* **Prepared by Sowmya**

**AE-Control Based Questionnaire:**

1. Is the Security Content Automation Protocol (SCAP) vulnerability compliant detecting tool implemented in the organization?   
    *SCAP comprises of numerous open security standards and it uses those standards to detect organization’s system for vulnerabilities and configuration issues.*

If NO- Then the Organization’s cyber security maturity and capability level will be calculated as per our standard maturity calculation formula.

If YES:

1.1 Are the hardware devices are recently scanned by SCAP to detect the potential vulnerabilities, an authenticated connection to the system and verify all security configuration and alerts are created when unauthorized events occur?

1. Does the organization have Automated Monitoring Tool to detect the unauthorized access to sensitive information?

*Automated Monitoring Tool will help the organization in conducting deeper analysis and implementing proactive security measures than spending time in monitoring manually to detect vulnerabilities.*

If NO- Then the Organization’s cyber security maturity and capability level will be calculated as per our standard maturity calculation formula.

If YES:

2.1 has the network boundaries are configured under this tool to detect unauthorized encryption use and unusual traffics?

1. Is Active Discovery Tool has been implemented to identify all transmissions done on the secured information?

*Active Discovery (Asset Discovery) tool is to detect the unlicensed software through which malwares can easily enter the network and it monitors continuously to eliminate most of the BYOD threats.*

If NO- Then the Organization’s cyber security maturity and capability level will be calculated as per our standard maturity calculation formula.

If YES:

3.1 has the sensitive information activities performed by local on-site or remote service provider is updated on the inventory list of this tool?

1. Is File Integrity Monitoring (Log Management System) or SIEM (Security Information and Event Monitoring) has been configured?

*SIEM used to detect security events and create log entries to identify signs of malicious activities across the whole network environment and it determines the nature of attack for a series of events with its success rate.*

If NO- Then the Organization’s cyber security maturity and capability level will be calculated as per our standard maturity calculation formula.

If YES:

4.1 Is detailed auto logging is performed on a regular basis whenever the sensitive data is been modified or accessed by the employees?

4.2 Is there an alert configured to detect any unauthorized or unsuccessful logins to administrative accounts?

4.3 Is there an alert configured whenever there is a change in elevated privileged group accounts and does all the hardware assets are configured to log entry?

4.4 Is the audit logging is monitoring the deactivated accounts?

4.5 Is there an alert configured when users perform an unusual login behaviour, such as time-of-day, workstation location and duration?

1. Does the Organization use any automated tools to maintain an Inventory for administrative accounts?

*Automated tool is one of the most important detection mechanisms required to maintain an inventory for admin accounts since attackers are always behind admin privileges.*

If NO- Then the Organization’s cyber security maturity and capability level will be calculated as per our standard maturity calculation formula.

If YES:

5.1 Does, the tool inventories all domain and local accounts to ensure that only authorized individuals to have access to the privileged level?

1. Is NetFlow Collection (Network Device Management System) is currently running in the organization?

*Network Management Software is an important tool to maintain the overall health by recording information and communications across the organization’s network.*

If NO- Then the Organization’s cyber security maturity and capability level will be calculated as per our standard maturity calculation formula.

If YES:

6.1 Is NetFlow and logging data collection enabled for all network devices?

* **Prepared by Mridul**

1. *Are the log records being reviewed regularly in order to identify the malicious activities?*

* Log records are critical in tracing the activities of attackers and stopping him/her from performing the attacks. If the log records are not reviewed regularly, the attacker’s footsteps can go undetected inviting further intrusion and potential attacks.

1. *Are all the URL requests from all users irrespective of their locations being logged in order to analyze and identify potential malicious activities?*

* All the URL requests should be logged in order to detect the users within the organization who are browsing to malicious websites being an active attacker or their accounts are unknowingly be used by the attacker for browsing these websites and installing malware.

1. *All the devices should automatically conduct anti malware scan when a removable media is connected. Is this implemented in your company?*

* If removable media such as USB drives, CDs and DVDs is not restricted by the company to be used, then it can be one the easiest way to inject a malware into the system. In order to detect the malware in such devices, a thorough scan should be done by the computer as soon as they are connected to the computer.

1. *There should be a centralized logging server setup which receives the event logs from all the logging enabled technologies and services implemented on the network. Do you have it setup?*

* Collecting and analysing the logs from all the devices in the network is efficient. One of the reasons is: Centralized logs allow the analysts to do log research outside the production environment. Searching through log files using tools like “grep” should not steal disk IOPs from your application servers. It’s better to do the searching in a centralized location.

1. *The configuration of the network devices should match with the approved configuration and the network devices should only perform security approved functions. An alert should be created if any changes are discovered. Is this being implemented?*

* This system in place will help in detecting the network devices which are performing disapproved functions. This can happen if a network device has been incorrectly configured or has been affected by a malware, thus, might be in control of an attacker. Generation of an alert is an alarm requiring further investigation.

1. *The query logging for DNS (Domain Name System) should be enabled in order to detect the hostname lookups related to known domains which are identified as malicious. Has this been implemented for you company?*

* By enabling query logging for DNS, you can help your company in detecting the websites related to the websites which were identified as malicious in the past. You can add these websites to blacklist and restrict users to browse to these websites protecting their accounts being affected.

1. *Regular scan for detecting the unauthorized connections across trusted network boundaries should be performed. Has this been implemented?*

* If an attacker somehow obtains access to the admin system, he will have the admin privileges over infrastructure. The main purpose of the application is monitoring the internet protocol traffic between local area network and Internet. In addition, this system aimed to detect unauthorized Internet Protocol addresses that are inside the network range.

1. *A monitoring system should be established at each network boundary to monitor and record the information packets passing through. Is this implemented?*

* Monitoring tools like SolarWinds Network Performance Monitor is a powerful tool which can be used for extensive monitoring of all the devices deployed on your network including the firewalls, etc. This monitoring will help you detect the intentional or unintentional transfer of critical information packets through the network boundary.

1. *The network-based IDS sensors should be deployed at each network boundary to detect the malicious activities and the system at these boundaries that have been compromised. Has this been implemented?*

* Network- based IDS like SNORT is a very powerful toolkit available for free which can be used for detecting the malicious activities. You can also customise it by setting up specific rules according to your network. Detection of an intrusion and the malware effected devices is critical to stop the potential network intrusions and cyber-attacks in future.

1. *At the boundary proxies, all network traffic that is encrypted should be decrypted before analysis. Has this been implemented?*

* Decrypt all encrypted network traffic at the boundary proxy prior to analyse the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.

1. *Unauthorized use of encryption should not take place in outbound data transfer. Is there any system established to monitor this and alert the analysts whenever detected?*

* Ex: An attacker has encrypted critical user data using unapproved encryption technique and trying to send it from the computer inside the company to his computer. This system will fail to decrypt the data, generating an alert, requiring investigation. This system not in place will allow him to easily transfer the data affecting the CIA of critical information.
* **Prepared by Ali**

**Organizational Assests Protection, Detection Process and Procedures of anomalous events?**

**Q1: Are the hardware devices and systems of organization is properly configured/ updated with anti-malware scan?**

Yes or no?

* All the assets used by organizational network, must be pre-registered or authorised to give access, and unmanaged and unauthorised devices must be found and prevented from gaining access. If the organization is not configured with procedures and updated software's, the common nonphysical threats will be found such as keylogger, DoS, DDoS, virus, Trojans, worms etc.

**Q2: what are the physical threats to organization? If there is lack of continuously monitoring of Assests?**

Yes or No

* Physical threats in organization can fall in three categories: internal, external and human, Internal**:** Fire threats could be prevented using automatic fire detectors and extinguishers that do not use water to put out a fire. The unstable power supply can be prevented using voltage controllers. An air conditioner can be used to control the humidity in the computer room. External: Lightning protection systems can be used to protect computer systems against such attacks, Humans: Threats such as theft can be prevented by use of locked doors and restricted access to computer rooms. Physical threats cause damage to computer systems hardware and infrastructure. Examples include theft, vandalism through to natural disasters.

**Q3: Does all the devices are regularly scanned by a port scanner to alert? if unauthorized ports are detected on a system?**

Yes & No?

* Port scanners regularly are very important for organizations network security and we can find the vulnerabilities on systems and can find which port are open/loose door from where hacker can enter. These techniques attackers use to discover services that they can exploit to break into targeted systems. Hackers use port scanners to conduct tests for open ports on Personal Computers/organization systems that are connected to the web.

**Q4: Does all devices are enabled with command-line audit logging for command shells, such as Python or Windows PowerShell with enhanced logging enabled?**

Yes or No?

* Auditing Windows event logs is necessary to protect your organization from potential security threats, it is a herculean task. EventLog Analyzer, an event log management and reporting tool, makes it easy for you.

**Q5: Do the network devices utilize at least three synchronized time sources to retrieve time information on a regular basis so that timestamps in logs are consistent?**

* Logs are the lifeblood of security: attacker may create a ton of noise on an endpoint while leaving little trace on the network or vice-versa. ACTIVATE AUDIT LOGGINGENABLE DETAILED LOGGING, CENTRAL LOG MANAGEMENT, DEPLOY SIEM OR LOG ANALYTIC TOOLS, REGULARLY REVIEW LOGS

Yes or no??

**Q6: How Security Threat detection and discover hidden information from log messages with SIEM?**

* The main function is to store, collect, search and correlate system generated log messages, which are generated by machines in human readable form in order to support, maintenance trouble shooting, monitoring or audit activities, with three main functions as: Aggregation of dispersed log messages in one central location to easy access, Persistent storage of large amount of log data for a specified period of time and Correlation of logs for threats or anomaly detection.

Yes or No?

**Q7: is the organizational Event detection information is communicated?**

Yes or No?

* identify assets that are most important to your organization – this could be sensitive data, servers, apps, networks—anything that could potentially put you out of business if it were compromised or forced offline. talk to the executive leadership team about the current security posture of the company, highlighting any key areas of concern and anomalies that could signal a potential incident.The severity of an attack is therefore determined by how well a company can mobilize and respond to the threats they detect.

**Q8: Ensure that appropriate logs are being aggregated to a central log management system for analysis and review?**

Yes or No?

* Ensure that local logging has been enabled on all systems and networking devices. Ensure that appropriate logs are being aggregated to a central log management system for analysis and review. security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers.

**Q9: organizational Public or Private IP’s Asset Protection?**

* Setting restrictions on how your IP can be used , Establishing guidelines when partnering with a third-party Creating technological and physical security protocol

Yes or No?

**Q10: Do the network devices utilize at least three synchronized time sources to retrieve time information on a regular basis so that timestamps in logs are consistent?**

Yes or No?

* Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

**Q11: Is the Detection processes are tested? /Cyber security assessment updated?**

**Yes or No?**

* Detection Process are the key component in a comprehensive cybersecurity plan. After the vulnerabilities in a security system have been identified and pinpointed, the security assessment uses that information to actively discover possible ways in which a cybercriminal could gain access. Then, by analyzing the nature and severity of the vulnerabilities and determining the risk factors they carry, it is possible for an organization to create a protocol that mitigates the potential of an attack.