KAAPAGAM
TECHNOLOGIES

CYBER KILL CHAIN

DEFENSE IN DEPTH STRATEGY

CLEMENT ARUL

CEO & EVANGELIST

AWARDS :

CYBER SECURITY PROFESSIONAL OF THE YEAR 2020 – ASIA , CS Excellence Awards

CYBER SECURITY PROFESSIONAL OF THE YEAR 2019 – APAC , CS Excellence Awards

CYBER SECURITY EDUCATOR OF THE YEAR 2019 – APAC , CS Excellence Awards

CYBER SECURITY PROFESSIONAL OF THE YEAR 2017, Cybersecurity Malaysia

CYBER SECURITY INNOVATION OF THE YEAR 2016, Cybersecurity Malaysia

CYBER SECURITY PROFESSIONAL OF THE YEAR 2014, Cybersecurity Malaysia

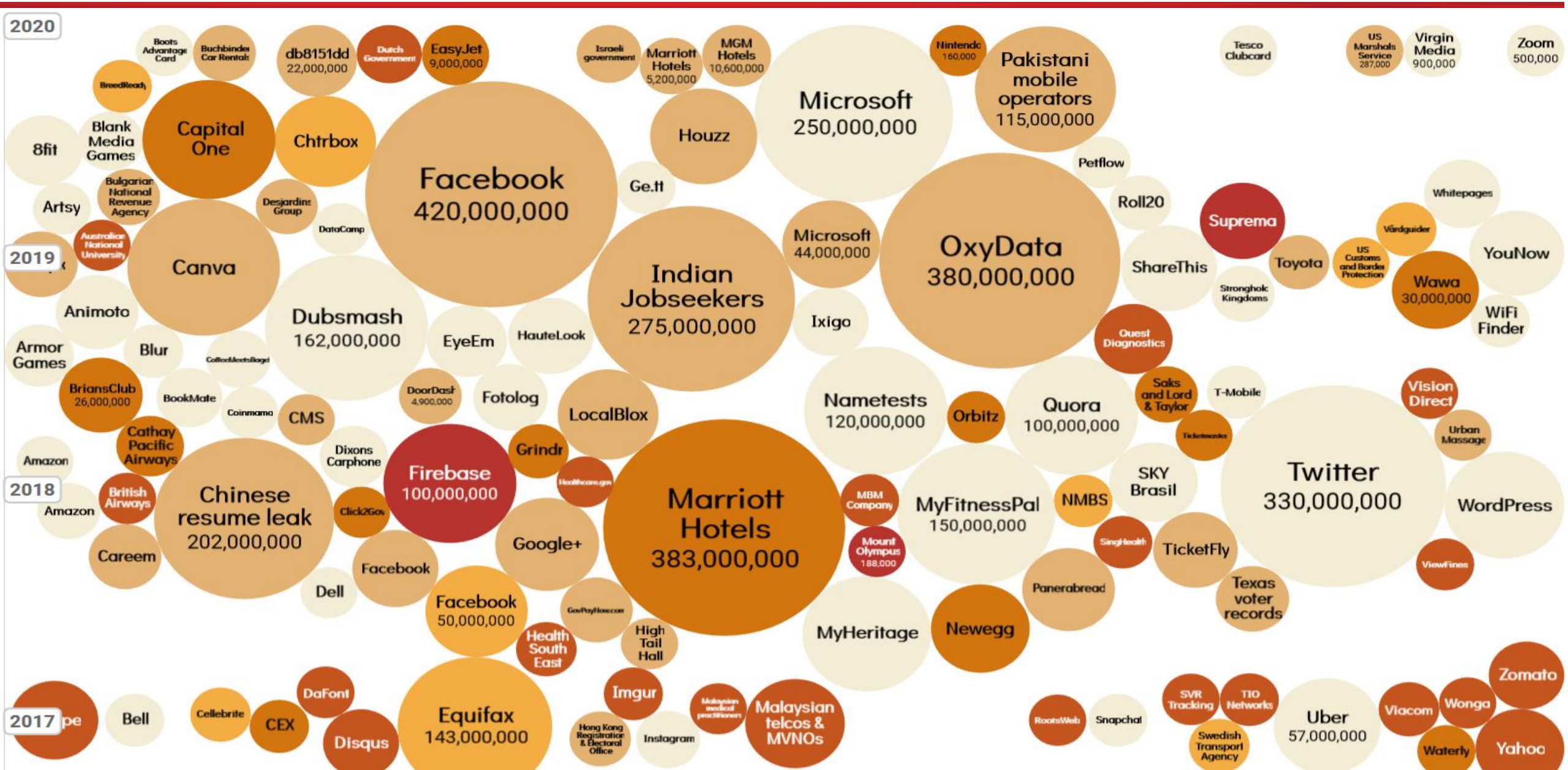
CERTIFICATIONS:

ISO 27001 LEAD AUDITOR, CEH, CHFI, ECSP, ECSA, LPT, CSAD, CES, ECSP.NET

FCiiSCM, CBAP, MCPD, EDRP, CCII, EMC BIG DATA ASSOCIATE, CPT, CWDP

KAAPAGAM TECHNOLOGIES

WORLD'S BIGGEST DATA BREACHES & HACKS



WHAT IS CYBER KILL CHAIN?

- Lockheed Martin derived the kill chain framework from a military model – originally established to identify, prepare to attack, engage, and destroy the target.
- Since its inception, the kill chain has evolved to better anticipate and recognize insider threats, social engineering, advanced ransomware and innovative attacks.
- A series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data.
- Helps understand and combat ransomware, security breaches, and advanced persistent attacks (APTs).

KAAPAGAM TECHNOLOGIES

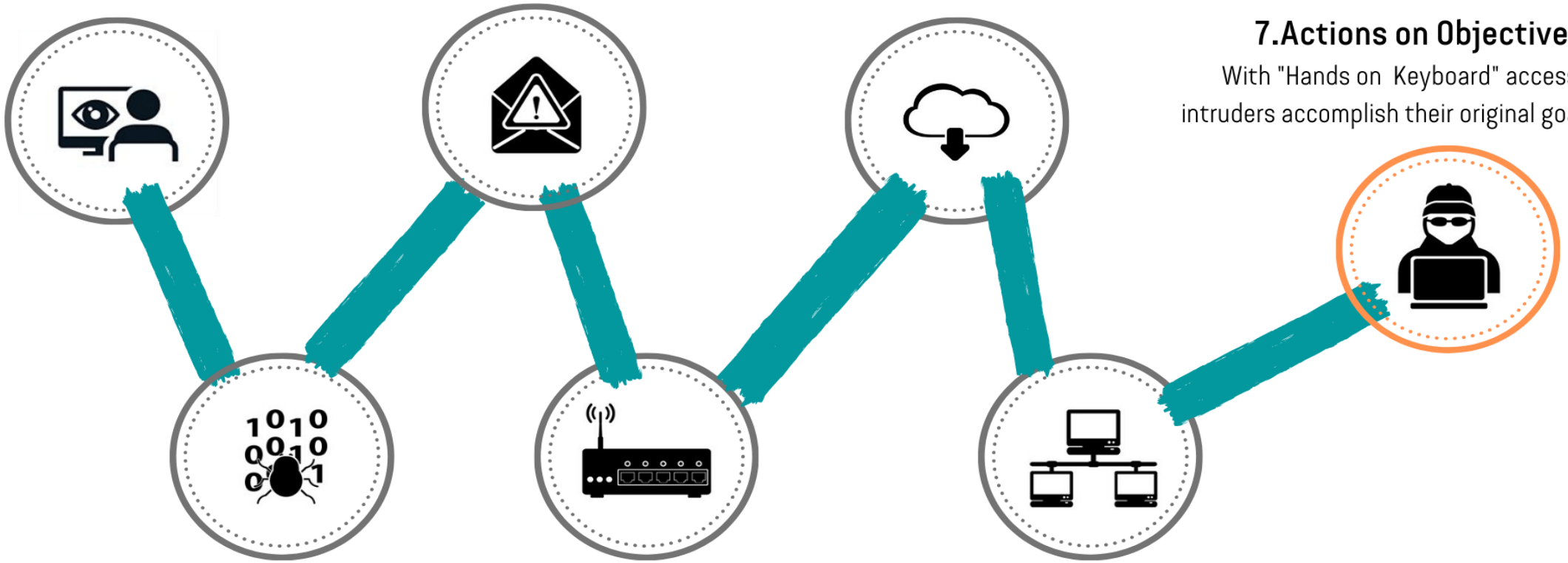
WHAT IS CYBER KILL CHAIN?

1.Reconnaissance
Harvesting email adresses, conference information, etc

3.Delivery
Delivering weaponised bundle to the victim via meail, web, USB, etc

5.Installation
Installing malware on the asset

7.Actions on Objectives
With "Hands on Keyboard" access, intruders accomplish their original goal



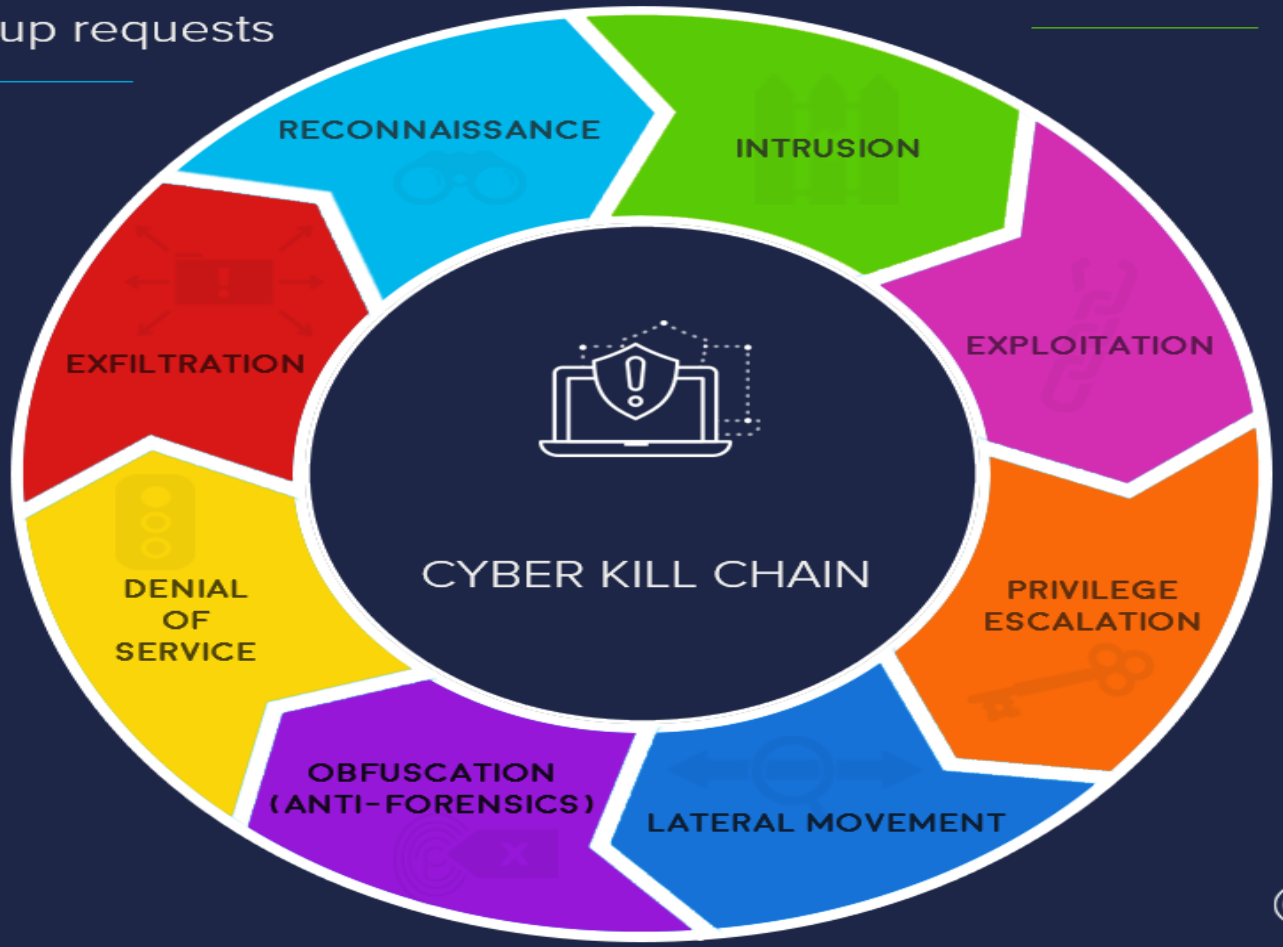
2.Weaponisation
Coupling exploit with backdoor into deliverable payload

4.Exploitation
Exploiting a vulnerability to execute code on a victim's system

6.Command / Control
Command channel for remote manipulation of the victim

KAAPAGAM TECHNOLOGIES

WHAT IS CYBER KILL CHAIN?



Abnormal DNS reverse lookup requests

Brute Force Attack

Unusual amount of data uploaded to external websites

Activity from blacklisted geolocationn

Unusual number of GDPR files deleted

Failed privilege escalation detected

Unusual number of messages marked as unread

A dormant service account was reactivated

KAAPAGAM TECHNOLOGIES

MITRE ATT&CK VS. CYBER KILL CHAIN

MITRE ATT&CK

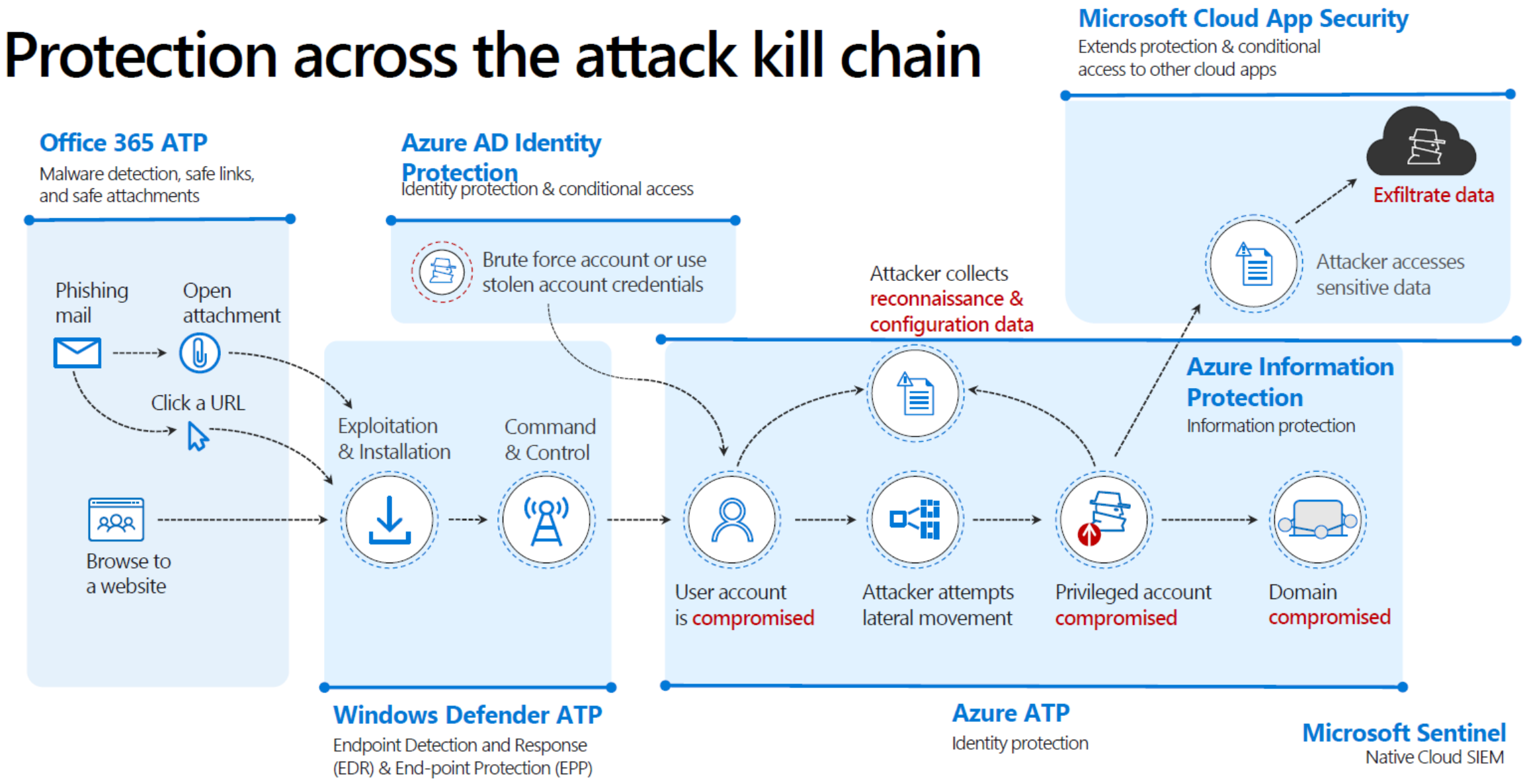
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

Cyber Kill Chain

- Reconnaissance
- Intrusion
- Exploitation
- Privilege Escalation
- Lateral Movement
- Obfuscation/ Anti-forensics
- Denial of Service
- Exfiltration

KAAPAGAM TECHNOLOGIES

MICROSOFT INTEGRATED SOLUTION



DEFENSE IN DEPTH STRATEGY

Cyber Security (Internal)	
Incident Response and Recovery	Configuration Management
IT Asset audit	Patch Management
Vulnerability Management	Security Governance
SIEM & Analytics	Awareness and Training
Penetration Testing / Red Teaming	Security Architecture
eDiscovery / Forensics	Risk Assessments / Compliance
Threat Hunting	Supply Chain Risk Management

Managed CyberSecurity Partner
Managed NAC
Managed SIEM
Managed Firewalls/IDS/IPS/Web Filtering
Managed IPS/IDS
eDiscovery/ Forenscis Retainer
Threat Hunting

Managed Clients
Endpoint Protection (EP)
Endpoint Encryption (EE)
Endpoint DLP
Endpoint DR
Device Authentication
VPN Client

CASB
MDM
NCA
MFA

On Premise	Private Cloud	Public Cloud	SAAS
Extranet/DMZ	**Extranet/DMZ**	**Extranet/DMZ**	**Extranet/DMZ**
Firewall	Firewall	IPS	E-mail Antimalware
IPS	IPS	Cloud DLP	SSO
Web Filtering	WAF	WAF	MFA
Edge DLP			CASB
Antimalware			
SSL Decryption			
WAF			
FIM			
EDR			
Servers	**Servers**	**Servers**	
EP	EP	EP	
DLP	EDR	EDR	
EDR	FIM	FIM	
FIM	DB Encryption	DB Encryption	
DB Encryption		Application Segmenting	
LAN/WAN			
NAC			
ACL			
Wireless ID			
NMS			

NIST Cybersecurity Framework

Identify
Governance
Risk Assessments
Compliance
Configuration Management
Vulnerability Scanning
Penetration Testing
Asset Management

Protect
Firewalls / ACLs
Remote Access (VPN)
Endpoint Protection (EP)
Email Antimalware
Intrusion Prevention (IPS)
Web Filtering
Identity and Access Management (IDAM)
Single Sign-On (SSO)
Multi-Factor Authentication (MFA)
Privileged Access Management (PAM)
IDAM Governance
Network Access Control (NAC)
Mobile Device Management (MDM)
Endpoint Encryption (EE)
Database Audit Monitoring
Device Authentication
Web Application Firewall (WAF)
Database Encryption
Cloud Access Security Broker (CASB)
Application Segmentation
Public Key Infrastructure (PKI)
Key Management
DDoS Protection
Application Whitelisting

Detect
SIEM & Analytics
Intrusion Detection (IDS/IPS)
Vulnerability Scanning
Wireless IDS
Endpoint EDR / HIDS
Endpoint DLP
Edge DLP
Edge Antimalware
SSL Decryption
NMS
File Integrity Monitoring (FIM)
Baselining
Threat Hunting
Threat Intelligence Feeds
Deception/ Honeypots
Code Analysis

Respond
Incident Response and Recovery
Endpoint Detection and Response
eDiscovery / Forensics

Recover
Disaster Recovery Planning
Incident Response and Recovery