Layered Cyberdefense controls
By Ubong Etim

This assignment researches appropriate cyberdefense controls for three types of organizations or Implementation Groups (IGs) based on the CIS security controls recommendations.

S/N	Organization	CIS control	Proposed tool	Features	OEM(Vendor)
1	FinTech, Telehealth, (ISP)	Inventory and access control (Hardware assets)	Server & Application monitor (SAM)	- Packet inspection - Network device scanning - Network device monitoring	Solar WInds
2	FinTech, ISP, Telehealth	Inventory and access control (Software assets)	IT service management	- Service management - Asset management and configuration management database	Solar Winds
3	Telehealth, (ISP), Fintech	Data protection	Data security Fabric (DSF)	- Data retention and archive - Data Risk analytics - Data encryption and tokenization	Imperva
4	FinTech, ISP, Telehealth	Secure configuration of assets and software	Distributed Version control system (VCS)	- Version control - Distributed architecture - Centralisation (branching & merging)	Git
5	FinTech,ISP, Telehealth	Account management	Google cloud Identity access Management (IAM)	- Permissions and roles - Access control - Privileged Access management	Google cloud
6	ISP, Telehealth, Fintech	Access Control Management	Google cloud Identity access Management (IAM)	- Credential management - Session management - Discovery	Google cloud

7	FinTech, ISP, Telehealth	Continuous Vulnerability Management	InsightVM	- Incident response - On Premises and cloud based asset scanning - Patch management integration	rapid7
8	ISP, Telehealth	SIEM (security Information and Event Management)	Falcon (next-gen SIEM)	- Centralized visibility - Advanced threat detection (AI and ML) - UEBA (User and Entity behaviour Analytics)	Cloudstrike
9	ISP, Telehealth	Email and Browser Protection	Darktrace/Email (previously Antigena Email)	- Phishing protection - ICES (Integrated Cloud Email Security) - MFA (Multi Factor Authentication	Darktrace
10	ISP, Telehealth	Malware Defense	McAfee Total Protection	- VPN - Antivirus - File shredder	McAfee
11	ISP, Telehealth, FinTech	Data Recovery	McAfee Total Protection	- Personal data cleanup - Identity restoration	McAfee
12	ISP, Telehealth	Network Infrastructure Management	Op Manager	- Network provisioning - Network performance Management - Network configuration management	Manage Engine
13	ISP, Telehealth	Network monitoring & Defense	Op Manager	- Network provisioning - Network performance Management - Network configuration	Manage Engine

				management	
14	Telehealth, FinTech, (ISP)	Security awareness & training	Guardey	- Gamified learning - Progress monitoring and leaderboards - Multi language support	Guardey
15	ISP, Telehealth	Third-party risk	Third-Party Management (OneTrust)	- Service management - Asset management and configuration management database	OneTrust
16	ISP, Telehealth	Application Security Posture Management (ASPM)	APPSec	- API security testing - Risk visibility and remediation - Automated risk assessment	Apiiro
17	ISP, Telehealth, FinTech	InsightIDR	Insight VM	- Incident response - On Premises and cloud based asset scanning - Patch management integration	rapid7
18	ISP, Telehealth	Penetration testing	Burp Suite pro	- Automated vulnerability scanning - Attack surface mapping - Loggin, interception and manipulation of websocket traffic	Burp suite