Human, Organizational, & Regulatory Aspects

	Managed	Defined	Predictable	Optimizing
1	All organizations should follow Cyber security Authorities regulations and recommendations (or vendors)	Have a qualified team (invest in security teams)	Build use cases/ scenarios in the SOC to identify zero-day vulnerabilities.	Have adequate CyberSecurity detection, mitigation, prevention, & recovery strategy for every business
2	Apply policies & standards for ex; NCA policy, OPT standards, ISO standards etc.	Train employees/ decesion makers on healthy cyber practices.	PURPLE team (red & blue) collaboration to discover vulnerabilities before attackers.	Have Research & development team (RND) to research vulnerabilities.
3	Enforce software/ Internet use policies.	Have a solid SOC center to detect & have 360° view of organization work.	Increase awareness/ educate users	Zero Day Initiative (bounty programs).
4	Apply human security hygenie concept.			Stay informed: Zero-day exploits aren't always publicized.
5	Understand & adhere to data privacy & compliance regulations (GDPR, PCI DSS, HIPAA, etc.)			Organizations should use threat sharing resources & vulnerability disclosures to stay aware.

By. Eman Bakri

Attacks and Defences

	Managed	Defined	Predictable	Optimizing
1	Monitoring applications /Solution.	Detect by looking for suspicious behavior.	Have an Incident Response Plan Ready.	Practice/ apply defense in depth.
2	Input Validation	Vulnerability Scanning	Patch Management	Zero trust security model.
3	Use encryption methods.	Covering each stage in attacks lifecycle (Cyber Kill Chain).	Invest in security control tools like DLP, Sandboxing Solutions, etc.	Use MITRE framework.
4		Use initial or temporary solutions to limit the impact.	Work out an emergency response solution.	Apply Threat intelligence.
5		Do not leave default configurations of security tools as it is.		

By. Eman Bakri

Systems Security

	Managed	Defined	Predictable	Optimizing
1	Remain in control of your data.	Enforce the least privilege model.	Resources availability have a direct role in ability to defend.	Apply an objective, passive & proactive approach.
2	Apply system security hygenie concept.	Be sure to back up: for data & datacenter.	Care of internal systems/servers & external servers/systems facing the Internet.	Apply the SASE architecture.
3	Do not share passwords & keys between systems.	Systems baselining & hardening (Detection).		
4				
5				

By. Eman Bakri

Software and Platform Security

	Managed	Defined	Predictable	Optimizing
1	Use only essential applications.	Use a firewall/ Web Application Firewall (WAF)	Use a comprehensive/ Next Generation antivirus software solution.	Application Whitelisting
2	keep updated.	Deploy an IDS or IPS (on software level).	Safe/secure administration of systems.	Deploy AI-based threat detection tools.
3	Assume you're compromised, & that you will get compromised again.	Use runtime application self-protection (RASP) agents	Follow the logs & traffic on firewalls.	Better Patches Could Reduce the Number of Zero-days.
4	Secure code.	Browser isolation	Use "heuristics-based" antivirus detection software	
5		Monitoring applications created automatically		

By. Eman Bakri

Infrastructure Security

	Managed	Defined	Predictable	Optimizing
1	Minimize number of devices facing the Internet.	Deploy an IDS or IPS on network level.	Adopt a multi-layered approach as your security posture.	Single packet authorization.
2	Use virtual local area networks (Virtual LAN)	Implement Network Access Control	Reduce your Attack Surface	Monitoring for persistence techniques.
3	Use secure ports for your network.	Implement IPsec, the IP security protocol.	Perform network scanning.	Monitoring for suspicious communication.
4	Check for unknown connection to foreign network.	Encryption of network traffic	Network segmentation, in form of VLANs.	
5	Comprehensive real-time Network Analysis & Visibility (NAV)	QoS, distribute the requests on multiple zones etc.	Have an inventory list of the entire organization infrastructure	

By. Eman Bakri