



SOC AND SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR) SERVICES

A UNIFIED PROCESS THAT COMBINES PREVENTION, DETECTION, ANALYSIS, AND RESPONSE FUNCTIONS TO STREAMLINE THREAT REMEDIATION AND CREATE IMMENSE ROI.

"Increased threat sophistication requires a streamlined yet adaptable mitigation and remediation process. You must protect your assets by preparing for the inevitable, while assuring your stakeholders that information security is a top priority."

Chen Heffer, CyTech Founder & CEO

THE SOC CHALLENGE



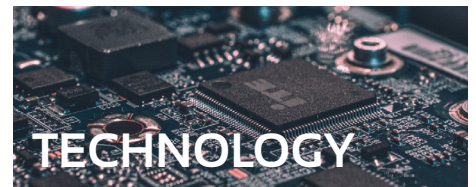
PEOPLE

Lack of knowledgeable security staff. Organization personnel can occupy multiple roles and functions, and must be cross-trained to wear multiple hats.



PROCESS

Lack of standardization leads to reactive ad hoc remediation efforts, which are not effective in today's landscape.



TECHNOLOGY

Legacy SOC's fail to address gaps between data sources, network controls and human capital. Limited visibility and collaboration between departments result in siloed decisions that do not support the organization's best interests.

CYTECH SERVICES

Security Orchestration Automation & Response (SOAR)

We help CISOs better utilize their Cyber Incident Response (CIR) resources and efforts. Security Automation utilizes technology to support and automate repetitive Security Operation Centre (SOC) actions. Security Orchestration involves all technologies and hands in the full Cyber Incident Response Process (CIRP) cycle, thus covering all critical incident response steps.

SOC Analyst Tier 1, 2 and 3

Our team will remotely connect to your SOC (view-only over VPN) and assist your incident containment, response and recovery efforts. If you need boots on the ground, our Cyber Incident Response Team (CIRT) will join forces with your IRT and help with incident remediation and investigation.

Ongoing SIEM Optimization

Our experts will conduct periodic SIEM rule analysis and review. This will help us recommend an optimization process that fits your security business needs and prepares you for evolving threats in your industry.

CIRT Training

Our CIRT will rely on their vast knowledge and worldwide experience to train your CIRT, thus putting your team in a better position to handle future incidents and fallouts.

Annual Organization Cyber Drill

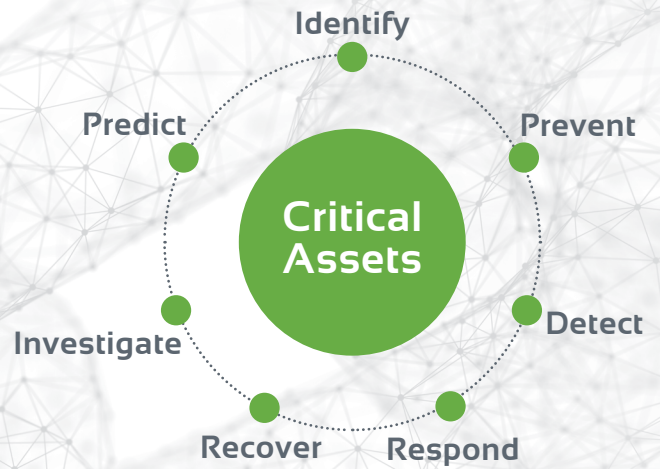
Our CIRT leadership will work with you to analyze your business environment and security requirements. This analysis will help us tailor an organizational cyber drill that will challenge your People – CIRT, Senior Management, IT, Users, Process and Technology controls.

THE CYTECH APPROACH

We've taken a majority of today's recommended approaches for managing cyber security such as NIST CSF, ISO 27001:2013, SANS Top 20 and others, and established an improved and holistic approach that can be adapted for organizations of all sizes and industries:

SECURITY OPERATIONS IS NO LONGER A CENTER. IT'S A PROCESS.

The need for a physical security hub has evolved into a virtual fusion of prevention, detection, analysis, and response. When all four functions operate as a unified process, your organization will be able to proactively combat changes in the threat landscape.

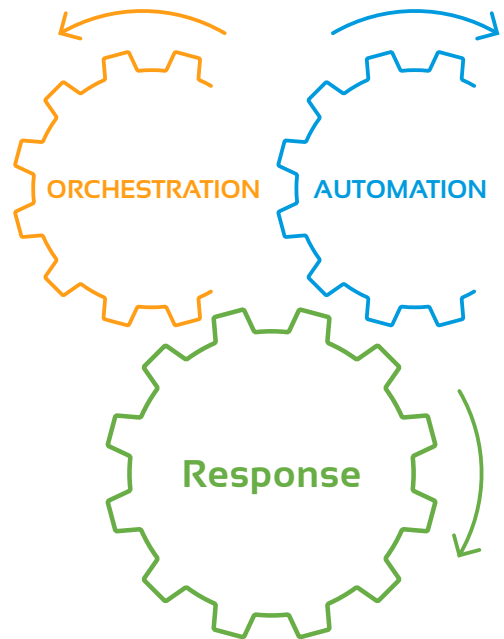


FUNCTIONAL THREAT INTELLIGENCE IS A PREREQUISITE FOR EFFECTIVE SECURITY OPERATIONS

Eliminate false positives by contextualizing threat data, aligning intelligence with business objectives, and building processes to satisfy your objectives.

IF YOU ARE NOT COMMUNICATING, YOU ARE NOT SECURE.

Collaboration eliminates siloed decisions by connecting people, processes, and technologies. With a transparent security operations process, you leave less room for error, consume fewer resources, and improve operational efficiency.



ABOUT CYTECH

CyTech is a unique one-stop-shop for CISOs. As a professional consulting firm, we partner with our clients to support their business goals and help create a secure and innovative cyber environment. We are always aware of technological advancements, **and are not affiliated with any vendors.**

Our consultants are all internationally certified, globally experienced and highly skilled in both business and cyber security. By improving decision-making and leveraging business insight, we help transform compliance efforts into a major competitive advantage.

CONTACT

Ms. Frewoini Adane | Mobile: +251 (0) 910372484 | Mail: fray.adane@ecs-et.com