

ROADMAP

CYBER SECURITY 2024/25

Endpoint Security

Automate benchmark assessment against CIS-CAT 3.0 and NIST 2.0 Framework.

Reduce the exposure score to low.

Office 365 / MS

Evaluate and Implement relevant new options available to securing Microsoft Services.

Remote Access

Evaluate and implement a Zero Trust Network Access Solution.

Cloud Infrastructure

Automate configuration assessment and audit.

Improve network and application-level segmentation to go with Zero-Trust Network Architecture.

Design and implement a layered defence approach.

Create infrastructure for adversary emulation within AWS.

User Training

Implement infrastructure for Phishing Simulations.

Conduct Regular Workshops and Training Sessions for end users.

Security Operation Center

Upgrade the SIEM.

Create a central repository of scripts and tools for analysis and mitigations.

Set-up a sandboxed environment for Malware Analysis and Triage.

Create more playbooks to cover top 10 incident response scenarios.

Insider Threat Management

Implement a privileged Access Management System.

Improve DLP Capabilities.

Implement and automate access reviews.

BWF Server

Migrate all sites hosted on BWF Servers to AWS by 2024.

Securing Supply Chain

Improve and implement tooling for automated code review and AppRisk Management.

Implement a Vulnerability Management System to keep track of vulnerabilities and their mitigations.

Adopt the OWASP SAMM 2.0 model by 2024.

Research & Development

Develop Tooling and other resources to study and develop mitigations for latest threats.