RCS
RAVEN CYBERSECURITY

SECURITY ASSESSMENT SERVICES

OUR DELIVERABLES

CONSULTATION AND PLANNING

Engage in collaborative sessions to understand your unique security needs and plan tailored assessments, ensuring a clear roadmap for our partnership

EXECUTIVE & TECHNICAL REPORT

Insightful documentation merging managerial perspective with technical details for strategic decision-making

TAILORED BEST PRACTICES RECOMMENDATIONS

Customized guidance to fortify security, aligning with practices from industry standards

COMPREHENSIVE SECURITY ASSESSMENT

Perform evaluations of your digital infrastructure, including systems, networks, and applications, to identify vulnerabilities and assess potential risks

RETESTING OF REMEDIATED VULNERABILITIES

Verify the elimination or mitigation of identified vulnerabilities, ensuring the efficacy of remediation efforts

TECHNICAL SUPPORT FOR REMEDIATION

Expert guidance and assistance during remediation, ensuring effective implementation of security measures

SERVICES OFFERED

CLOUD SECURITY ASSESSMENT

Evaluate cloud security configurations, enhance access controls, and fortify data protection protocols

INTERNAL NETWORK SECURITY AUDIT

Identify vulnerabilities within your internal network through robust penetration testing and audits

EXTERNAL NETWORK SECURITY AUDIT

Thoroughly assess external-facing systems to fortify perimeter defenses against potential cyber threats

RED TEAM ASSESSMENT

Simulate real-world cyber-attacks, test defenses, and enhance incident response capabilities

WEB APPLICATION PENETRATION TESTING

Secure web applications through meticulous testing, identifying and mitigating potential vulnerabilities

SECURITY CONTROLS REVIEW

Audit and optimize security policies, procedures, and employee awareness programs for effectiveness

PCI DSS SECURITY AUDIT

Ensure compliance with Payment Card Industry Data Security Standard and fortify cardholder data protection

GDPR SECURITY AUDIT

Evaluate data protection measures, conduct impact assessments, and enhance breach response plans

CYBER THREAT DEFENSE

SERVICES OFFERED

SECURE CODE REVIEW

Assess code quality, identify vulnerabilities, and provide guidance on secure coding practices

MOBILE APPLICATION PENETRATION TESTING

Evaluate mobile app security, including data storage, transmission, permissions, and authentication mechanisms

IOT PENETRATION TESTING

Assess communication protocol security and evaluate resilience against physical tampering for IoT devices

THREAT INTELLIGENCE & DARK WEB CYBER INTELLIGENCE

Monitor dark web forums, leverage open-source intelligence, and stay ahead of potential threats

DIGITAL FORENSICS AND INVESTIGATIONS

Conduct expert-led digital forensics, uncovering root causes and implementing proactive measures

3RD PARTY RISK ASSESSMENT REVIEW

Evaluate cybersecurity posture of suppliers and vendors, ensuring a secure supply chain

CYBER THREAT DEFENSE

SERVICES OFFERED

SOCIAL ENGINEERING – PHISHING SIMULATION

Conduct realistic simulations to test and enhance employee resilience against phishing attacks

RED TEAM ASSESSMENT

Simulate real-world cyber-attacks, test defenses, and enhance incident response capabilities

ENDPOINT DETECTION AND RESPONSE

Real-time monitoring and automated threat response to protect endpoints, ensuring security and rapid response to cyber threats.

SECURITY AWARENESS AND EDUCATION

Develop customized awareness campaigns and deliver ongoing educational content for enhanced cyber vigilance

GDPR SECURITY AUDIT

Evaluate data protection measures, conduct impact assessments, and enhance breach response plans

CYBER THREAT DEFENSE

Acronis Cyber Protection

# OUR METHODOLOGY

SCOPING

- Conduct scoping through questionnaires and interviews to understand the client's business, assets, and specific security needs.

PLANNING

- Develop a detailed assessment plan outlining the specific requirements and objectives.
- Collaborate with the client to establish a timeline and allocate the necessary resources.

EXECUTION OF ASSESSMENT

- Perform the assessment based on the established plan and scope.
- Utilize a combination of tools, with automated and manual testing to identify vulnerabilities.
- Assess the security posture of in-scope assets.
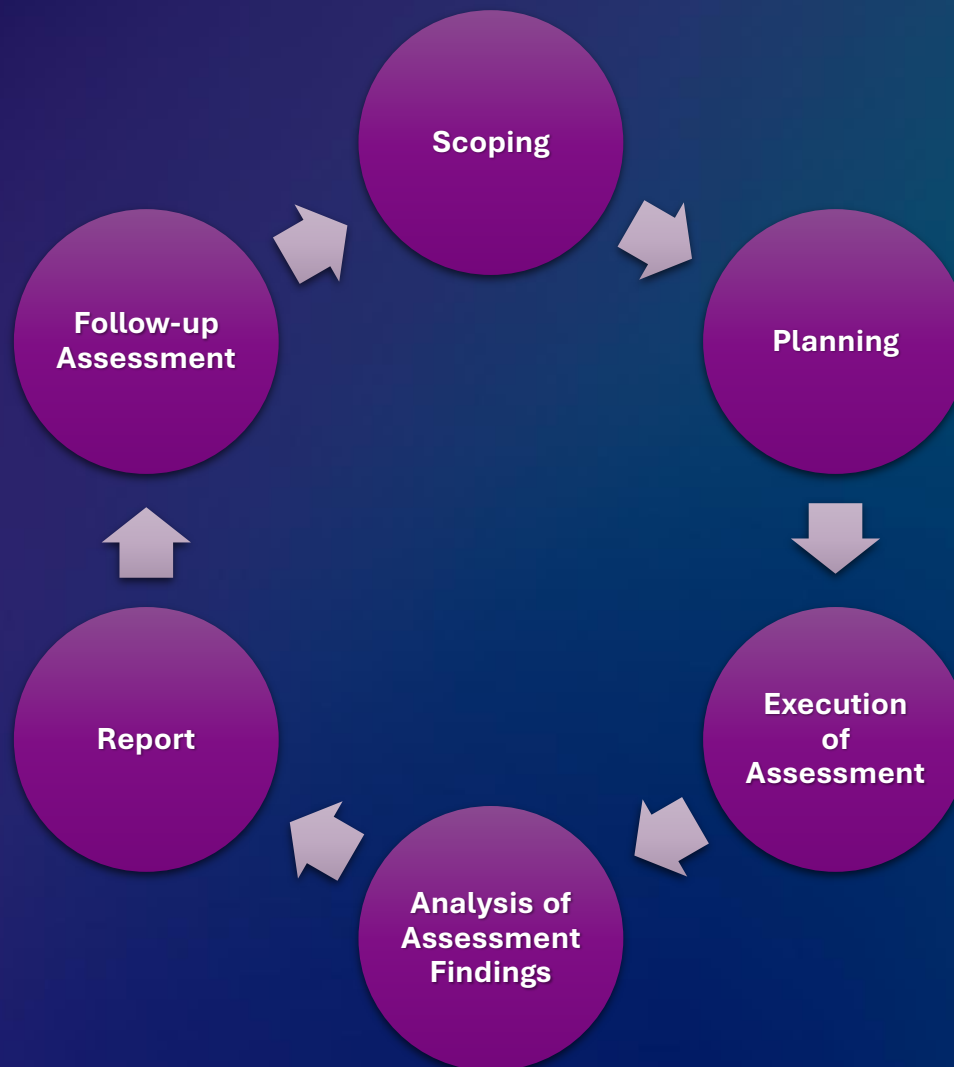
ANALYSIS OF ASSESSMENT FINDINGS

- Analyze assessment findings, classify vulnerabilities, and categorize risks.
- Collaborate with the client to understand risk tolerance and align findings with business priorities.

REPORT

- Deliver comprehensive reports to the client.
- Executive Report for non-technical stakeholders, highlighting strategic actions.
- Technical Report for IT and security teams, detailing vulnerabilities and remediation steps.

FOLLOW-UP ASSESSMENT

- Reassess post-remediation to verify security improvements.
- Update assessment report to reflect changes in security posture.

Circle diagram: Scoping → Planning → Execution of Assessment → Analysis of Assessment Findings → Report → Follow-up Assessment

WHY CHOOSE US FOR YOUR SECURITY ASSESSMENT?

HOLISTIC SOLUTIONS

Comprehensive security services tailored to safeguard your digital landscape

PROVEN PENETRATION TESTING SUCCESS

Demonstrated success in identifying and addressing vulnerabilities, with a growing track record of enhancing the security posture of clients

SPECIALIZED EXPERTISE

Professionals offering specialized assessments to address your unique security needs

CLIENT-CENTRIC APPROACH

Prioritizing client satisfaction and trust through personalized, results-driven security solutions

DATA PRIVACY

Assured confidentiality of your sensitive information through stringent Non-Disclosure Agreements (NDAs)

BUSINESS CONTINUITY

Manage uninterrupted operations with thorough assessments and recommendations designed to maximize cybersecurity

GET IN TOUCH

ravensec.eu

+30 6948379112

Raven Cybersecurity