alpha TECHNOLOGIES

SOC

# Security Operations Center as a Service.

alpha TECHNOLOGIES

# Tony Schliesser

## Chief Information Security Officer

A SOC, or Security Operations Center, is a specialized function within a organization consisting of people, processes, and technology that continuously monitors an information system for security events. A SOC receives data from a wide array of devices, as well as intelligence sources, that is used to identify events that require further investigation. Once an event is determined to be a security event, the response is guided through predetermined procedures, sometimes called playbooks, to limit the impact of the event.

A SOC also brings proactive capabilities, in the form of threat hunting, which allows an information security analyst to search for attack indicators within the environment. Threat hunting uses advanced monitoring tools that combine multiple data sources from the organization's IT infrastructure to help the analyst identify the early signs of an attack. Once an attack has been identified, response plans can be implemented to contain, eliminate, and guide necessary recovery efforts.

## Phishing: How SOC Can Help

How would a SOC handle a reported phishing attempt? After receiving notice of the phishing attempt, an information security analyst would review a sample of the phishing email against known threat intelligence, determine the risk the phishing attempt poses to the organization. Then counter measures would be implemented in the organization's IT environment, such as filtering specific URLs contained in the phishing email, searching for evidence that the attack was successful, and removing other copies of the email from the rest of the company.

## Who Needs SOC Services

The short answer is that every organization needs the ability to monitor their IT environment for threats and respond to them at some level. Every company should have antivirus, email/URL filtering, firewalls, and intrusion protection with the time to develop a disaster response plan. It is best practice to have these responses in place before a cyber threat happens.