Datasheet

24x7 Security Operation Center

Active Monitoring

We at ActiveBytes, follow a 7-step Investigation and incident response procedure as part of our day-to-day monitoring.

1 **Identify cyber security event**

2 **Define investigation objectives**

- Conducting triage
- Performing initial analysis
- Using cyber threat intelligence
- Carrying out first response

3 **Identify cyber security event**

- Containing the cyber security incident
- Eradicating the cause of the incident
- Gathering and preserving evidence

4 **Recover systems, data and connectivity**

5 **Report incident to relevant stakeholders**

6 **Carry out a post incident review**

7 **Communicate and build on lessons learned**

As part of an investigation of an Alarm triggered, a Security analyst will start with step 1 - 'Identify cyber security event' and declare the event as the case when it qualifies to investigate further and continue to step 2. 'Define investigation objectives'. The case is further investigated for its exposure to the environment and impact on business and found to be applicable then the case is converted as an incident otherwise the case is closed with investigation results based on the outcome of Step step 2.

This Alert to Case, then to Incident classifying approach helps organizations to clearly understand the real Incidents and act on them with priority.

The People

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

Fully Automated

Tier 1 SOC analysts

Tier 2 SOC analysts

SOC Leader/Manager, Incident response team, customer IT team, Forensic team etc.

TIER – 1 team

- Responsible for delivering first-line analysis of information and passing it to designated escalation points
- Attend emails and phone calls related to security incidents from clients or users
- Monitor the security management consoles, analyze intrusion, and vulnerability management, and investigate and document security incidents
- Review the alerts received in the SIEM console/dashboards, does initial triage and converts this to a security incident ticket based on the initial investigation results and alarm threshold settings
- Identifies the alert to be a false positive or escalates it to TIER – 2 depending on the initial triage results
- Assign the severity to each incident based on type and parameters as defined in the organization's Security Incident Management Procedure
- The process of escalation will be as per corporate/MSSP SOC escalation policy requirements
- Proactively identify major or common attacks, oversee the ongoing maintenance of security tools
- Develop policies & procedures as per the suggestions of the executive team

TIER – 2 team

- Responsible for in-depth analysis of security events and review of escalated cases until closure including investigating and recommending appropriate corrective actions for data security incidents
- Analyze network, application and system log events in order to provide advice and guidance to the SOC team
- Responsible for coordinating the post-incident's actions with the constituency.
- Ensure appropriate analysis of events across multiple services including intruder detection systems, and malware detection, to identify malicious activity, log management and vulnerability management, evaluate the impact of security incidents, and prepare and deliver Security, Risk and compliance reporting
- For relevancy check, the Tier-2 team trusts the application/system criticality data, the data available from vulnerability management solutions, adversary information provided by commercial/open-source threat intelligence providers, Information provided by the partners/manufacturers of the product, history of similar kinds of threats that have happened in the past and other documented data like the response time in Service Level Agreement (SLA) are considered for the process of escalation.
- Maintain SOC documentation as well as communicate and interact directly with other staff to ensure individual and group performance

- Incidents may be associated with hundreds to thousands of security events.
- It may take a few hours to even weeks for them to do the deep analysis. There may be multiple levels of teams above Tier-2, the incidents will be escalated to them in order if the situation demands.
- Recovery from an incident usually demands the participation of internal and external experts. Forensic analysis or malware analysis may be performed based on the nature and behaviour of the threat.
- Proper consumption of Cyber Threat Intelligence (CTI) equips the SOC team to accurately define and execute response actions.

SOC Manager – Design and Operations

- Ensure the development of policies, procedures & documentation as per the agreements with the customer along with SLAs
- Establish, document, and manage the scope, schedule, and resource allocation for projects and sustaining activities to ensure successful project execution
- Implement and maintain integrated work schedules and plans which ensure that the necessary deliverables are ready & available
- Oversee the daily operations of the 24x7x365 Security Operations Centre
- Develop & maintain SOC documentations
- Produce relevant cyber security metrics that allow the SOC to provide customers with metrics
- Support Security Analysts monitoring the network and answering phone calls and emails,
- Support 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)
- Ensure the service quality is met as per SLA.

(For details on Service Level Agreement, please contact us)

For Quote Contact us @

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

🌐 www.active-bytes.com