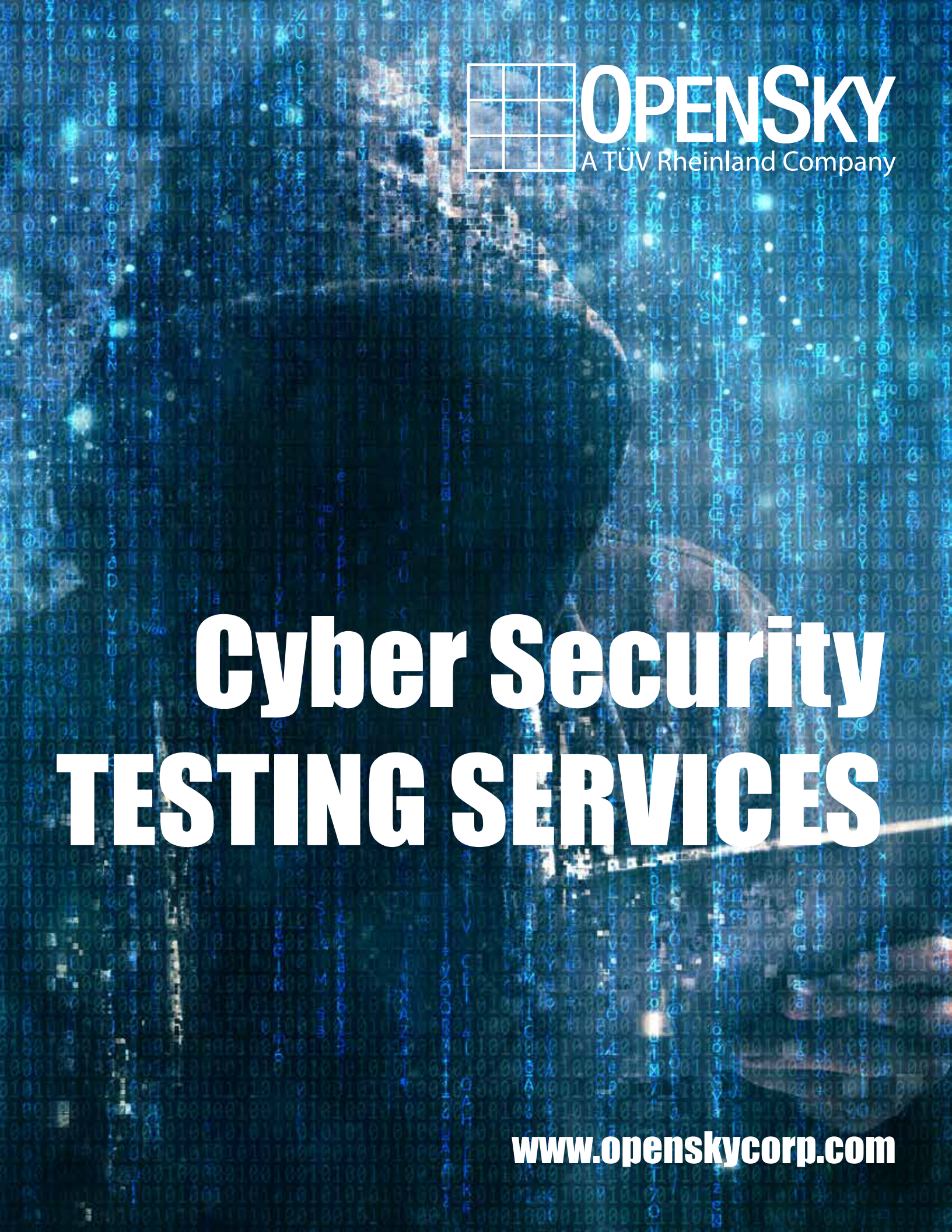
OPENSKY
A TÜV Rheinland Company
Cyber Security
TESTING SERVICES
www.openskycorp.com

Digital Enterprise. Protected.

Cyber Security Testing Services

OpenSky offers a diverse portfolio of cyber security testing services that can be delivered as project based work or as a subscription based service. Whether you need a one-time testing engagement or on-demand continuous testing capability, OpenSky's cyber security testing services can be customized to meet the unique needs of your evolving enterprise.

Project Based

OpenSky's project based cyber security testing is tailored and sized to your specific business needs. After a quick discovery conversation and scoping discussion, OpenSky will develop a testing approach to meet your specific goals and deliver efficient and effective testing in a short-term engagement.

Subscription Based

OpenSky's broad catalog of cyber security testing services, delivered by a team of experienced professionals, is made available for ongoing testing through a subscription based service. Supplement or replace your organization's testing capabilities with dedicated testing hours per week or per month to be used at your direction. This solution offers a compelling alternative to hiring FTEs or staff augmentation resources by providing access to a team of highly skilled professionals, utilizing a collaborative approach to testing, along with OpenSky's testing tools, methodology, and intellectual property. OpenSky can also execute testing utilizing your organization's tools and methodology as a true extension of your team.

Portfolio of Testing Services

Vulnerability Assessment

Anyone can configure and run one of the many vulnerability scanning tools readily available on the market today. Where OpenSky adds value to your organization is in the analysis and interpretation of the results of automated scans. OpenSky testers remove false positives and manually validate findings. They also implement custom scanning to further explore vulnerabilities present on your network. The delivered product isn't just the results of an automated scan, but a comprehensive report outlining your organizations biggest risks as well as actionable short, mid and long term plans to strengthen your security posture.

Typical scopes include internal and external perspectives.

Vulnerability Assessments Included:

- Automated vulnerability scanning of internal or external assets
- Analysis of automated findings for false positive reduction
- Additional scans performed with commercial, OpenSource and custom scripts after initial analysis
- Further manual testing to identify complex vulnerabilities not typically detected by automated scanners
- Analysis of findings and customization of severity and business impact
- Custom recommendations for remediation and mitigation
- A report outlining the greatest areas of risk with actionable next steps for remediation

Penetration Testing

Attackers are adept at finding the path of least resistance into an organization's networks and knowing what can be exploited to gain additional access. OpenSky testers mimic this behavior to simulate a targeted attack. Where a Vulnerability Assessment focuses on breadth, a Penetration

Test is designed to test the depth of your organization's current defenses and demonstrate the business impact of security weaknesses in human, procedural, and technical controls.

A Penetration Test can help illustrate where and how an attacker may strike, and what the attack looks like as it progresses through its various phases, including post exploitation activities. This perspective can often reveal business risks that are not evident through vulnerability assessments. Penetration testing may optionally be scoped to evaluate the organization's security awareness, intrusion detection, and incident response capabilities during the testing, by limiting knowledge of the test in progress.

OpenSky employs a time-boxed methodology to attempt to acquire defined business targets during the testing period, with the scope of testing and rules of engagement well defined during project initiation. Testers use a combination of publicly available methods and custom tools to execute exploitation of vulnerabilities in a controlled manner that is designed to avoid disruption of services.

Social Engineering campaigns are offered as an option to include in penetration testing. Social Engineering campaigns not only reveal areas in which an organization's personnel could benefit from security training and education, but also evaluate the effectiveness of controls and processes related to these types of attacks and demonstrate the associated business risk.

Physical security testing is offered as an option to evaluate physical security controls and security awareness by attempting to gain unauthorized physical access to one or more locations, such as corporate offices and data centers.

OpenSky offers Penetration Testing as a standalone service or as a combined service with a Vulnerability Assessment. Typical scopes include internal, external, wireless, and PCI DSS perspectives.

Penetration Testing Includes:

- Reconnaissance activities, leveraging public data to profile targets
- Evaluation of target environment for potential exploitation paths
- Research, as required, into publicly available exploits and current techniques for bypassing security controls your organization has in place
- Controlled exploitation of select vulnerabilities and security weaknesses
- Optional social engineering campaigns, such as the following:
- Phishing emails to determine how many employees will click on suspicious links
- Phishing emails that attempt to recover employee credentials
- Phishing emails with payloads that attempt to establish a presence on your corporate network
- Phone calls to the organization to attempt unauthorized password resets and retrievals
- Reporting and statistics on all the above: how many users clicked, how many credentials were retrieved, etc.
- Optional physical security testing, including physical intrusion attempts into one or more target locations. This may include social engineering if required.
- Post exploitation activities, such as privilege escalation and lateral movement, to locate and acquire defined targets
- A report that includes a detailed narrative of the testing process and results, including actionable next steps to mitigate your organization's risk

OpenSky offers Penetration Testing as:

- A pure Black-box activity, whereby OpenSky is provided little to no information, beyond testing scope, in regards to the external perimeter or internal network
- White-box testing whereby OpenSky and the client review and discuss external and internal network design and implementation
- Hybrid testing of both Black-box and White-box, whereby initial testing is provided as a Black-box and eventually shifts to a White-box at a predetermined time within the testing cycle.

Application Security Testing

There has been a noticeable rise in web application attacks across industries. With applications becoming ever more complex and including more access to privileged and sensitive information, it is no surprise that applications have become the target of cybercrime. It is critical to perform ongoing dynamic and static assessment of applications, APIs and web services to truly ensure they can withstand today's cyber-attacks.

Dynamic Application Security Testing

Performing automated dynamic assessments of applications is a great starting point. Manually validating automated findings is a required next step. However, automated tools can only identify some of the vulnerability types that affect modern-day applications. These tools can struggle or even fail when attempting to identify complex vulnerabilities. Many classes of attack, including authentication bypasses, access control weaknesses, Cross-Site Request Forgery vulnerabilities, and logic flow issues, are often missed by simple automated scanning.

OpenSky's experienced testers know where to look for vulnerabilities that automated tools will always miss and perform in-depth manual testing in these areas. OpenSky has a wealth of experience testing all types of applications from up and coming startups to massive internal applications. For each DAST assessment, OpenSky takes the time to understand how the application is used, and often leverages that information to reach and understand functional areas that traditional automated scanners barely touch. This could include multi-tiered access controls, multi-stepped business processes, SAML or OAUTH authentication, and much more.

OpenSky's DAST reports contain application-specific business risk language and recommendations, including steps to reproduce vulnerabilities identified so development and QA teams can easily re-test deployed fixes.

Dynamic Application Testing includes:

- Automated Application Security Assessment to identify potential areas of concern and low hanging vulnerabilities
- Analysis of automated findings for removal of false positives
- In-depth manual testing in the following categories: Authentication, Access Controls, Session Management, Input Validation, Error Handling, Logic Testing, Client Side Testing
- Manual testing of Web Services & APIs identified as in scope for assessment
- Controlled exploitation of vulnerabilities to demonstrate risk and severity
- Analysis and custom rating of Risk to system and business
- Actionable recommendations for remediation and/or mitigation

Static Application Security Testing

Performing automated static analysis against the application code base is a quick way to identify potential issues and vulnerabilities. However, this often falls short. Automated tools frequently work off signature and keyword matching, which leaves them open to missing vulnerabilities within the code. OpenSky testers add value through manual testing by analyzing the code for potential intellectual property (within the code), dead code, hard coded passwords and credentials, poor code quality and logging mechanisms.

OpenSky testers implement a combination of commercial, OpenSource and custom built tools and scripts to provide an automated scan of the code. Using these findings as a baseline of the application, further manual testing and analysis is performed to identify additional vulnerabilities and issues. The testers then apply their experience and expertise to the risk

analysis of the findings and provide practical recommendations for remediation.

Static Application Testing includes:

- Automated static analysis to identify potential areas of concern and low hanging vulnerabilities
- Analysis of automated findings for removal of false positives
- In-depth manual testing and code analysis to identify potential threat vectors within the code
- Analysis and custom rating of risk to system and business
- Actionable recommendations for remediation and/or mitigation

Purple Team Testing

A collective Purple Team is established when the Ethical Hacking Team (Red Team) and the Security Operations Team (Blue Team) work together to achieve their respective objectives to test the organization's security and responses in a manner that is safe and controlled. OpenSky offers collaborative purple team testing in the form of table top exercises, functional exercises, and collaborative penetration testing. During this testing, OpenSky performs the lead role for the Ethical Hacking Team.

Table Top Exercises

Tabletop exercises are discussion-based exercises where the Ethical Hacking Team meets with Security Operations Personnel, and potentially other corporate stakeholders, to discuss and review the organization's preparedness for specific types of security incidents.

A facilitator from the Ethical Hacking Team presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants related to security controls, roles, responsibilities, processes, coordination, and decision-making.

Tabletop exercises are conducted in an informal environment, with the facilitator guiding participants through a discussion designed to meet pre-defined objectives. One or more scenarios may be discussed during a single tabletop exercise. The duration of a tabletop exercise (typically two to four hours) varies depending on the audience, the topic being exercised, and the exercise objectives.

Tabletop exercises are a cost-effective way to validate security controls and processes, raise awareness of roles, communication, and coordination during an incident, and identify opportunities for improvement related to incident prevention, detection and response.

A tabletop exercise is discussion-based only and does not involve any technical simulation or testing. Tabletop exercise may generate lessons learned or areas of improvement documentation as well inspire playbooks to be used for real-world incidents.

Although tabletop exercises will focus on likely threats or scenarios faced by the organization, occasional exercises should also cover low likelihood, high impact scenarios.

Table Top Exercise consist of the following activities:

- Evaluate Need and Create Schedule
- Design the Tabletop Exercise Event
- Develop the Tabletop Exercise Material
- Conduct the Tabletop Exercise
- Evaluate the Exercise

Functional Exercises

Functional exercises are technical exercises where the Ethical Hacking Team simulates a security incident, or aspects of a security incident, to validate the effectiveness of specific security controls and the related operation capabilities for prevention, detection, and response.

Functional exercises typically do not simulate entire attack chains, in the manner of penetration testing, but rather focus on testing the effectiveness of specific security controls and capabilities through simulating the relevant parts of the attack chain necessary to test the targeted control.

Functional exercises vary in complexity and duration based on the specific scope of the project and may last hours or weeks.

The Ethical Hacking Team may conduct functional exercises with Security Operations personnel aware of the exercise and actively participating across all testing phases. Alternatively, this service may initially be conducted without the knowledge of Security Operations personnel, and then include them in latter phases of the exercise.

Functional Exercises include:

- Evaluate Need and Create Schedule
- Design the Functional Exercise Event
- Develop the Functional Exercise Material
- Conduct the Functional Exercise
- Evaluate the Functional Exercise

Penetration Testing

Purple team penetration testing is conducted using OpenSky's penetration testing methodology, but is performed with participation of one or more members of the security operations team. The type and frequency of collaboration with the Blue Team can vary and is determined at project initiation.

Mix & Match Services

Every organization's needs are different. OpenSky can work with you to determine which of our services or combination of services is the best fit. OpenSky's rapid delivery of services reduces reporting and analysis time, allowing for a lower price-point while still providing outstanding value.

Customized Service

While OpenSky has robust service offerings, sometimes something special is needed. Ask your sales representative to setup a call with one of OpenSky's experienced experts to help build a custom fitted service or ongoing services to meet your needs.

OPENSKY
A TÜV Rheinland Company

DIGITAL ENTERPRISE PROTECTED

www.openskycorp.com