Responsibilities

Logs

- Onboard logs of all infrastructure tools, security devices, sourcecode repository and applications
- Define event correlation rules related to network threats and vulnerabilities, ensure all events related to networks are monitored.
- Monitor for mis-use, threats, compromises relevant to operations/threats/services
- Monitoring of Shadow IT (via Network access/Helpdesk)
- User Behavior analysis on ELK Stack (incl network traffic, data exfiltration, AV and identity) inline with threat risk assessment
- Monitor IOCs via ELK Stack.
- End to End Security Monitoring (incl End points, Datacentre, Network and Cloud IaaS/PaaS/SaaS workloads).

Vulnerability Assessment

- Conduct Vulnerability scans on full stack (application, database, web-server, Operating system, firmware) for Datacentre/ Cloud hosted services and ancillary equipment (incl Printers)
- Must be proficient in identifying vulnerabilities and security loop holes in the existing implementation
- Establish processes to receive, analyze and respond to vulnerabilities from internal/external sources.
- Prioritization of remediation actions based on threat level and environment/asset rating
- Subscribe to public and vendor/proprietary security advisories
- Log and track vulnerabilities. Analyze vulnerabilities to determine applicability and evaluate severity.
- Review of all security patches issued by vendors for infrastructure and services. Monitor security patching and deployment for all hardware and software.
- Produce reporting on the presence of these vulnerabilities and any actual exploitation or attempts made.

Threat Intel

- Subscribe to threat intel (OSINT, CERT-IN and proprietary) and vulnerability advisories for assets/services in use
- Integrate the feeds with ELK Stack

Incident Response

- Triage and conduct security incidents with help of application/infra administrators.
- Perform analysis & remediation activities

Access Review

- Conduct periodic access reviews of application (on premise or cloud) and infrastructure devices
- Access Management Operations Processes such as Joiner/Leavers/Transfers. Ensure Access Appropriate to Role Review for each employee once in 365 days.
- Responsible for managing access to applications and infrastructure, and importantly ensuring access is provisioned appropriately, according to role per time period.

Compliance

- Implement mitigating controls and assess operating effectiveness of the controls
- Monitor for deviation from approved technical standards/benchmarks/configuration
- Define/Manage exception approval process for deviation from polices/standards