Cyber Security
MVA New Model

	Identify	Protect	Detect	Respond	Predict
Function / **Layer**	Asset Inventory, Vulnerability Assessment, measuring attack surface, assess risk profiling.	limiting attack surface such as patching, containment, isolating, hardening, managing access, and remediation	Discover and detect events, triggering alerts on anomalies, detect, and perform security analytics	Acting on detected events, remove intrusion footholds, assess current damage, and, reconstruct evidences for forensic investigations	Anticipate threats and attacks before it is taking place. Gather & correlate intelligence from different sources
Devices — Laptops, Desktops, servers, VoIP phones, tablets, IoT, storage, network devices, etc.	GFI Software, IBM Security, nuix, ALIEN VAULT	Symantec, KASPERSKY, McAfee, TREND MICRO, CISCO, nuix, GFI Software	Symantec, KASPERSKY, FireEye, McAfee, nuix, TREND MICRO	Symantec, KASPERSKY, TREND MICRO, McAfee, IBM Security, nuix, FireEye	ALIEN VAULT, Symantec, McAfee, FireEye, TREND MICRO, CISCO, Hewlett Packard Enterprise, IBM Security, KASPERSKY
Applications — The software and application installed and/or running on the devices	nuix, ALIEN VAULT	Symantec, McAfee, IBM Security, CISCO, Hewlett Packard Enterprise, A10, GFI Software	Symantec, CISCO, A10, Hewlett Packard Enterprise, McAfee, FireEye, ALIEN VAULT, IBM Security	Symantec, A10, FireEye	
Networks — The connections and network traffic between devices and applications	CISCO, GFI Software, ALIEN VAULT	Symantec, McAfee, CISCO, A10, IBM Security, TREND MICRO	Symantec, KASPERSKY, ALIEN VAULT, FireEye, A10, Hewlett Packard Enterprise, McAfee, CISCO	FireEye, A10, McAfee, Hewlett Packard Enterprise	
Data — The data stored, processed, and/or transmitted by devices, applications and network	Symantec, nuix, FireEye, IBM Security, McAfee	Symantec, McAfee, GFI Software, IBM Security, Hewlett Packard Enterprise	Symantec, McAfee, Hewlett Packard Enterprise, GFI Software, FireEye, IBM Security	nuix, FireEye	
Users — Individuals using the devices, applications, networks, and data	PHISHME, IBM Security, CISCO	PHISHME	nuix, KASPERSKY, PHISHME	nuix	

		Identify	Protect	Detect	Respond	Predict
	Function / **Layer**	Asset Inventory, Vulnerability Assessment, measuring attack surface, assess risk profiling.	limiting attack surface such as patching, containment, isolating, hardening, managing access, and remediation	Discover and detect events, triggering alerts on anomalies, detect, and perform security analytics	Acting on detected events, remove intrusion footholds, assess current damage, and, reconstruct evidences for forensic investigations	Anticipate threats and attacks before it is taking place. Gather & correlate intelligence from different sources
Devices	Laptops, Desktops, servers, VoIP phones, tablets, IoT, storage, network devices, etc.	**Configuration Mgmt.** **System Mgmt.** **MDM** **Vulnerability Mgmt.**	**Identity & Access Mgmt.** **AV** **HIPS** **Virtual Patching** **Malware protection**	**Sandboxing** **Static Analysis** **pot**	**Device Isolation** **Central Security Mgmt.**	**Threat Intelligence**
Applications	The software and application installed and/or running on the devices	**Configuration Mgmt.** **System Mgmt.** **VM** **Certificate Mgmt.**	**Source Code Analysis** **WAF** **IAM** **Whitelisting** **IAM** **Authentication**	**Web Malware Detection** **Load Balancing** **SSLI** **DDOS Detection**	**Central Security Mgmt.**	
Networks	The connections and network traffic between devices and applications	**Configuration Mgmt.** **System Mgmt.** **NetFlow** **Vulnerability Mgmt.**	**NFW** **IPS** **Proxy** **DNS Security** **IAM** **Authentication**	**Sandboxing** **SIEM** **IDS** **DDOS Detection** **BotNet**	**SIEM** **DDOS Alert & Protection** **Security Mgmt.**	
Data	The data stored, processed, and/or transmitted by devices, applications and network	**Data Inventory** **Data classification** **Database Security**	**Data Encryption** **MDM** **Data Leakage Protection** **IAM** **Authentication**	**Data Leakage Detection**	**Data Acquisition** **Digital Forensics** **DRM** **Security Mgmt.**	
Users	Individuals using the devices, applications, networks, and data	**IAM** **Authentication** **Password Management**	**Social Engineering Tests** **Phishing Awareness** **IAM** **Authentication**	**User Behavior Analysis** **Insider Threat**	**User Blocking/Isolation** **Security Mgmt.**	