FAQ: CISCO-FUNDED CUSTOMER SECURITY ASSESSMENT

General Information

1. **Who is paying for this security assessment?** Cisco is funding this security assessment as part of their commitment to enhancing customer security.
2. **Who will be conducting the assessment?** Enable, as a Cisco partner, will be conducting the security assessment.
3. **What information will be collected during the assessment?** We collect minimal personal information, primarily for proof of performance. The Assessment will be covered under the Enable Assessment NDA, which provides for sharing relevant information required by Cisco.
4. **How is my personal information protected?** Cisco handles personal information in accordance with their Online Privacy Statement, available at https://www.cisco.com/c/en/us/about/legal/privacy-full.html.
5. **What does the assessment process involve?** The assessment typically includes analysing your security requirements, evaluating your current setup, and proposing Cisco solutions to address any identified gaps or improvements.
6. **How long does the assessment process take?** The duration can vary depending on the complexity of your environment, but typically requires a day of your time to complete the Security Interview phase.
7. **Can public sector organisations participate in this assessment program?** Unfortunately, public sector opportunities, including national, federal, state, and local governments, as well as education customers, are not eligible for this Customer Assessment Incentive.
8. **Can the assessment be modified or cancelled?** Enable reserves the right to modify or cancel the assessment at its discretion without notice.
9. **How is the assessment conducted?** The assessment is conducted through an interview process:

    - It is an interview-only assessment and does not require access to the customer's IT infrastructure.
    - No penetration testing will be performed.
    - No log analysis or review of system logs is involved.
    - There are no physical connectivity activities or direct interactions with the customer's systems.

10. **Am I obligated to make a purchase after the assessment?** No, you are under no obligation to make any purchase as a result of this assessment. The assessment is provided as a free service to help you understand your security posture, and any decisions to implement recommendations or purchase solutions are entirely at your discretion.

Assessment Report

11. **Will I receive a report after the assessment?** Yes, you will receive an output report or project plan detailing the assessment findings and proposed Cisco solutions.
12. **What is included in the findings report?** The report typically includes an executive summary, detailed inspection findings, security recommendations, next steps, and an appendix with additional details.
13. **Will there be a final readout of the assessment results?** Yes, there will be a final customer readout meeting to discuss the assessment findings. Cisco may be invited to this meeting at their discretion.
14. **Does the report include pricing information for recommended solutions?** Yes, the Appendix typically includes pricing information for recommended products and may provide details about follow-on services.

Assessment Areas

16. **What areas does the assessment cover?** There are four assessments that are available, covering:
    - Campus and Edge
    - Cloud
    - IoT (Internet of Things)
    - Data Centre and Virtual Infrastructure
17. **What aspects are examined in the Campus and Edge Inspection?** This inspection covers Perimeter Controls, Internal Network Controls, Endpoint Controls, Application and Data Controls, Identity and Access Controls, Security Policies, Training, and Incident Response, IT Sustainability, and Compliance and Audit.
18. **What does the Cloud Inspection involve?** The Cloud Inspection examines Cloud Provider Controls, Customer Controls, and Shared Controls. It also addresses multi-cloud environments, cloud-specific incident response, and data protection in the cloud.
19. **What areas does the IoT Inspection cover?** The IoT Inspection covers Device Controls, Network Controls, Authentication and Access Control, Application Controls, Data Privacy and Integrity, Incident Response and Management, Compliance and Audit, Supply Chain Security, and Continuous Improvement.
20. **What is included in the Data Centre and Virtual Infrastructure Inspection?** This inspection covers Network Controls, System Controls, Administrative Controls, Compliance & Audit Controls, and Virtual Infrastructure including aspects like Hypervisor & VM Controls, Data Protection and Privacy, and Continuity and Resilience.

Scope and Limitations

21. **Is this assessment comprehensive and legally binding?** While thorough, this assessment is not exhaustive. Enable does not accept liability for the

validity of the finding. It's designed to provide valuable insights into your security posture and potential improvements.

22. **How can I use this report to improve my organisation's security posture?** You can use the report to understand current security gaps, prioritise investments, make informed decisions about new security solutions, and plan for future improvements.