DATA SHEET

SECURITY ASSESSMENT AND RISK CONSULTING SERVICES

Professional Services

AT A GLANCE

Leverage our cyber security team combined with the world's leading technologies.

Our Security Assessment & Risk Consulting team provides professional services to identify vulnerabilities and assess real business risk against local and international compliance standards, such as ISO 27002, PCI DSS, HIPAA, SANS 20 and other security compliance mandates. Our range of services include:

- Vulnerability Assessment & Penetration Testing
- Web Application Security Testing
- Social Engineering Testing & Awareness
- Network Risk Assessments
- Configuration and Compliance
- GRC Audits
- ISO 27001 Preparation and Audits
- Digital Forensics
- Security Incident and Emergency Response

VULNERABILITY ASSESSMENT & PENETRATION TESTING

Our team takes away the complexity of delivering routine scanning on a scheduled and continuous basis. Ensuring that scanning objectives are met in an environment which only allows scanning outside of business hours is a challenge for most organisations. We deploy and maintain scanning infrastructure, conduct and monitor the scanning and analyse the results to advise on prioritised remediation activities. Services include:

- Penetration testing of external public facing assets
- Vulnerability testing of internal servers and networks
- Vulnerability testing of endpoints
- Wireless networking assessments
- Simulation and manual testing to verify exploits against detected vulnerabilities
- Simulation of social engineering attacks
- Compliance benchmarking against PCI 3.x, FFIEC, HIPAA
- Testing your team's response and detection capabilities
- Validate your patching/hardening program
- Support for patching and remediation

WEB APPLICATION SECURITY TESTING

Our Web Application Security Testing service provides granular interrogation of our customer's web applications, web sites, web APIs and mobile applications to identify vulnerabilities and exploitable weaknesses within these systems. We work with customer application teams to harden these environments via rigorous testing by undertaking:

BLACK BOX TESTING

An attacker's eye view where we attempt to exploit the web user interface, either for entering data or observing program behaviour without credentials.

GREY BOX TESTING

Attacker has obtained credentials or has limited knowledge of the program internals. In this instance, our testing team has some credentials or limited knowledge of the application's backend.

SOURCE CODE REVIEW

Testing is based on knowledge of the source code and the tests may target specific constructs found in the source code or try to achieve a certain level of code coverage.

SOCIAL ENGINEERING TESTING & AWARENESS

Our testing team simulates social engineering tradecraft to evaluate the vigilance of your staff against convincing social engineering attempts and spear-phishing threats that work to exploit trust and lack of security awareness.

HOW IT WORKS

PHISHING TESTING

Will your users click on emailed links? What do they do when faced with legitimate looking websites? Are their browsers and plugins updated? Without conducting an actual campaign this data is absent so your risk level is unknown, but that data is waiting to be collected.

We simulate an organisation level phishing campaign by:

Step 1: Design – Designing an organisation specific campaign.

Step 2: Target – Target specific users within the organisation - HR, Finance, R&D, Admin.

Step 3: Email Customisation – Customise the phishing email, including the message envelope as well as its contents.

Step 4: Web Customisation – Build a custom page comprising a landing page and a post-authentication page with a phishing URL that looks authentic.

Step 5: Analysis – Capture and report on users at various stages of the Phish trail and analyse:

- Who gave away credentials
- Who browsed the phishing page
- Who opened the mail
- Who enabled image loading in the mail
- Who resisted the phishing attack

SOCIAL ENGINEERING CALLS

We obtain some basic information with which to test the resilience of our customer's staff against social engineering calls.

DATA SHEET

SECURITY ASSESSMENT AND RISK CONSULTING SERVICES

Professional Services

NETWORK RISK ASSESSMENTS

We conduct risk assessments on our customer environments to determine security gaps and weaknesses across their end-to-end networks. We study the layers of architecture against the industry best practices and provide detailed configuration compliance against documented standards such as NIST, CIS, DISA STIGs.

GRC AUDITS

We deploy GRC automation as a service to enable security leaders to better understand and communicate risks to the business environment from their IT infrastructure. Powered by Symantec Control Compliance Suite, our risk management team translates technical issues into risks relevant to business processes, delivers customised views of IT risk for different stakeholders, and helps prioritise remediation efforts based on business criticality rather than technical severity.

STANDARDS MANAGER
Security Assessment of Technical Controls

ASSESSMENT MANAGER
Security Assessment of Procedural Controls

POLICY MANAGER
Security Policy Lifecycle Management

VENDOR RISK MANAGER
Security and Risk Assessment 3rd Party Service Providers and Applications

RISK MANAGER
Calculate and Aggregate Risk Scores for Remediation and Risk Reduction

SECURITY INCIDENT AND EMERGENCY RESPONSE

Efficient incident response handling is a highly skilled and process driven operation used to tackle security breaches, intrusion and malware infections. Our incident response team is capable of providing rapid response to support customers during these challenging situations.

DIGITAL FORENSICS

We provide an incident forensic investigation service to support incident response efforts. Our team has extensive experience in forensic investigation to identify root cause analysis, internal corporate investigations or intrusion investigations.

FIREWALL MIGRATION

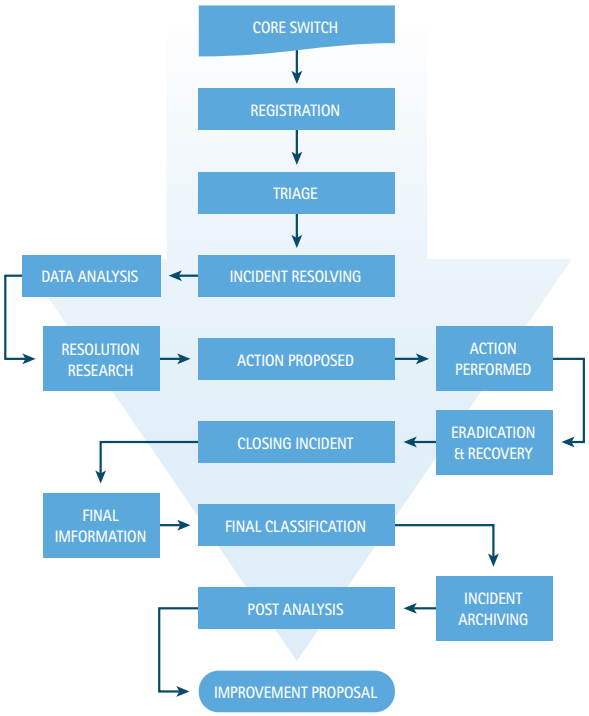
Our professional services team can assist organisations from applying a standard methodology to executing a firewall migration. We support all the leading firewall vendors with firewall management, migration, optimisation and support services. Our team benefits from in depth expertise relating to the complete range of network security appliances and we work collaboratively with our technology partners to optimise processes and toolsets for the implementation of firewall migration services.

ISO 27001 PREPARATION AND AUDITS

We offer a range of compliance services based on industry best practices. Our lead compliance advisors/auditors are leaders in their field and in certain instances are sector specialists in areas such us banking, finance and government. We provide risk assessments, policy and process development and control audits in readiness for certification against:

ISO 27001:2013	DUBAI INFORMATION SECURITY REGULATION (ISR)
PCI DSS	ABU DHABI (ADSIC) SECURITY REGULATION
COBIT	UAE FEDERAL - NATIONAL ELECTRONIC SECURITY AUTHORITY (NESA) STANDARDS
CIS SANS 20	QATAR QCERT REGULATIONS
HIPPA	UK CESG'S GOOD PRACTICE GUIDE 13

SECURITY INCIDENT RESPONSE PROCESS



Contact Us: Sales@siconsult.com