### Threat Monitoring

24/7 monitoring and analytics of security events including triage, incident management, remediation guidance, and tailored security information and event management (SIEM) content development for industry-specific use cases. Security Orchestration, Automation, and Response (SOAR) for clients with mature playbooks.

### Threat Hunting and Response

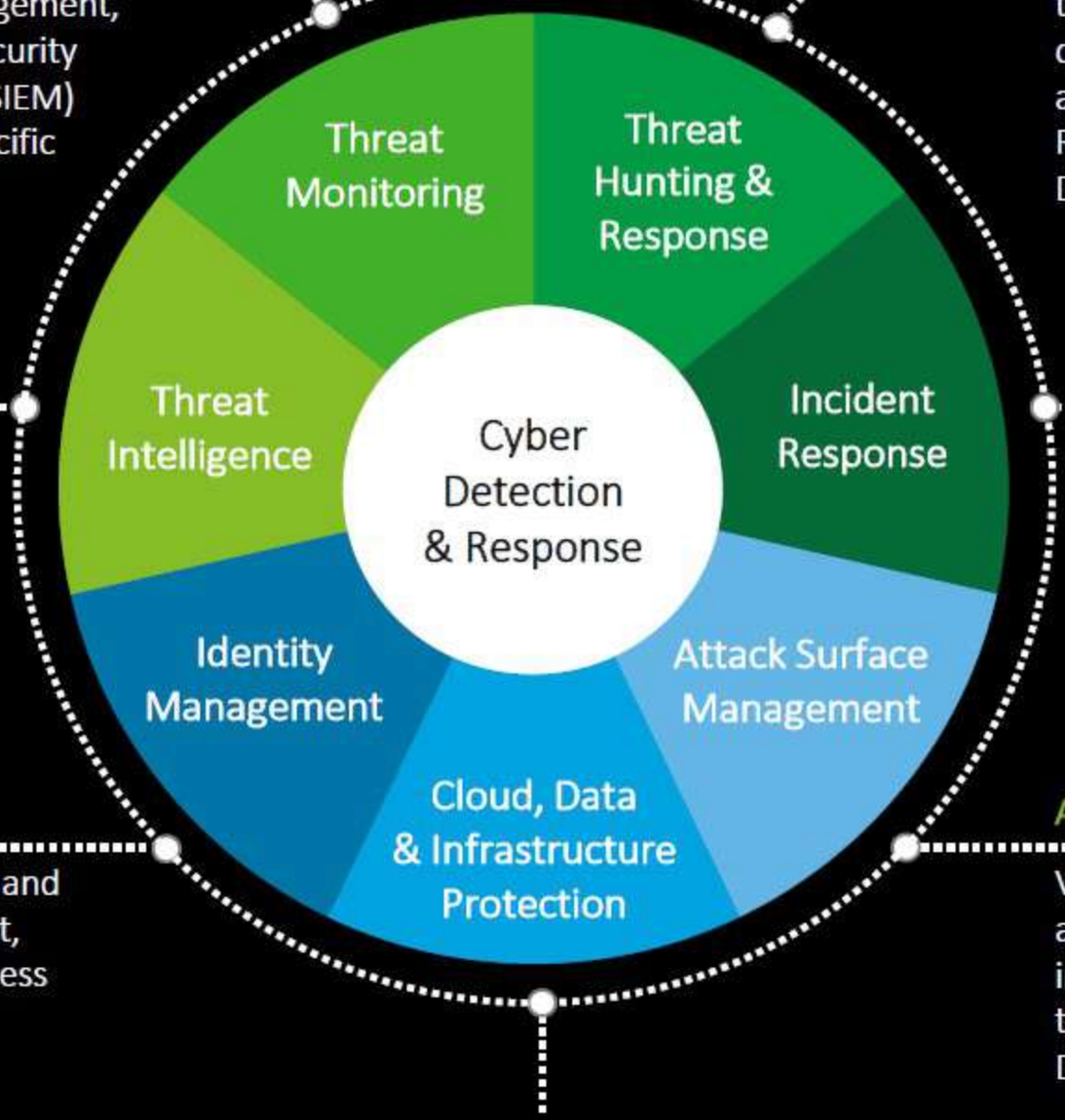
Proactive hunting for sophisticated threats that may evade the first line of defence. Hunt activities using big data analytics, with Managed Detection and Response (MDR) and Endpoint Detection and Response (EDR).

### Threat Intelligence

Data collection from a variety of internal and external sources to identify client-relevant threats targeting your brands, your infrastructure or your people.

### Incident Response

Post breach incident investigation, digital forensics, crisis management, privacy advice with mandatory disclosure, incident containment and recovery.




### Identity Management

Managed identity lifecycle for internal and customer identity, access management, identity governance and privileged access management.

### Attack Surface Management

Vulnerability management, application security management and integration of security controls into the development pipeline with DevSecOps.

### Cloud, Data and Infrastructure Protection

Cloud platform, host and container protection, cloud platform security compliance monitoring. Data protection with managed encryption, Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB). Infrastructure security covering a range of network, endpoint, web and email security controls.

Advise — Implement — Operate