BRIEF

/ Essential Eight Control Effectiveness Assessment

LevelBlue

Get technical assurance of ACSc's essential eight security controls

Independent assessment and recommendations supporting risk management and compliance

The Australian Cyber Security Centre's Eight Mitigation Strategies and Maturity Model are high-impact security controls to mitigate common cyber threats, but organisations can struggle to assess their effectiveness.

Give your stakeholders a higher level of comfort with LevelBlue's Essential Eight Control Effectiveness Assessment service, which provides a controls assessment report with actionable recommendations to resolve control weaknesses and misconfigurations.

This service can either supplement an Essential Eight maturity assessment or be used as a repeatable point-in-time independent assessment of control effectiveness. As a standalone service, it can provide an economical approach to understanding and remediating risk using the controls recommended by the ACSC to mitigate the most common cyber threats, resulting in a rapid uplift of your organisation's cybersecurity posture.

Upon engagement, LevelBlue will determine the scope, agree on the test environment, and deliver the assessment, resulting in an actionable Essential Eight Control Effectiveness Assessment report detailing findings and recommendations, with a suggested implementation roadmap.

Increase visibility of security control effectiveness

LevelBlue's Essential Eight Control Effectiveness Assessment is performed by experienced consultants or LevelBlue's renowned SpiderLabs team in tandem with your organisation on a representative Microsoft Windows environment.

Benefits

- Delivered by specialist LevelBlue consultants trained in Essential Eight control assessments
- Can provide a higher level of comfort and assurance than typical interview–based Essential Eight compliance or maturity assessments
- Assesses if technical security controls appear to be functioning as designed and implemented
- Can uncover Essential Eight security control weaknesses and misconfigurations that vulnerability scanners cannot
- Results in a detailed findings report with actionable remediation recommendations, including an implementation roadmap
- Offered as a repeatable service that can be run again after remediating recommendations or to augment internal audit or third-party assessment services
- Supports organisational risk management and compliance assessment goals and compliance assessment goals

The Essential Eight Control Effectiveness Assessment service:

- Provides an independent third-party assessment of your organisation's technical security controls within ACSC's Essential Eight Mitigation Strategies up to Maturity Level One.
- Employs a tools based, or a SpiderLabs led assessment of a Standard Operating Environment (SOE), server or Microsoft Active Directory Domain configuration:
  - » Application Control;
  - » Patch Applications;
  - » Patch Operating Systems;
  - » Restrict Microsoft Office Macros; and
  - » User Application Hardening controls.
- Uses a tools based, or SpiderLabs led assessment of the effectiveness of any application control solution and associated policies for weaknesses or exceptions, including PowerShell checks for Microsoft Defender, Microsoft Office, and Microsoft's Attack Surface Reduction (ASR) rules.
- Assesses whether working, publicly available exploits exist for any known application or operating system vulnerability, coupled with a review of vulnerability mitigation duration.
- Examines whether email filter controls are successfully blocking the delivery of files containing Microsoft Office macros and the robustness of Office macro configuration settings.
- Reviews user application hardening controls considering appropriate access to resources to reduce the risk of undesirable threat vectors.
- Includes Multi-Factor Authentication (MFA) effectiveness testing of VPN or remote access services by LevelBlue's world-renowned SpiderLabs team, considering prevalent threats and MFA evasion attack techniques used by real-world adversaries.
- Incorporates an assessment of the hidden and often unintended privilege relationships within an Active Directory or Azure Entra ID environment to inform the organisation of potential attack paths which can contribute to the Essential Eight requirement: Restrict Administrative Privileges.
- Includes an evidence-based assessment of your organisation's backup processes, including a technical assessment of the robustness of your backup repositories that are often targeted for destruction in a cyber-attack, by examining network segregation and privileged access controls.

Support risk management and compliance objectives

LevelBlue's Essential Eight Control Effectiveness Assessment service is ideal for any organisation in support of an organisational cybersecurity risk assessment or in support of a need to comply with aspects of related security frameworks, including, for example: NIST CSF, ISO 27001, PCI-DSS, IS18, PSPF, DISP and the Australian Information Security Manual (ISM).

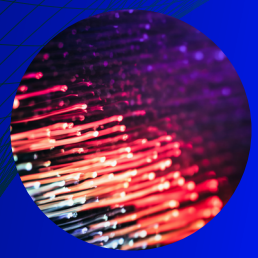
Regulatory: Enterprises facing regulatory requirements, such as the Security of Critical Infrastructure (SOCI) Act (2018) may elect to implement the Essential Eight Mitigation Strategies to Maturity Level One, to satisfy legislative requirements. These obligations require risk management approaches that should consider how an organisation designs, implements, and validates technical security controls.

Similarly, organisations that need to implement the CPS 234 Information Security standard must "implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls".

Scale: With consultants throughout Australia, LevelBlue can provide your organisation with the Essential Eight Control Effectiveness Assessment, regardless of your location.

Commercial Responsiveness and Flexibility: Our flexible models allow you to procure one time or repeat assessments to support your assurance programs with three levels of service offering: Lite, Standard, and Advanced.

Upon engagement, LevelBlue will determine the scope, agree on the test environment, and deliver the assessment, resulting in an actionable Essential Eight Control Effectiveness Assessment report detailing findings and recommendations, with a suggested implementation roadmap.



LevelBlue

Contact us www.levelblue.com