WORKSHOPS AND ASSESSMENTS

Cybersecurity Resilience:

GUIDING YOUR CYBERSECURITY IMPROVEMENT JOURNEY

getstarted

The challenge

Security assessments have become an integral part of how businesses measure their cybersecurity-maturity level. They enhance how we prioritize projects and define milestones in our security program by evaluating capabilities, technology, and risk-management processes. Is your business resilient to the threats of the current times?

Our solution

This workshop will evaluate your security posture across four critical pillars: Zero Trust, Security Infrastructure, eXtended Detection and Response (XDR), and Security Operations leveraging the Zero Trust Model.

The benefits

The workshop offers five key benefits:

1. **Enhanced Security Posture:** Identifies gaps and strengthens defenses against cyber threats, on or off premises
2. **Regulatory Compliance:** Ensures adherence to relevant cybersecurity regulations and standards, helping to avoid legal penalties and fines.
3. **Trust and Confidence:** Demonstrates a commitment to data security, enhancing your customer trust and business reputation.
4. **Risk Management:** Provides insights for informed decision-making in managing and mitigating cyber risks.
5. **Business Continuity:** Helps prevent security breaches that can lead to costly downtime and disruption of business operations.

Workshop details

- The workshop is designed to empower you with the knowledge and tools necessary to assess and enhance your organization's security posture. The engagement is delivered in the following format:

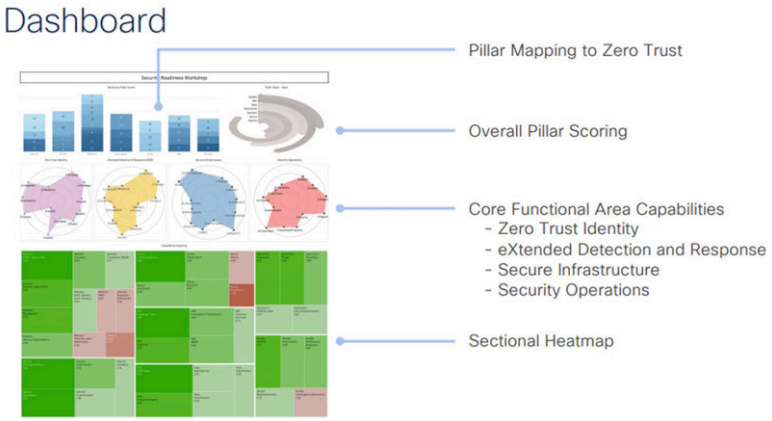
Activity	Description
Session 1: Introduction to the workshop 45 Minutes	• Introduction to security resilience assessment pillars and core functional areas • Workshop and the guided assessment framework and success criteria
Session 2: Guided Assessment 2 hours	During the guided assessment, with the help of pre-build questionnaires tool, we will facilitate the engagement in self-assessment of your environment across 7 key security resilience pillars (not products). We will provide insights into best practices, emerging threats, and effective strategies for safeguarding critical assets. After completing the assessment, we will compile and present a comprehensive capability view during session 3.
Session 3: Report review and next steps recommendations 1 hour	In this report review session, we will cover: • What we did and how we did it – Event View • What were the findings – Dashboard • Recommendations for how to address the findings • Follow-up actions

Workshop deliverables

We will compile and share a comprehensive capability view, providing valuable insights into your current security posture.

The heatmap of capabilities across the seven pillars will outline technical control competencies and areas that require review.

We will highlight the strengths and weaknesses within each pillar based on the inputs that you have provided into the forms.



Learn more about how Compucom sources, inegrates, and supports all your technology needs at compucom.com.