# Blue Teaming and Cyber Defense

## BLUE TEAMING AND CYBER DEFENSE

The Blue Team allows us to detect targeted attacks that are not detected by common tools and security software. threat hunting is an evolving process, not a technology. We have a thorough knowledge of actual attacks and exfiltration techniques. We describe the attackers' methods so that we can identify them independently of the tools used to carry them out. In addition, we can use the resulting data for our threat information and CTI (Cyber Threat Information).

## CONTACT


:Phone
026 368 06249

:Website
unk9vvn.com

:Email
info@unk9vvn.com


## ARCHITECTURE AND SECURITY ENGINEERING

Independent program maturity assessment provides your organization with cyber security in four main areas: security governance, security architecture, cyber defense, and security risk management. After an in-depth analysis of your current plan, we offer the best practical advice to improve your security situation based on your specific risk profile and security maturity level. Needs assessment and field evaluation of your organization, architectural design plan and cybersecurity engineering, will be determined according to the level of services and communication.

## CYBER RISK MANAGEMENT

Evaluate your existing cyber risk management program for security strengths and weaknesses. Identify your organization's cyber threats and anticipate your business approach to cyber risk management and effective decision making and risk reduction. Define appropriate guidelines for quick response to risk management and try to harden cyberspace. Our experts take these findings to identify program flaws and in turn provide practical, technical, strategic and prioritized advice for creating or improving your cyber risk management plan and achieving a mature security situation and ultimately reducing future risks and their impact on your business.

## ACTIVE THREAT

We know how to effectively identify the signs of an attack and the presence of an attacker in the organization's infrastructure. This requires threat hunter to run proprietary software (such as a HoneyPot) or monitor DNS traffic and incoming logs within a network that seeks out malicious activity.

Checking the entropy of different types of DNS requests and comparing domains with attack attributes or (IoCs) received from threat information and so on. On the other hand, log analysis in this case is not limited to monitoring system events, but also means in-depth analysis of processes and examining the connection of processes of many resources, which can indicate a compromise of integrity.

## ACTIVE PROTECTION

For active protection, existing tests and security measures should be used to identify vulnerabilities and security audits should be fully established, also existing vulnerabilities should be assessed as a complement by intrusion testing services. Newer cases, such as cloud security and social engineering, and red team simulations, will be more specific cases about active protection.

Security assessments based on active vulnerability detection is another area of active protection, meaning that the blue team must always update systems reports on published vulnerabilities.

## ACTIVE IDENTIFICATION

Active detection means that the blue team expert manually designs active signatures for malicious files based on events reservoir discoveries , and constantly updates the signature repositories of detection mechanisms.

Active detection also monitors the communications and exploits of the protocols, and if the Exfiltration techniques in the MITRE ATT&CK documentation are observed by experts, immediately intercepts and data mining the connection and eliminates the connection if it is invalid.

## CLOUD SECURITY

Evaluate your existing security and hardware techniques for the most popular cloud-based assets, including Microsoft Office 365, Microsoft Azure, Amazon Web Services, and Google Cloud Platform. Understand security threats and controls for your cloud environment. Demonstrate your ability to identify, investigate, and respond to attack activity at all stages of the attack lifecycle. Examine security configurations and controls that are constantly running and identifying potential vulnerabilities. Also use reporting that includes detailed practical advice to harden the cloud, increase visibility, and identify and improve processes to reduce potential risk.

## OSINT

We use OSINT (Open-Source Intelligence) to gather significant information about the target organization on the Internet. The information obtained can be used to identify vulnerable assets and vulnerabilities that threaten targets. Information retrieved using OSINT techniques includes details about employees, organizational structure, physical assets, IT infrastructure, and more.

## SECURITY INFORMATION AND EVENT MANAGEMENT

CTI is used to continuously update information from an external source about a given organization. This service consists of two main parts: information about security teams and IOC (Compatibility Index), which is mostly for automatic data mining for internal monitoring with SIEM, IPS (Intrusion Prevention System) or IDS / NIDS / HIDS (Intrusion Detection System) systems. The simplest example of such data mining could be obtaining IP address information from the honeypot network used by attackers or detecting open port changes in the company's infrastructure. We use proprietary software that automatically looks for potential threats depending on the customer's needs. We support infrastructure monitoring with CTI data that allows us to detect targeted attacks on an ongoing basis.