

# Meet our Team



**Zisis Ziogas – Offering Manager**

## **How does Neurosoft benefit from the exclusivity of its service Neutrify?**

Neutrify is Neurosoft's 24x7 Cyber Security Team, completely dedicated to monitoring and responding to threats and attacks in an organization. Neurosoft is staffed with cyber-security analysts and engineers as well as managers who oversee security operations and oversee the specific service. They cooperate with organizational incident response teams to ensure that security issues are addressed promptly. Neutrify team detects, analyzes, and responds to cybersecurity incidents using a combination of technology solutions and a strong set of processes.

## **Briefly describe Neutrify's responsibilities.**

Neutrify monitors and analyzes the activity of networks, servers, endpoints, databases, applications, websites, and other systems, all the while looking for anomalous activity that could be indicative of a security incident. Neutrify is directly responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported to clients. Beyond just monitoring, Neutrify offers additional capabilities including advanced forensic analysis, malware reverse engineering, UBA, threat intelligence, deception technology and many more services and solutions which are aiming to protect client's infrastructure even against 0-day attacks.

## **What strategic methodologies and processes does Neutrify use in order to maintain Neurosoft's cybersecurity defenses?**

Through its active surveillance and analysis, Neutrify uses strategic methodologies and processes to build and maintain the company's cybersecurity defenses. These procedures are broken down into the following identifiable tasks:

- Establishing awareness of assets - For Neutrify to help a company stay secure, it has a complete understanding of what resources they need to protect.
- Proactive monitoring - Neutrify must be vigilant in its monitoring practices.
- Managing logs and responses - Data is extremely important for Neutrify to function properly and logs serve as the key source of information regarding network activity.

- Alert Management - Automated systems are great at finding patterns and following scripts. The human element of Neutrify proves its worth when it comes to analyze further an automated alert.
- Root Cause Analysis - After an incident occurs and is resolved, Neutrify's job begins. Cybersecurity Analysts will analyze the root cause of the problem and diagnose why it occurred in the first place.
- Compliance Audits - Companies want to know that their data and systems are safe but also that they are being managed in a lawful manner. Neutrify team performs regular audits to confirm their compliance in the regions where they operate.

Each of these tasks is a critical function of Neutrify that keeps the organization well-protected. By covering all these bases, Neutrify maintains control of the company's array of systems and acts immediately and intelligently if an intrusion occurs.