the implementation of a professional computer forensic laboratory so that they can perform proper actions in different situations, hunting and incident response specialists at the Security Operations Center are always in charge of data mining from data collection databases.

COMPUTER SECURITY INCIDENT RESPONSE TEAM

A team responding to known incidents can provide cyber assistance to government agencies and institutions in an emergency. This response to an incident at the time of a cyber attack is very important and can assist forensic teams in conducting an explicit investigation. For example, if an organization’s operating systems become infected with ransomware, it usually takes a short time for the ransomware to reach the Impact stage. If the digital forensic response team acts quickly, it can respond appropriately to the attack.

MALWARE ANALYSIS

Malware analysis is one of the key issues in data collection and forensic, which can be used to neutralize anti reverse engineering and anti-coding methods, It is also possible to perform appropriate operations in order to Behavior recognition and create a signature on the malicious file formats entered into the system and start data mining after reverse engineering the area in question.