Managed.sa

Cybersecurity Orchestrator

Vulnerability and Risk-Focused Assessments

Threat Simulation and Response Testing

Compliance and Best Practices Assessments

Assurance

Operations Services

Managed.sa
Cybersecurity Orchestrator

Vulnerability Assessment

Risk Assessment

Cloud Security Assessment

Application Security Assessment

IoT Security Assessment

Vulnerability and Risk-Focused Assessments

Operations Services

Managed.sa
Cybersecurity Orchestrator

Vulnerability Assessment

1. Comprehensive scanning and identification of vulnerabilities.
2. Prioritization of vulnerabilities based on risk and impact.
3. Continuous vulnerability monitoring.

Managed.sa
Cybersecurity Orchestrator

Vulnerability Assessment is a service that helps organizations identify and assess potential vulnerabilities in their systems, networks, and applications. The goal of vulnerability assessment is to identify and prioritize vulnerabilities that could be exploited by an attacker and provide recommendations for mitigating or eliminating those vulnerabilities. The service typically includes the following:

1

Discover

Identification of all systems, networks, and applications within the scope of the assessment.

2

Scanning

Use of automated tools to scan the identified systems, networks, and applications for known vulnerabilities.

3

Analysis

Evaluation of the results of the scan to determine the potential impact of each vulnerability, and the ease of exploitation.

4

Reporting

Generation of a report that includes an overview of the assessment, a list of vulnerabilities identified, and recommendations for mitigating or eliminating those vulnerabilities.

Key Features

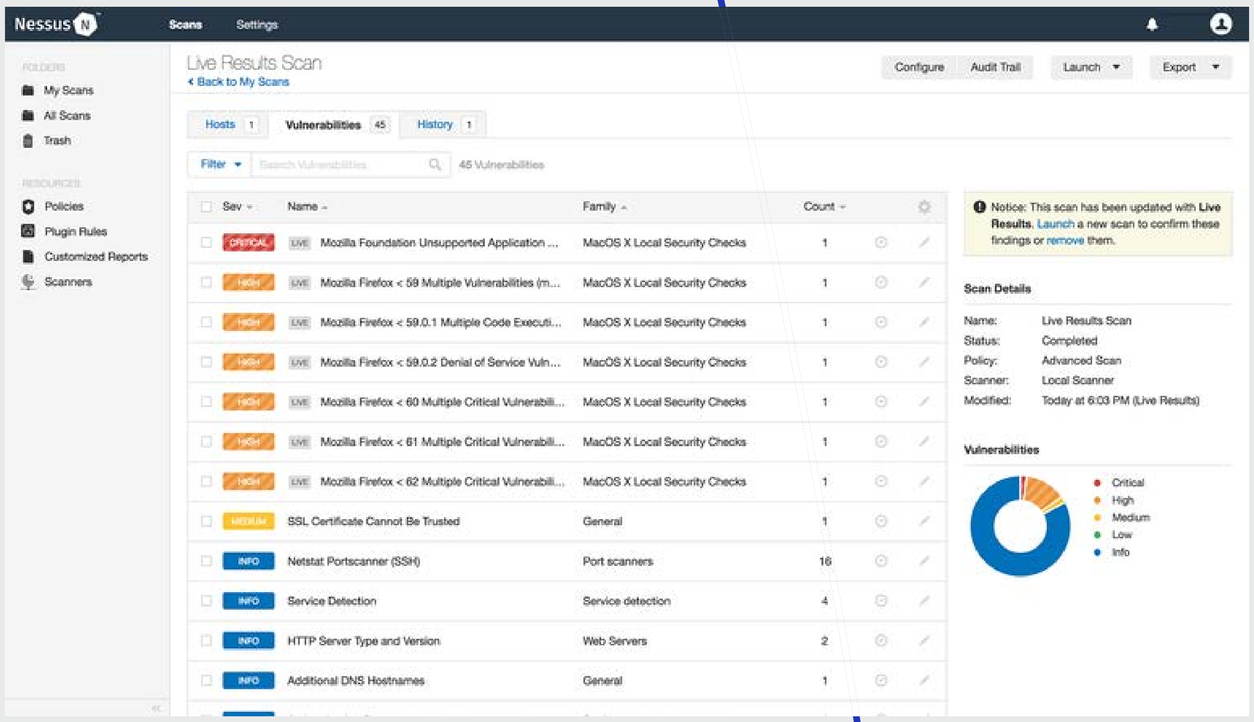
1. **Automated scanning**
   Use of automated tools to scan systems, networks, and applications for known vulnerabilities.
2. **Comprehensive coverage**
   Identification of all systems, networks, and applications within the scope of the assessment.
3. **In-depth analysis**
   Evaluation of the results of the scan to determine the potential impact of each vulnerability, and the ease of exploitation.
4. **Clear and actionable reporting**
   A report that includes an overview of the assessment, a list of vulnerabilities identified, and recommendations for mitigating or eliminating those vulnerabilities.
5. **Scalability**
   Ability to handle a large number of devices, networks and applications.
6. **Customization**
   Ability to be customized to the customer's specific needs.
7. **Integration**
   Ability to integrate with other security tools that the customer already uses.
8. **In-depth analysis**
   Evaluation of the results of the scan to determine the potential impact of each vulnerability, and the ease of exploitation.
9. **Risk prioritization**
   Prioritization of vulnerabilities based on their risk level, to help customers prioritize their remediation efforts.

Managed.sa
Cybersecurity Orchestrator

Methodologies and Tools

Our Vulnerability Assessment service uses a combination of **automated** scanning tools and **manual** testing methods to identify vulnerabilities in systems, networks, and applications. We perform both **external** and internal scans, using a variety of protocols and ports to ensure comprehensive coverage. Our scans include checks for a wide range of vulnerabilities, including those related to network security, web application security, and database security.

During our assessment we will use the professional version of Nessus®, Nessus Professional automates point-in-time assessments to help quickly identify and fix vulnerabilities, including software flaws, missing patches, malware, and misconfigurations, across a variety of operating systems, devices and applications. Virtual Environment Monitoring. Mobile Device Security.



Managed.sa
Cybersecurity Orchestrator

Risk Assessment

Transform Your Security Decision-Making

Make confident security decisions backed by data-driven risk insights. Our comprehensive Risk Assessment service helps you understand, quantify, and prioritize security risks across your organization's entire technology landscape.

Managed.sa
Cybersecurity Orchestrator

Expert Risk Analysis That Matters

Our seasoned security professionals analyze your organization from every angle:

1 **Asset Protection**

We identify and evaluate your critical business assets - from sensitive data to crucial infrastructure - ensuring nothing is overlooked in your risk landscape.

2 **Threat Intelligence**

Stay ahead of threats with expert analysis of current and emerging risks specific to your industry and technology environment.

3 **Vulnerability Discovery**

Uncover hidden weaknesses across your systems, applications, and processes before they can be exploited.

Why Choose Our Risk Assessment Service?

Data-Driven Decisions

Transform complex risk data into clear, actionable insights that help you make informed security investments.

1

Business-Aligned Analysis

We evaluate risks in the context of your business objectives, ensuring security enhances rather than hinders your operations.

2

Clear Path Forward

Receive practical, prioritized recommendations that help you build a stronger security posture step by step.

3

What You'll Receive

1 **Executive Insights**

Clear, board-ready reports that communicate your risk landscape and recommended actions at a strategic level.

2 **Technical Analysis**

Detailed findings and recommendations that give your technical teams the specifics they need for implementation.

2 **Strategic Roadmap**

A prioritized action plan that helps you address risks systematically and cost-effectively.

Managed.sa
Cybersecurity Orchestrator

Your Security Journey Starts Here

Partner with us to:

- Make smarter security investments
- Meet compliance requirements confidently
- Build stakeholder trust
- Strengthen your security foundation

Turn risk assessment into your competitive advantage. Contact us today to start building a stronger, more resilient security program.

Managed.sa
Cybersecurity Orchestrator

Cloud Security Testing

Assessment of cloud service providers (e.g., AWS, Azure, Google Cloud).

1

Testing cloud confi gurations, storage, and identity management.

2

Analysis of cloud-based applications and services.

3

Application Security Assessment

Secure Your Applications from Code to Cloud

In today's digital landscape, your applications are the gateway to your business. Our Application Security Assessment service helps you identify and eliminate security vulnerabilities before attackers can exploit them, protecting your valuable data and maintaining customer trust.

1. **Testing for OWASP Top 10 vulnerabilities and beyond.**
2. **Assessment of web applications, APIs, and web services.**
3. **Analysis of authentication, authorization, and session management.**

Managed.sa
Cybersecurity Orchestrator

Comprehensive Application Security Testing

1. **Full-Stack Security Analysis**
   From front-end interfaces to back-end systems, we examine every layer of your applications to uncover potential security weaknesses.
2. **Modern Architecture Coverage**
   Whether you're running traditional applications, cloud-native systems, containerized microservices, or mobile apps, our assessment adapts to your technology stack.
3. **Secure Development Lifecycle**
   Integrate security from the start with assessments that align with your development process, from design reviews to production deployment.

What Sets Us Apart

1. **Beyond Automated Scanning**
   We combine advanced security tools with expert manual testing to find vulnerabilities that automated scanners miss.
2. **Business Logic Analysis**
   Our experts think like attackers, identifying security flaws in your application's business logic and workflow.
3. **Actionable Remediation**
   Receive detailed guidance that helps your developers fix vulnerabilities quickly and effectively, complete with code examples and best practices.

Our Assessment Coverage

Security Architecture Review

1. Authentication and authorization mechanisms
2. Session management
3. Data protection controls
4. API security
5. Cloud service configuration
6. Mobile app architecture

Dynamic Application Testing

1. Injection flaws
2. Cross-site scripting
3. Authentication bypasses
4. Access control weaknesses
5. API vulnerabilities
6. Mobile runtime analysis

Secure Code Review

1. Security bug detection
2. Third-party component analysis
3. Cryptographic implementation
4. Secure coding patterns
5. Framework-specific vulnerabilities
6. Mobile SDK security review

Our Assessment Coverage

Mobile Application Security

1. Platform-specific security controls (iOS/Android)
2. Local data storage security
3. Runtime manipulation protection
4. Secure communication analysis
5. Mobile malware detection
6. App store compliance requirements
7. Anti-reverse engineering controls
8. Biometric authentication security
9. Mobile payment security
10. Mobile API security

Deliverables That Drive Action

1
Executive Summary

Clear insights into your application security posture and risk exposure for leadership teams.

2
Technical Report

Detailed findings and recommendations that give your developers exactly what they need to fix issues.

3
Remediation Roadmap

Prioritized action items that help you address vulnerabilities systematically and efficiently.

4
Mobile Security Guidelines

Platform-specific security best practices and configuration guides for mobile development teams.

Benefits That Matter

- Protect sensitive customer data across all platforms
- Maintain compliance with security standards and app store requirements
- Reduce the cost of fixing security issues
- Build customer trust through secure applications
- Speed up secure application delivery
- Ensure consistent security across web and mobile platforms
- Meet mobile-specific regulatory requirements
- Protect your brand reputation in mobile app stores

Your Applications, Our Expertise

Whether you're developing web applications, mobile apps, or both, our Application Security Assessment helps you deliver secure, reliable software that your customers can trust.

Managed.sa
Cybersecurity Orchestrator

Threat Simulation and Response Testing

Operations Services

Penetration Testing

Red Teaming

Social Engineering Assessment

Incident Response Readiness Assessment

Managed.sa
Cybersecurity Orchestrator

Penetration Testing

Physical Penetration Testing is a comprehensive assessment service that involves a simulated physical attack on an organization's physical assets, including buildings, data centers, and other facilities. The objective of this service is to identify vulnerabilities in the physical security controls and provide recommendations for improvements.

1. **Testing physical security controls (locks, cameras, alarms).**
2. **Access control assessment and bypass techniques.**
3. **Social engineering for physical access.**

Managed.sa
Cybersecurity Orchestrator

Key Features

1. Detailed reconnaissance and intelligence gathering to simulate realistic threat actors
2. Social engineering and tailgating assessments
3. Physical security control testing and bypass techniques
4. Assessment of the physical security posture of the organization
5. Comprehensive reporting and recommendations

Methodology

In Aim to conducting our social engineering assessment, we employed a structured methodology designed to simulate various social engineering attacks, identify vulnerabilities, and assess the organization's susceptibility to these threats.

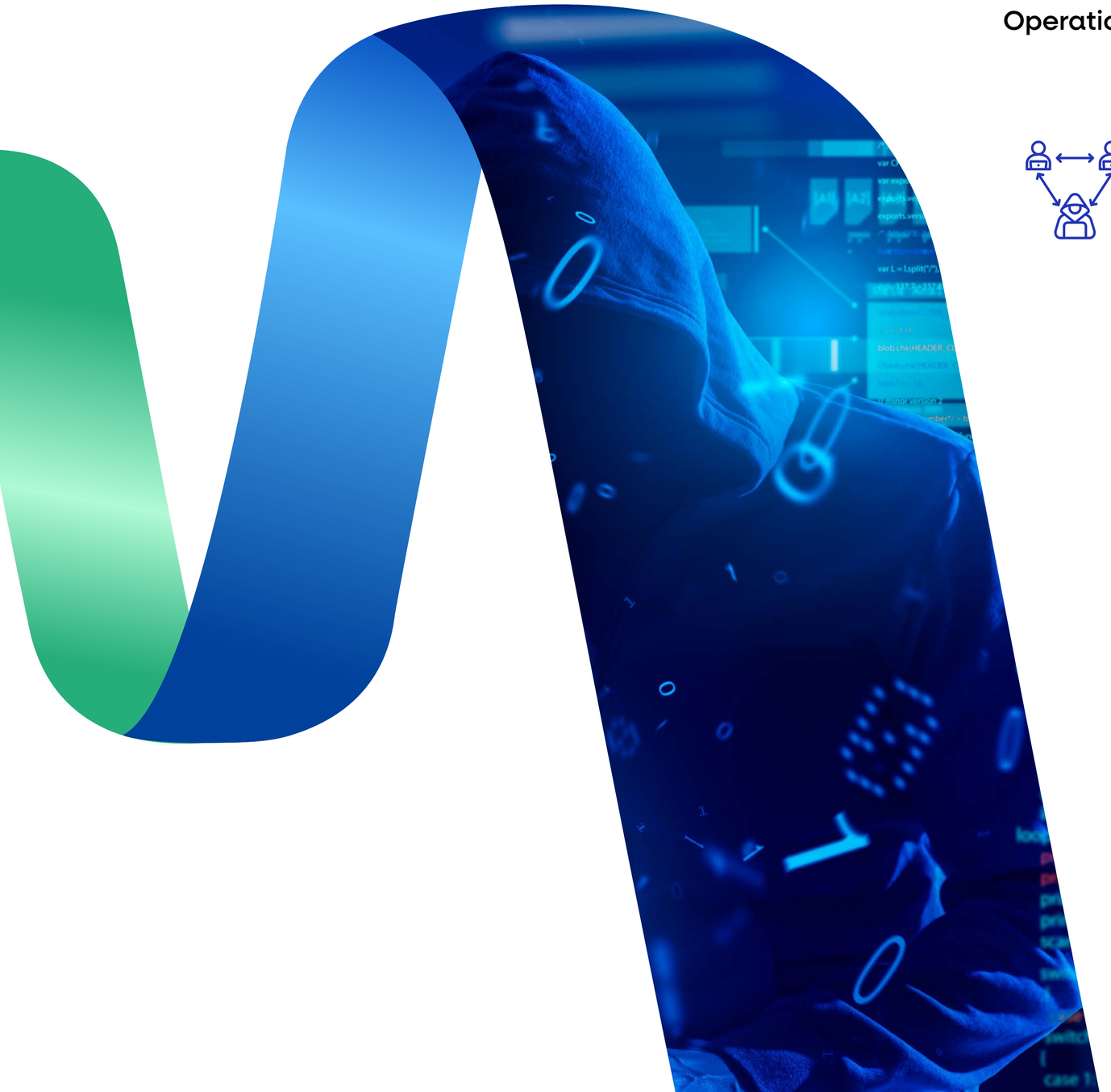
Scope

The services scope of work covers all Physical assets of organization.

Deliverables

One comprehensive report for all vulnerabilities and information gathered during the assessment. The report will include recommendations and step by step Proof of concept.

Managed.Sa
Cybersecurity Orchestrator



Red Teaming

Our Read Teaming is a comprehensive security assessment service that simulates a real-world cyber-attack on an organization's network infrastructure. The goal of the service is to identify vulnerabilities that could be exploited by an attacker and provide recommendations for mitigating or eliminating those vulnerabilities. This service is designed to mimic the techniques used by real-world attackers and is used to improve the organization's overall security posture.

1. **Simulated attacks mimicking real-world threat actors.**
2. **Full-scope assessments including physical, social engineering, and digital attacks.**
3. **Testing incident response capabilities and detection measures.**

Managed.sa
Cybersecurity Orchestrator

Operations • Threat Simulation and Response Testing • **Red Teaming**

Key Features

1. **Simulate External threats.**
2. **Minimized false positive.**
3. **Detailed report.**
4. **Aligned with MITRE ATT&CK®.**
5. **Remediation Suggestions.**

Methodology

Our assessments methodologies for external assessments can vary depending on the specific goals and objectives of the assessment, but generally, they include the following steps:

1. **Simulate External threats.**
2. **Minimized false positive.**
3. **Detailed report.**
4. **Aligned with MITRE ATT&CK®.**
5. **Remediation Suggestions.**

Managed.sa
Cybersecurity Orchestrator

1 Reconnaissance

Multiple passive information gathering methods will be used such as:

1. **Footprinting.**
2. **Search engine reconnaissance.**
3. **Archive search, online directories, locations, and webcams.**
4. **Malicious websites and websites used for adding the attacker.**
5. **Shared hosting enumeration.**
6. **Gateway device enumeration.**
7. **Source code analyses.**

2 Enumeration

Multiple active information gathering methods will be used such as:

1. Firewall / IPS behavioral analyses.
2. Detection of different types of port scans.
3. Detection of packet fragmentation.
4. Detection of sweep ICMP attempts.
5. Service detection.
6. Web based service enumeration and banner grabbing.
7. Mapping and banner grabbing of common services.
8. FTP, telnet, SSH and SMTP
9. Database related ports (oracle TNS listeners, MSSQL and MySQL ports)
10. Mapping and banner grabbing of common network services (Blackbox)
11. Network Device management services (telnet, HTTP management consoles ...etc.)
12. Detection of VPN services
13. Mapping other miscellaneous devices and services

3 Threat Analysis

This phase will cover:

1. **Manual verification of known vulnerabilities on services detected during Enumeration threats phase.**
2. **Assessment of service functionality and misconfiguration**
3. **Detecting password protected services.**
4. **Automated scanning**
5. **OWASP top 10 based automated scan on web-based services**

4 Exploitation

Multiple exploitation methods will be covered such as:

1. **Exploitation of manually discovered vulnerabilities.**
2. **Exploitation of service functionality and misconfiguration**
3. **Performing brute force attacks**
4. **Exploitation of vulnerabilities detected by the automated scanner.**
5. **Exploitation of OWASP top 10 findings**

5 Reporting

This step involves generating a report that includes an overview of the assessment, a list of vulnerabilities identified, and recommendations for mitigating or eliminating those vulnerabilities.

Managed.sa
Cybersecurity Orchestrator

References MITRE ATT&CK®

MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. Our solution complies to the MITRE ATT&CK® framework and covers, but is not limited to, the following tactics:

It is important to note that the service is not limited to these specific tactics and techniques and that the scope and focus of the engagement can be tailored to the specific needs of the customers.

ID	Name	Description
TA0001	Initial Access	Techniques used to gain a foothold in a targeted system or network.
TA0002	Execution	Techniques used to execute malicious code on a target system or network.
TA0003	Persistence	Techniques used to maintain access to a target system or network after initial compromise.
TA0004	Privilege Escalation	Techniques used to obtain higher privileges on a target system or network, often by exploiting vulnerabilities.
TA0005	Defense Evasion	Techniques used to bypass or undermine security measures on a target system or network.
TA0006	Credential Access	Techniques used to steal or collect login credentials from a target system or network.
TA0007	Discovery	Techniques used to gather information about a target system or network, including its infrastructure, applications, and user accounts.
TA0008	Lateral Movement	Techniques used to move through a target system or network, often to gain access to valuable assets or systems.
TA0009	Collection	Techniques used to gather data or information from a target system or network, including user files, network traffic, and system logs.
TA00010	Exfiltration	Techniques used to extract data or information from a target system or network and transfer it to an external system controlled by the attacker.
TA00011	Command and Control	Techniques used to establish and maintain communication channels between a target system or network and an external system controlled by the attacker.

Managed.sa
Cybersecurity Orchestrator

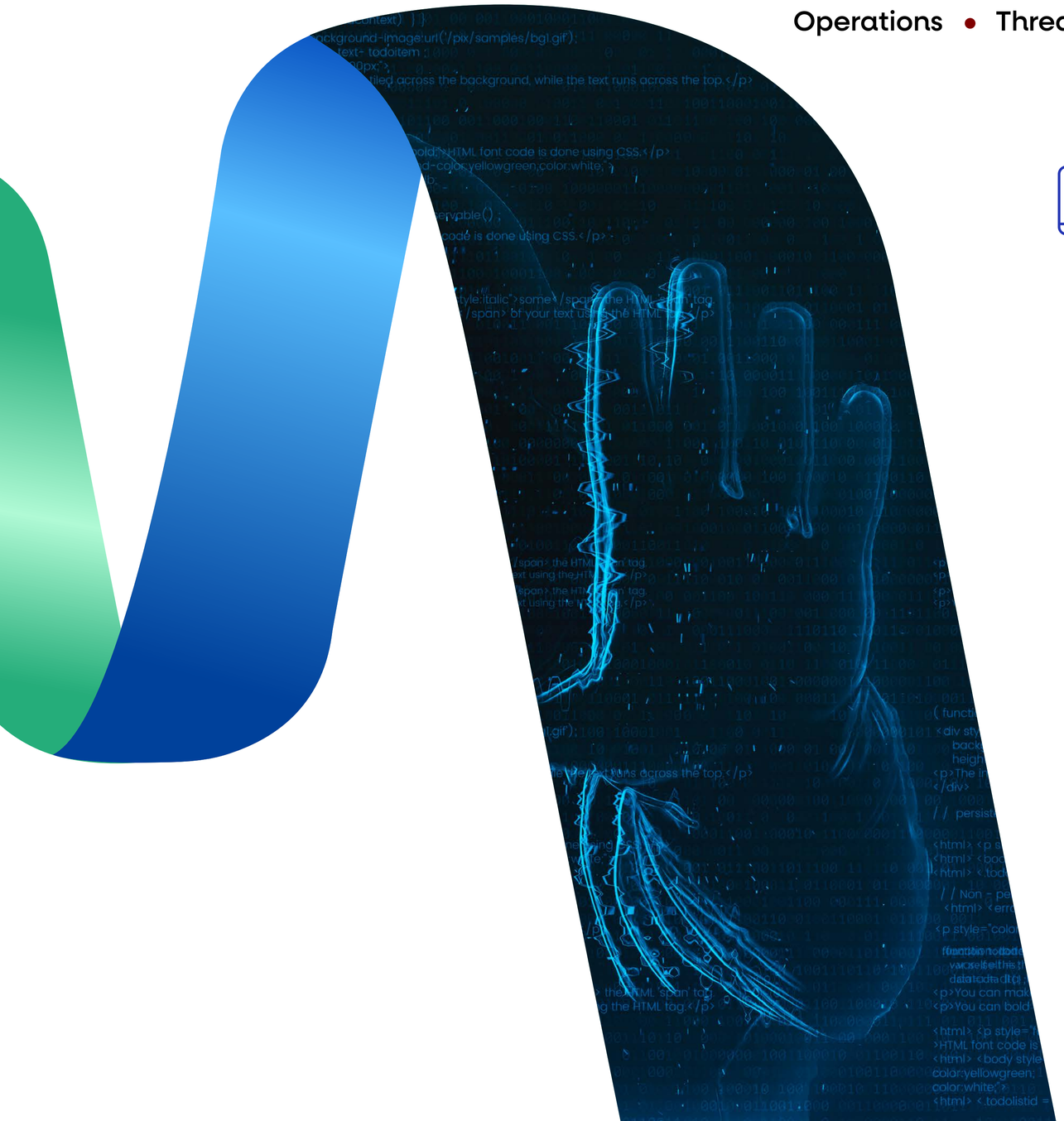
References OWASP™ Top 10 - Web Applications Vulnerabilities

For Web Applications Penetration Testing we'll be covering The Open Web Application Security Project™ (OWASP™) list for top 10 web applications vulnerabilities in 2021 listed below:

NO.	Category
A01:2021	Broken Access Control
A02:2021	Cryptographic Failures
A03:2021	Injection
A04:2021	Insecure Design
A05:2021	Security Misconfiguration
A06:2021	Vulnerable and Outdated Components
A07:2021	Identification and Authentication Failures
A08:2021	Software and Data Integrity Failures
A09:2021	Security Logging and Monitoring Failures
A10:2021	Server-Side Request Forgery

References OSINT Framework

OSINT is a process of identifying, harvesting, processing, analyzing, and reporting data obtained from publicly available sources for intelligence purposes. During this service we will conduct an Open-source intelligence against the targeted organization using the **OSINT framework** to identify what is the possible attack surfaces.



Social Engineering

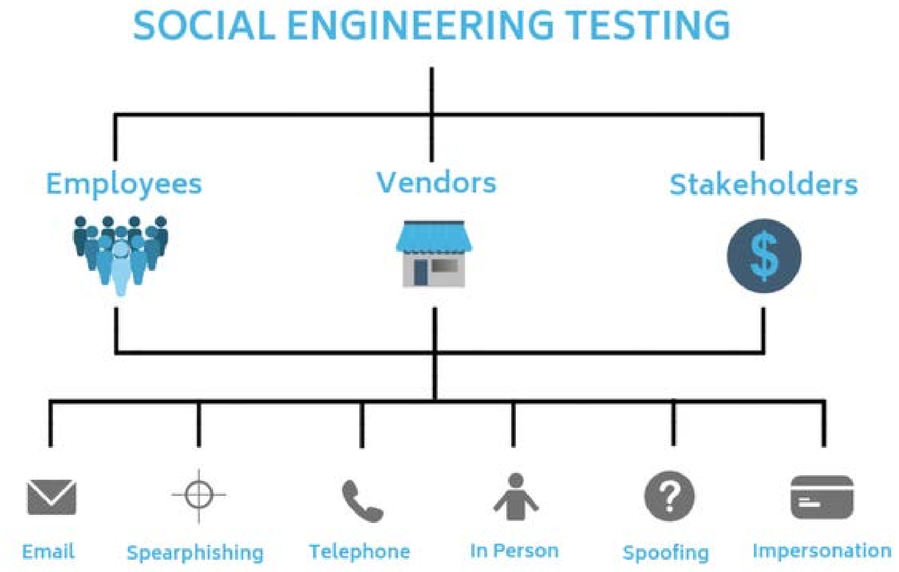
Our Social Engineering Service aims to assess the level of an organization's security awareness by simulating real-world social engineering attacks. Our team of experienced social engineers will work with your organization to identify potential vulnerabilities that could be exploited by attackers, including phishing, pretexting, baiting, and other social engineering tactics. This service helps organizations identify areas where employee awareness and training can be improved, in order to better protect against social engineering attacks.

1. **Phishing simulations and email spear-phishing.**
2. **Pretexting and vishing (voice phishing) attacks.**
3. **Physical security testing (e.g., tailgating, badge cloning).**

Managed.sa
Cybersecurity Orchestrator

Our Social Engineering Service includes the following types of assessments:

1. Email Phishing Assessment
2. Phone Phishing Assessment
3. Pretexting Assessment
4. Baiting Assessment



Managed.sa
Cybersecurity Orchestrator

Key Features

1. **Realistic, customized social engineering simulations**
2. **Experienced social engineering team**
3. **Detailed reporting on identified vulnerabilities and areas for improvement**
4. **Analysis of employee security awareness and training needs**
5. **Optional employee training and awareness sessions**

Methodology

In Aim to conducting our social engineering assessment, we employed a structured methodology designed to simulate various social engineering attacks, identify vulnerabilities, and assess the organization's susceptibility to these threats. The following sections outline the key components of our social engineering methodology

Scope

Depends on the number of employees, objectives and customer industry.

References

OSINT Framework

OSINT is a process of identifying, harvesting, processing, analyzing, and reporting data obtained from publicly available sources for intelligence purposes. During this service we will conduct an Open-source intelligence against the targeted organization using the **OSINT framework** to identify what is the possible attack surfaces.

Managed.sa
Cybersecurity Orchestrator

Incident Response Readiness Assessment

Be Prepared When Seconds Count

In today's threat landscape, it's not if but when a cyber incident will occur. Our Incident Response Readiness Assessment ensures your organization is prepared to detect, respond, and recover effectively when every moment matters.

Evaluate Your Cyber Defense Capabilities

1. **Detection Effectiveness**
   Assess your ability to identify security incidents across your infrastructure before they escalate into major breaches.
2. **Response Capabilities**
   Test your incident response procedures, team coordination, and crisis management readiness through real-world scenarios.
3. **Recovery Readiness**
   Validate your business continuity plans and ensure minimal disruption to critical operations during security incidents.

Managed.sa
Cybersecurity Orchestrator

What Sets Our Assessment Apart

1. Real-World Scenarios

Experience customized incident simulations based on current threats targeting your industry.

2. Cross-Functional Evaluation

Test coordination between IT, security, legal, communications, and executive teams during crisis situations.

3. Actionable Results

Receive practical recommendations to strengthen your incident response capabilities and close critical gaps.

Key Assessment Areas

1

People

- Incident response team roles and responsibilities
- Staff awareness and training effectiveness
- Crisis communication readiness

2

Process

- Incident response procedures and playbooks
- Escalation and notification protocols
- Documentation and reporting mechanisms

3

Technology

- Security monitoring capabilities
- Incident detection tools and systems
- Response and recovery technologies

Managed.sa
Cybersecurity Orchestrator

Deliverables That Drive Improvement

Readiness Score

Quantified evaluation of your current incident response capabilities against industry benchmarks.

1

Gap Analysis

Detailed assessment of strengths and weaknesses in your incident response program.

2

Enhancement Roadmap

Prioritized recommendations to strengthen your incident response readiness.

3

Transform Response into Resilience

Partner with us to:

- Minimize incident impact and recovery time
- Strengthen team coordination during crises
- Protect your reputation and customer trust
- Meet regulatory compliance requirements

Contact us today to assess and enhance your incident response capabilities.

Managed.sa
Cybersecurity Orchestrator

Cybersecurity Compliance Assessment

Security Configuration Assessment

Zero Trust Assessment

Threat Modeling

Compliance and Best Practices Assessments

Operations Services

Managed.sa
Cybersecurity Orchestrator

Cybersecurity Compliance Assessment

Navigate Complex Security Requirements with Confidence

Stay ahead of evolving cybersecurity regulations and standards. Our Compliance Assessment service helps organizations achieve and maintain compliance with leading security frameworks while strengthening their overall security posture.

Framework Coverage

We provide comprehensive assessment and guidance across major cybersecurity frameworks:

1 NIST Cybersecurity Framework
Align your security program with industry-leading practices for identifying, protecting, detecting, responding to, and recovering from cyber threats.

2 ISO 27001/27002
Evaluate your information security management system against international best practices for comprehensive security control implementation.

3 CIS Controls
Assess your security measures against proven, prioritized best practices developed by the Center for Internet Security.

4 SOC 2
Validate your security, availability, processing integrity, confidentiality, and privacy controls against AICPA Trust Services Criteria.

5 Cloud Security Standards
Ensure compliance with cloud-specific frameworks including CSA STAR, ISO 27017/27018, and major cloud provider security requirements.

Managed.sa
Cybersecurity Orchestrator

Beyond Checkbox Compliance

1. Strategic Alignment

Transform compliance requirements into business advantages through strategic security improvements.

2. Integrated Assessment

Get a unified view of your compliance status across multiple frameworks, eliminating redundant assessments.

3. Continuous Monitoring

Stay compliant with real-time visibility into your security controls and compliance status.

What Sets Us Apart

1

Technical Depth

Our assessors combine deep technical expertise with thorough understanding of compliance requirements.

2

Practical Guidance

Receive clear, actionable recommendations that help you achieve and maintain compliance efficiently.

3

Future-Ready Approach

Stay ahead of evolving standards with forward-looking guidance and continuous compliance monitoring.

Managed.sa
Cybersecurity Orchestrator

Deliverables You Can Trust

1. Compliance Dashboard

Get clear visibility into your compliance status across all relevant frameworks.

2. Gap Analysis

Detailed assessment of your current state against framework requirements with prioritized remediation guidance.

3. Implementation Roadmap

Strategic plan for achieving and maintaining compliance across multiple frameworks.

4. Evidence Portfolio

Comprehensive documentation package supporting your compliance claims.

Business Impact

Partner with us to:

- Reduce audit preparation time and costs
- Streamline multiple compliance requirements
- Build customer and stakeholder trust
- Strengthen your overall security program
- Stay ahead of regulatory changes

Managed.sa
Cybersecurity Orchestrator

Security Configuration Assessment

Optimize Your Security Controls with Expert Configuration Assessment

Don't let misconfigured systems be your security weakness. Our Security Configuration Assessment service helps you align your technology configurations with industry best practices, hardening your defenses against cyber threats.

Beyond Basic Security Checks

Our comprehensive assessment evaluates every layer of your technology stack:

1 System Hardening
Deep analysis of operating systems, databases, and network devices against industry-leading security benchmarks and hardening guidelines.

2 Cloud Configuration
Thorough review of cloud service configurations to protect against common misconfigurations and security gaps in your cloud environment.

3 Security Controls
Detailed assessment of security tools and controls to ensure they're configured for maximum effectiveness.

4 Access Management
In-depth evaluation of user privileges, access controls, and authentication mechanisms to prevent unauthorized access.

Managed.sa
Cybersecurity Orchestrator

Why Our Configuration Assessment Matters

1. Prevent Security Gaps

Identify and fix misconfigurations before they become security incidents.

2. Optimize Performance

Balance security with system performance through proven configuration best practices.

3. Ensure Compliance

Meet regulatory requirements with configurations that align with compliance frameworks.

4. Reduce Risk

Minimize your attack surface through properly configured systems and security controls.

What Sets Us Apart

01

Industry Benchmarks

We evaluate against recognized standards including CIS Benchmarks, NIST guidelines, and vendor security recommendations.

02

Automated + Manual Analysis

Combine automated configuration scanning with expert manual review for comprehensive coverage.

03

Practical Recommendations

Receive clear, actionable guidance for improving your security configurations.

04

Business Context

Configuration recommendations that consider your operational needs and business requirements.

Managed.sa
Cybersecurity Orchestrator

Deliverables You Can Trust

1. Executive Summary

Clear overview of your configuration status and priority improvements needed.

2. Technical Analysis

Detailed findings and specific remediation steps for your technical teams.

3. Remediation Roadmap

Prioritized plan for implementing configuration improvements.

4. Best Practices Guide

Custom documentation for maintaining secure configurations over time.

Secure Your Foundation

Partner with us to:

- Strengthen your security baseline
- Implement proven security controls
- Reduce configuration-related vulnerabilities
- Build a more resilient infrastructure

Managed.sa
Cybersecurity Orchestrator

Zero Trust Assessment

Validate Your Zero Trust Journey

In today's hyperconnected world, traditional security models are no longer enough. Cyber threats are evolving faster than ever, and outdated "trust but verify" approaches leave organizations exposed. Zero Trust—a modern security framework built on the principle of "never trust, always verify"—is the gold standard for safeguarding critical assets, data, and users. But how do you know if your organization is truly aligned with Zero Trust?

Managed.sa
Cybersecurity Orchestrator

Operations • Compliance and Best Practices Assessments • **Zero Trust Assessment**

Our Zero Trust Assessment provides the clarity you need. We evaluate your existing security architecture, policies, and workflows against core Zero Trust principles, identifying gaps and opportunities to strengthen resilience. Whether you're just starting your Zero Trust journey or refining an existing strategy, our assessment delivers actionable insights to help you:

1. **Reduce risk by eliminating overprivileged access and siloed security controls.**
2. **Enhance visibility across users, devices, networks, and workloads.**
3. **Simplify compliance with frameworks like NIST, CISA, and industry-specific regulations.**
4. **Future-proof your defenses against ransomware, insider threats, and sophisticated attacks.**

Why Choose Our Zero Trust Assessment?

1. Proven Expertise

Backed by cybersecurity leaders with deep Zero Trust implementation experience.

2. Tailored Insights

Customized recommendations aligned to your unique infrastructure and business goals.

3. Speed to Value

Prioritized roadmap to accelerate measurable improvements in security maturity.

Transform your security architecture with expert Zero Trust Assessment services. We help organizations evaluate their current posture and build a practical roadmap toward a true Zero Trust environment.

Managed.sa
Cybersecurity Orchestrator

Comprehensive Zero Trust Evaluation

1 Identity & Access

- User authentication and authorization practices.
- Identity governance and lifecycle management.
- Privileged access controls and monitoring.

2 Network Security

- Micro-segmentation effectiveness
- Network access controls
- East-west traffic protection

3 Data Protection

- Data classification and handling
- Encryption implementation
- Access control granularity

4 Application Security

- Application access patterns
- API security controls
- Service-to-service authentication

Why Choose Our Zero Trust Assessment

1 Expert Guidance

Navigate the complexity of Zero Trust implementation with our specialized expertise.

2 Practical Approach

Receive actionable recommendations that align with your business capabilities and goals.

3 Industry Alignment

Assessment based on proven frameworks including NIST SP 800-207 and industry best practices.

4 Clear Roadmap

Get a structured path to achieve Zero Trust maturity across your organization.

Managed.sa
Cybersecurity Orchestrator

What You'll Receive

1. Maturity Assessment

Detailed evaluation of your current Zero Trust capabilities against industry benchmarks.

2. Gap Analysis

Clear identification of areas needing improvement to achieve Zero Trust objectives.

3. Implementation Plan

Prioritized roadmap for enhancing your Zero Trust security posture.

4. Executive Brief

Strategic overview and recommendations for stakeholder alignment.

Transform Your Security Architecture

Partner with us to:

- Validate your Zero Trust strategy
- Identify security gaps
- Prioritize improvements
- Accelerate Zero Trust adoption

Managed.sa
Cybersecurity Orchestrator

Threat Modeling

1. Identification of potential attack vectors and threat actors.
2. Analysis of security controls and risk assessment.
3. Development of threat models and mitigation strategies.

Managed.sa
Cybersecurity Orchestrator

Managed.sa
Cybersecurity Orchestrator

3273 Anas Ibn Malik - Al Sahafah Dist.
Riyadh 13321 - 8347
Kingdom of Saudi Arabia

+966 11 4185222

managed.sa