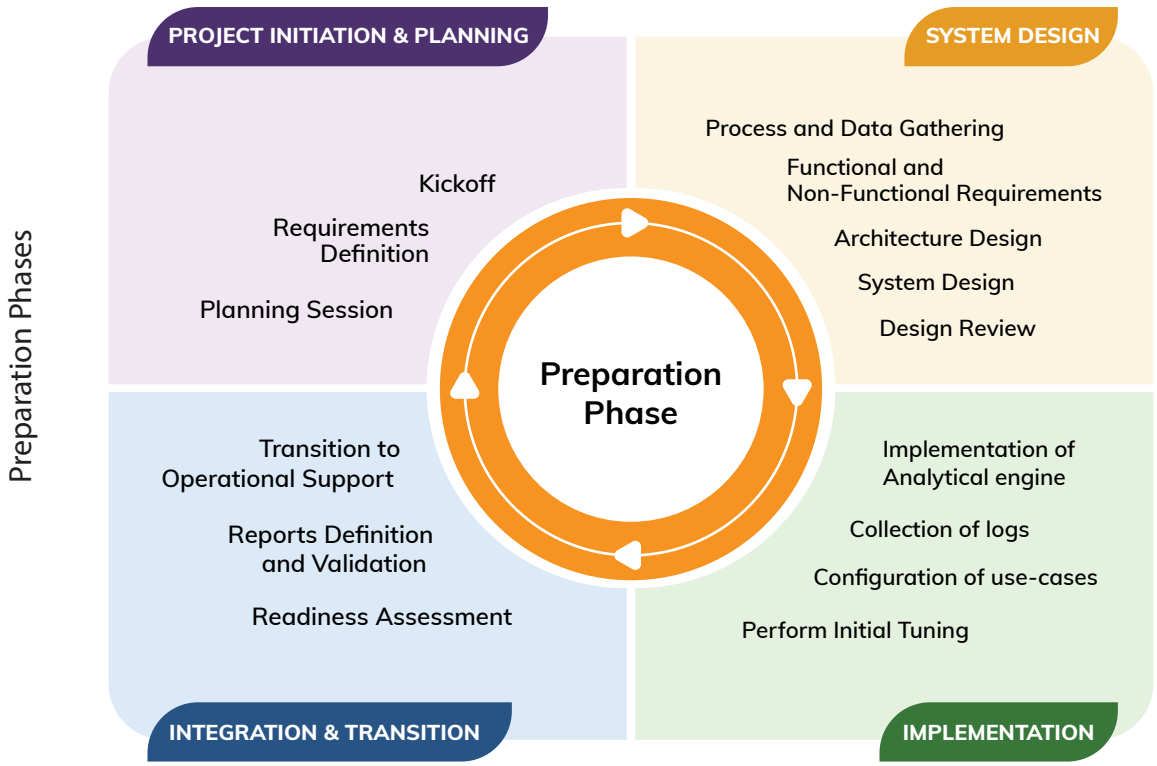
Datasheet

24X7 SECURITY OPERATION CENTER

Our expert SOC team provides a swift response and a decisive resolution to combat security issues as they arise. SOC is the heart of continuous threat monitoring and analysis, mitigation and prevention of cyber-attacks.

We have developed a structured process for our clients to experience uninterrupted business operations and maintain customer trust. The steady-state operations of our team will begin after the preparation phase



Project Initiation and Planning:

ActiveBytes team will define and compile requirements and develop a project plan.

System Design:

ActiveBytes team will work to design the elements for the monitoring system which will include data source integrations based on your stated requirements and deployed security technologies.

Implementation:

Our team will install and configure the monitoring System in the production environment and assist with the transition to managed operations as documented in the Project Plan.

Integration and Transition:

Our team will develop processes and corresponding documentation and begin transitioning management and monitoring to the operational support team. This phase also includes the MSS onboarding and activation.

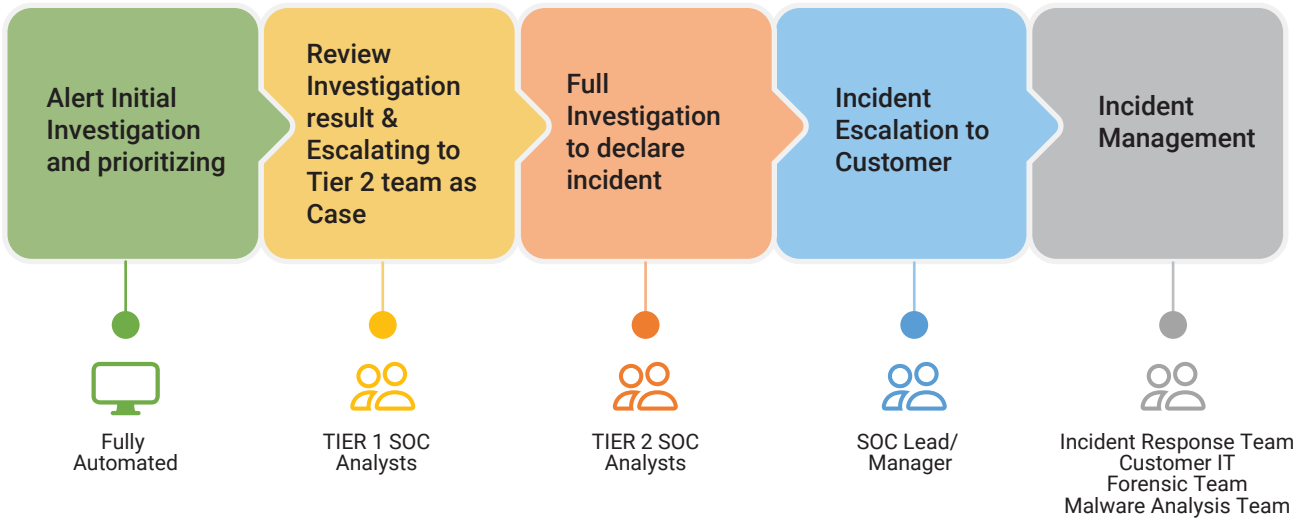
Key Features of our 24/7 SOC Managed Service

- Incident Reporting
- Advanced detection & rapid response
- Threat Intelligence feeds
- Threat Hunting
- Penetration testing & vulnerability management

We follow multiple structured steps in Investigation and incident response procedure as part of our day-to-day monitoring.

- Detect Incidents
- Confirm & Prioritize risks
- Contain Incidents
- Forensics
- Threat Model Change
- Remediate
- Hardening Systems
- Divert Attackers

ActiveBytes has multiple levels of teams performing one specific or different task



Fully Automated

The Alerts and initial prioritization will be an automated process. The output of this stage will be handled by the Tier 1 team

TIER – 1

Our Tier 1 team is dedicated to perform duties like deliver first line analysis of information and pass it to designated escalation points, attend emails/phone calls related to security incidents, monitor events, analyze intrusion, investigate and document security incidents, review the alerts, identify it or escalate it to TIER – 2 depending on the results, assign severity etc. and more.

TIER – 2

Our Tier 2 team will be responsible for duties like in-depth analysis of security events, review escalated cases, analyze network, application and system log events, coordinate the post incident's actions, ensure appropriate analysis of events from intruder detection systems and malware detection, to identify malicious activity, log management to evaluate the impact of security incidents, prepare and deliver Security, Risk and compliance reporting .The team will maintain SOC documentation as well as communicate and interact directly with other staff to ensure individual and group performance. We also leverage Cyber Threat Intelligence (CTI) to accurately define and execute response actions.

SOC Manager

Our SOC manager shall ensure the development of policies, procedures & documentation, manage the scope, schedule, resource allocation to ensure successful project execution, oversee the daily operations of the 24x7x365 SOC, support Security Analysts and cyber operations to respond to, analyze, and manage the cyber incidents affecting the client information and information systems in accordance with the client Incident Response Plan (IRP) and also ensure the service quality is met as per SLA.

Benefits

- Fill gaps in skill shortage
- Right integration of tools
- Increase in enterprise-wide visibility
- Never miss investigation on a security alert
- Contextualize observations
- Intelligent prediction
- Rapid incident response
- Recovery & Steady operation

Contact us

contact@active-bytes.com +971 50 513 3973

www.active-bytes.com