Nixu Security Operations Center (SOC)

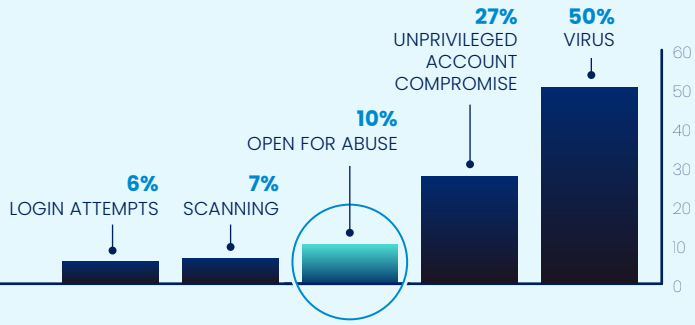
Detection and Investigation Data Snapshot

Q1/2022

Virus attacks and unprivileged account compromises accounted for majority of security incidents

Based on Nixu's SOC data, there were no dramatic changes in the volume of security incidents in Q1. Also relative changes within the top 5 **ENISA* security incident categories** were minimal.

Top 5 Enisa security incident categories



Preventable attacks against systems, Open for Abuse detected with MITRE ATT&CK based in-depth detection

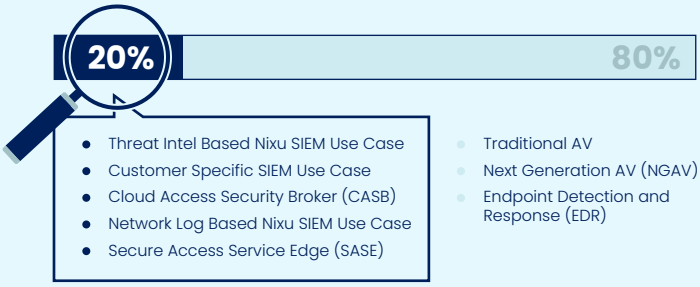
Drilling down on the Open for Abuse category and structuring it according to the **MITRE ATT&CK** framework**, we see that the most commonly used tactics were Defense Evasion and Initial Access. Other detections were based on **Persistence, Credential Access** and **Lateral Movement** tactics.

33% of open for abuse incidents that were detected by **Initial Access**

35% of open for abuse incidents that were detected by **Defense Evasion**

Detect-in-depth – Multiple methods are needed to detect malicious code

About one fifth of malicious code detection relies on less commonly used detection methods. Traditional and next generation antivirus software go a long way in catching malicious activity, but more in-depth detection methods are crucial in obtaining comprehensive security.



***ENISA**, The European Union Agency for Cybersecurity, is dedicated to achieving a high common level of cybersecurity across Europe. It has created a common Reference Incident Classification Taxonomy, which also Nixu relies upon in its SOC data analysis.

****MITRE ATT&CK** is a globally accessible knowledge base, which is used as a foundation for the development of specific threat models and methodologies. Nixu has the capability to utilize the ATT&CK Matrix for Enterprise in further analysis and categorization of its SOC data.