Cybersecurity Maturity Assessment

CrowdStrike evaluates an organization's cybersecurity maturity level in relation to its ability to prevent, detect, and respond to advanced adversaries. Within this context, CrowdStrike will assess the Customer's environment for opportunities to close gaps in their cybersecurity people, processes, and technologies. Customer will select from among three available Cybersecurity Maturity Assessment ("CSMA") offerings designed to scale with the complexity and size of their organizations.

Concept of Operations

CrowdStrike's Cybersecurity Maturity Assessment ("CSMA") offering takes a multi-faceted approach to gaining an understanding of the Customer's existing cybersecurity program. CrowdStrike will review relevant internal cybersecurity documentation and then conduct workshops with individuals within the organization who understand how the Customer's existing cybersecurity program works in reality – regardless of what the documentation may say. We also use our Falcon agent to collect information from the Customer's endpoints in order to gain a better understanding of the technical hygiene in the environment. Optionally, the CSMA can be performed without the use of the Falcon agent. By combining these information sources, CrowdStrike will help to paint the picture of where the organization's capabilities are strong, where it can improve, and what steps are recommended for the organization to mature.

Scope of Assessment

CrowdStrike's three CSMA offerings utilize similar methodologies but vary in scope and scale. The assessment scope and scale will depend on the specific offering that Customer selects:

CSMA (Core)

CrowdStrike will focus its assessment across six core cybersecurity areas:

- Security Foundations
- Detection
- Prevention
- Response
- Governance
- Threat Intelligence

CSMA (Expanded)

CrowdStrike will assess the six core cybersecurity areas, as well as three additional focus areas agreed by CrowdStrike and Customer based on Customer's risk profile or operational challenges.

Core cybersecurity areas:

- Security Foundations
- Detection
- Prevention
- Response
- Governance
- Threat Intelligence

Additional focus areas may include:

- Identity and Access Management
- Asset and Vulnerability Management
- Disaster Recovery and Business Continuity
- Server and Endpoint Security
- Network Security

- Cloud Security
- Application and Database Security
- Operational Technology Security
- Clinical Technology / IoMT Security
- Artificial Intelligence Security

CSMA (Enterprise)

CrowdStrike will focus its assessment across areas to include:

- Strategy and Governance
- Culture, Awareness, and Training
- Risk and Compliance
- Identity and Access Management
- Asset and Vulnerability Management
- Disaster Recovery and Business Continuity
- Server and Endpoint Security
- Network Security
- Cloud Security
- Application and Database Security
- Cybersecurity Incident Detection and Response
- Threat Intelligence

Depending on the Customer's risk profile or operational challenges, an additional area of focus could include:

- Operational Technology Security
- Clinical Technology / IoMT Security
- Artificial Intelligence Security

Potential Engagement Artifacts

CrowdStrike may provide the following artifact for this engagement:

- An executive summary that succinctly summarizes the scope of the assessment and surveys, at a high level, the primary observations noted during the assessment. Observations include key strengths, areas for improvement, and associated recommendations. This report will also, at Customer's discretion, include the graphical representation of the organization's cybersecurity maturity, as determined through the assessment.
- A full assessment report with descriptions of the CSMA methodology, maturity scores and proposed target maturity levels for each capability area, recommendations for achieving the target maturity levels, prioritization of which recommendations to pursue first, and any technical hygiene findings from Falcon enrichment analysis. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.
- Mapping to NIST Cybersecurity Framework (CSF) (Optional)