Managed Endpoint Detection and response - Consulting Services

Objectives & Scope

- Evaluate the customer's current endpoint security posture across on-prem, cloud, and hybrid environments
- Identify threat visibility gaps, detection blind spots, and operational inefficiencies
- Provide actionable recommendations aligned to industry best practices and Microsoft/CrowdStrike ecosystems

Assessment Scope

- Review existing EDR/XDR tools, configurations, and operational processes
- Evaluate endpoint coverage, telemetry, and detection effectiveness
- Analyze licensing optimization and cost efficiency
- Assess SOC maturity, workflows, and response playbooks
- Review integration other platforms

Assessment of Existing Environment EDR & XDR Capabilties

Detection Visibility
- Coverage across the enterprise
- Technical capabilities across threats

Integration and Operational maturity
- Endpoint coverage and sensor health
- Policy structure and security baselines
- OS/platform coverage

Response and Automation
- Investigation, automation and response
- Threat hunting capabilities
- Remediation effectiveness

Alignment with business & Security Objectives

Risk Coverage & threat landscape alignment
- Critical assets and crown jewels protection
- Industry specific threat mitigation planning

Regulatory compliance
- Alignment with regulatory frameworks
- Data residency and privacy obligations

Costs assessment
- License cost + operational cost vs indirect savings through risk mitigation
- Over vs under utilization of the EDR/XDR solution

Future Readiness & Security Roadmap

Scalability & Cloud readiness
- Scalability readiness across hybrid and multi-cloud
- Support for future cloud workloads

AI-Driven Functionality
- Availability and usage of AI driven features

OEM roadmap and ecosystem strategy
- OEM roadmap vs customer organization IT landscape strategy comparison