Performanta stack

Client Needs and Expected Outcomes

Service Delivery

Account Management

Identify

EASM/CASM

Vuln Prio

Pen testing

Assessments

Consulting Services

DRP/BAS/CPSM

Recover & Prepare

Security Optimisation Manager

IR Retainers / Forensics

Remediate

PERFORMANTA

SAFE XDR

Powered by Safe Platform

Protect

Implementation Services

Managed Controls

Resource Augmentation

Detect & Respond

Detection Engineering

Attack Disruption / Containment

EDR/SIEM/XDR/DLP/IDR/NDR

Managed Phishing

Attack Surface Management

Attack Surface Management	Detect	Defend	Prepare/ Recover

Cloud Posture Management

Cloud Infrastructure Entitlement Management

Vulnerability Prioritisation / Management

CAASM/EASM/CTEM

Penetration Testing

Threat Intelligence

Digital Risk Posture/Brand protection

Security or Control Maturity Assessment

Breach & Attack Simulation

Attack Surface Management (ASM) is the continuous process of discovering, analysing, prioritizing, and mitigating vulnerabilities and potential attack vectors across an organization's digital footprint. It takes an external, attacker's perspective to identify exposed assets—such as servers, applications, cloud services, or shadow IT—that could be exploited.

Detect

| Attack Surface Management | **Detect** | Defend | Prepare/ Recover |

Detect is suite that integrates multiple security layers into a cohesive platform, enabling organizations to detect, respond to, and mitigate cyber threats across their entire digital ecosystem. It is customizable enough to scale from EDR to SIEM or into XDR by combining offerings such as:

- Cloud Environments
- Network Security
- SIEM Integration
- Identity & Access Management
- And many others

Managed Detection & Response (MDR)

Security Operations Center (SOC / SIEM)

Managed Email (Phishing)

Identity Threat Detection & Response (ITDR)

Network Detection & Response

Prepare / Recover

ASM	Detect	Defend

Prepare/Recover

This offering is all about proactive preparation and post-incident recovery, ensuring organizations are ready for cyber incidents and can bounce back quickly when they occur.

- **Incident Management**
- **Digital Forensics**
- **Recovery & Hardening**
- **Incident Response Retainers**
- **Tabletop Simulations**
- **Awareness Campaigns and training**

ASM

Cloud Posture Management

Cloud infrastructure Entitlement Management

Vulnerability Management

Vulnerability Prioritisation

Attack Survance Management

Threat Intelligence

Digital Risk Posture

Breach & Attack Simulation

Penetration Testing

Security Maturity Assessment

Detect

Managed Detection & Response (EDR)

Security Operations Center (SOC / SIEM)

Identity Threat Detection & Response (ITDR)

Managed Email (Phishing)

Network Detection and Response

Protect

Firewalls
FORTINET
algosec
tufin

Endpoints
Microsoft
CROWDSTRIKE

Secure Web Gateway
netskope
FORCEPOINT

Data Loss Prevention (DLP)
Microsoft
FORCEPOINT
netskope

Cloud Access Security Broker (CASB)
Microsoft
FORCEPOINT
netskope

Privileged Access Management (PAM)
Microsoft
CYBERARK

Identity and Access Management (IAM)
Microsoft

Web Application Firewalls (WAF)
CLOUDFLARE

Workload Protection
Microsoft
CROWDSTRIKE

Email
Microsoft
IRONSCALES
SAFER TOGETHER

Vulnerability Scanning
tenable
RAPID7

Managed SIEM
Microsoft

ENCORE
ATTACK SURFACE MANAGEMENT

Recover

Incident Management

S-RM

Cyanre — the digital forensic lab

PERFORMANTA

Incident Forensics

S-RM

Cyanre — the digital forensic lab

Incident Recovery & Hardening

PERFORMANTA

Tabletop Simulations

S-RM

Cyanre — the digital forensic lab

PERFORMANTA