Cyber Centre of Excellence
for Local Public Services

Validato
SECURITY CONTROLS • VALIDATED

VALIDATO SERVICE DEFINITION DOCUMENT

What is Validato?

Validato is a next-generation Security Validation platform, now part of the CCoE Protect Suite, designed to help organisations test and strengthen their resilience against the latest malware and ransomware threats. Validato enables IT and security professionals to safelysimulate hundreds of real-world cyber threat scenarios, ranging from ransomware to the latest government threat advisories, without any risk of damage or disruption to operations.

Why choose Validato?

- **Independent, unbiased validation:** Validato provides clear, objective data on your organisation's internal risk posture, whether for ongoing assurance, acquisition due diligence, or critical vendor risk assessment.
- **Comprehensive threat coverage:** Simulates hundreds of cyber threat scenarios based on MITRE ATT&CK techniques, including ransomware and advanced adversary tactics.
- **Safe and non-disruptive:** All simulations are performed in minutes, with no risk to business operations or data integrity.
- **Tailored remediation guidance:** Receive actionable recommendations to close security gaps quickly and effectively.
- **Framework mapping:** Results can be mapped to leading control frameworks, including NIST CSF/800-53 and ISO 27001, supporting compliance and audit requirements.
- **Regulatory readiness:** Supports resilience testing required by new regulations and legislation, such as DORA and NIS2 in the EU and GLBA in the USA.
- **Ideal for mergers and acquisitions:** Obtain an independent assessment of a target company's cyber risk posture, or conduct critical vendor risk assessments with confidence.
- **Compliments AppGuard:** Validato works seamlessly alongside EDRs and advanced zero-trust solutions like AppGuard, providing an additional layer of assurance and validation.

What is included in the Validato Service?

- **Breach & Attack Simulation (BAS):**
  - Use our expert team to conduct independent tests on your behalf.
  - Uses up to two images of your current environment and EDR defences to simulate real-world attacks.
  - The most popular and current threat scenarios are tested and mapped against MITRE ATT&CK techniques.
- **Security Controls Effectiveness Testing:**
  - Validates your ability to protect against adversaries.
  - Ability to isolate your EDR defences and test your cyber resilience with and without these layers.
  - Provides unbiased data on the resilience of your controls against specific cyber threats.
- **Tailored Remediation Recommendations:**
  - Actionable guidance to harden your defences and close identified gaps.
  - Option to measure the detection levels of your SCO/SIEM to aid their configuration.
- **Framework Mapping:**
  - Results mapped to NIST CSF/800-53 and ISO 27001 for compliance and reporting.
- **Reporting:**
  - Clear, executive-friendly reports with technical detail for IT. and security teams.
  - Includes benchmarking and suggested actions for improvement.
- **Quarterly Cyber Resilience Testing:**
  - Maintain an up-to-date assessment of your constantly changing systems with quarterly validation tests to maintain a strong security posture.
  - More frequent testing is available on request.

Validato is also available as an installed cloud-based service for you to manage and run internally as frequently as you need. Please contact us if you would like to discuss this option.

iese

CYBER ESSENTIALS CERTIFIED PLUS

Cyber Centre of Excellence
for Local Public Services

Validato
SECURITY CONTROLS • VALIDATED

Features include:

- Breach & Attack Simulation (BAS) platform.
- MITRE ATT&CK-based scenario coverage.
- No risk of operational disruption.
- Tailored remediation guidance.
- Mapping to NIST CSF/800-53 and ISO 27001.
- Executive and technical reporting.
- An option for quarterly resilience testing.

Benefits include:

- Independent, unbiased assessment of cyber risk posture.
- Rapid identification and closure of security gaps.
- Enhanced compliance with regulatory and audit requirements.
- Improved resilience against malware, ransomware, and advanced threats.
- Confidence in mergers, acquisitions, and vendor risk management.
- Actionable insights for IT, security, and executive teams.

About CCoE

The Cyber Centre of Excellence (CCoE) was established in direct response to the escalating threat of cyber-attacks facing UK public services. Founded by IESE CIC and shaped by collaboration with local authorities and sector experts, CCoE's mission is to make the UK the safest place to live, work, and play in the digital world. CCoE brings together leading expertise from across the public and private sectors to deliver military-grade cyber protection, training, and strategic support tailored for councils, schools, care providers, and small businesses.

By identifying, testing, and packaging advanced cyber security tools and services - including solutions like Validato - CCoE helps public sector organisations build resilience against both current and emerging threats. As a not-for-profit, sector-led initiative, CCOE operates with agility and a clear public benefit focus, ensuring that the latest cyber defence capabilities are accessible and affordable for all UK communities.

Through innovation, collaboration, and a commitment to continuous improvement, CCOE is building a digitally secure future for the UK.

iese

CYBER ESSENTIALS CERTIFIED PLUS

For more information about:

CCoE, visit: www.ccoe.org.uk

IESE, visit: www.iese.org.uk