Services to be provided:

1. **Defender for Endpoint Proof of Concept**
   Description: Security Risk Advisors ("SRA") will work with CLIENT ("CLIENT") to implement Windows Defender for Endpoint on the Windows OS to a defined pilot group (up to 27,000 workstations and/or servers) with the goal of enhancing server and workstations security visibility and blocking. SRA will validate the efficacy of the Defender configuration using test cases that simulate the threats that CLIENT is most likely to encounter.
   Deliverable: Status Reports, Defender environment configuration documentation, and test efficacy of expected detective and preventive security configurations.

SRA will work with the CLIENT Software Deployment Team to deploy Windows Endpoint Defender to Windows workstations and servers. SRA will enable baseline configurations and features including:

- **Network Discovery:** Network Discovery will be configured to identify enterprise devices, network devices, and IOT devices to validate the scope of deployment. This will support identifying further attack surface of unknown and unmanaged devices on the network.
- **Anti-Virus:** Windows Defender will be configured as the primary Anti-Virus for scanning files. Active Mode will be enabled to remediate threats and serve as a building block for developing automated responses.
- **RealTime Protection:** Settings will be deployed to continuously scan endpoints and files for malicious activity. This includes raw volume writes that can provide an early indicator for ransomware activity.
- **Behavioural Monitoring:** Behavioural monitoring will be configured to detect fileless malware based on Microsoft Artificial Intelligence and Machine Learning capabilities.
- **Potentially Unwanted Applications Protection (PUA):** SRA will configure PUA to identify and block programs that could increase the attack surface of CLIENT endpoints. These applications are often associated with system performance issues and can contain application vulnerabilities.
- **Cloud Protection:** SRA will configure Cloud Protection to integrate with Microsoft Advanced Protection Service (MAPS) to provide near real-time updates across numerous threat telemetry.

Following the successful implementation of the baseline Defender controls, SRA will continue with implementation of Defender features, but that require additional testing and caution before moving into production:

- **Attack Surface Reduction (ASR):** SRA will configure and deploy up to 16 hardening features for Windows workstations or servers against common ways attackers compromise systems and credentials. SRA will initially deploy these in audit mode and observe them through the Defender API to identify potential policy conflicts. SRA will work with the CLIENT team to provide specific recommendations for allow lists to minimize any business impact in the transition to block configuration. SRA will document a repeatable process to continue the deployment after the initial pilot phase.
- **Exploit Protection:** SRA will configure and deploy up to 6 exploit hardening features to improve the hardening of workstations. These configurations will be deployed in audit mode to identify potential business impacts.
- **Controlled Folder Access:** SRA will work with CLIENT to identify additional folders that can be protected with Microsoft Defender Controlled Folder Access to restrict unauthorized or script based engines from interacting with files.
- **Custom Detection Rules:** SRA will build and deploy 50 custom detection rules within Defender for Endpoint to look for specific MITRE ATT&CK techniques. (rules will come from SRA existing library)
- **Tamper Protection:** SRA will configure Tamper Protection to safeguard CLIENT endpoints from an attacker attempting to modify or disable security settings which help support the Security Team's ability to respond to attacks. Deployment of Tamper Protection via modern management will provide granular group-based deployment control.

- **Endpoint Hardening**: SRA will review 10 priority endpoint configuration settings on Windows workstations to identify and recommend hardening configurations.
- **SIEM Integration:** SRA will integrate Windows Defender with SIEM to provide a single pane of glass for all security events, track alerts, and coordinate response activities.

SRA will create documentation for any new security controls or processes that are introduced as part of this engagement. We will also provide knowledge transfer/training sessions for CLIENT teams and/or third parties who will be responsible for the maintenance and operations of security controls, configurations, or processes implemented during this engagement.

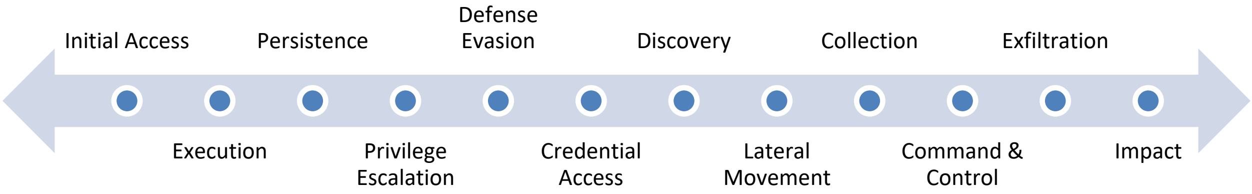
Following the technical implementation, SRA will create a concise roadmap outlining deployment options to the rest of the organizations, as well as recommendations for further enhancements to improve overall Defender capabilities.

SRA will also implement a limited number (up to 100) instances of Defender for Mac on supported systems, document the implementation and configuration process, and share with CLIENT.

2. Quality Assurance Testing

Description: SRA Consultants will work side-by-side with CLIENT security analysts to validate the effectiveness of current detection capabilities as well as identify, improve and tune detection gaps in existing defensive toolsets. SRA will lead scripted attack simulations to test rules, identify gaps, and transfer knowledge to CLIENT team members.
Deliverables: Status Reports, Findings and Recommendations.

SRA will start with a workshop to understand the scope of defenses (Protect and Detect Controls), and previous efforts to align to the MITRE ATT&CK Framework. SRA will discuss your toolsets, integrated log sources, and known visibility gaps (if any). SRA will recommend various testing scenarios across the MITRE ATT&CK “tactics”:



SRA will draft and configure a Windows Endpoint focused campaign, which will include red team operations/test cases mapped to the MITRE ATT&CK Framework. This campaign will document how simulations can be consistently carried out and scored.