Integrity360

your **security** in mind

Cyber Security Testing Portfolio Overview

Presentation to <CUSTOMERNAME> DD-MMM-YYY

Integrity360

your **security** in mind

1. Why do Cyber Security Testing?
2. CST Portfolio
    1. Vulnerability Scanning and Assessment Services
    2. Penetration Testing Services
    3. Red Team Services
    4. Audit Services
    5. User Testing and Awareness training
3. Why Integrity360 for Cyber Security Testing?
4. Summary and Next Steps

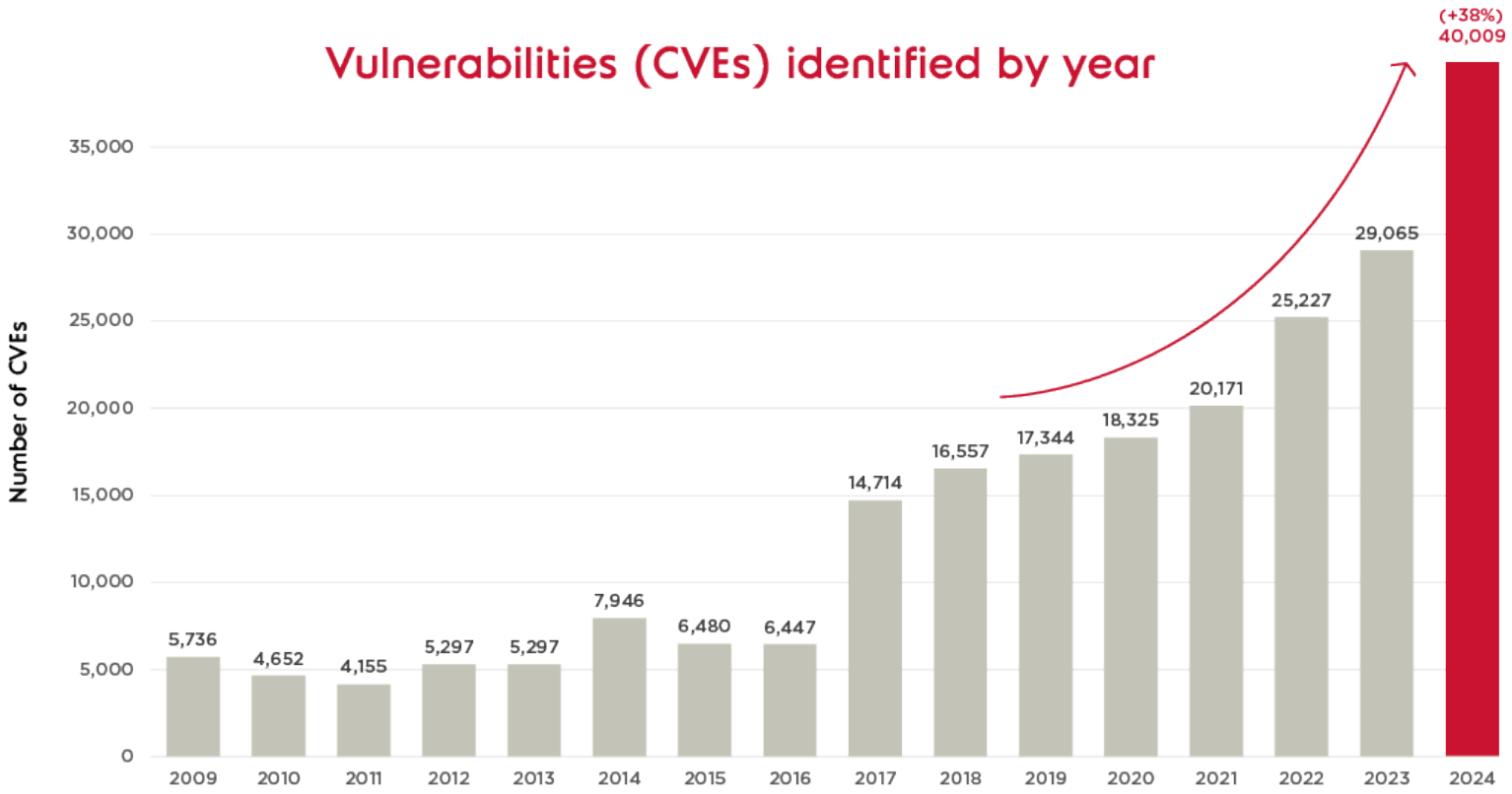
Integrity360

your **security** in mind

Why do Cyber Security Testing?

Integrity360
your security in mind

Why do Cyber Security Testing?



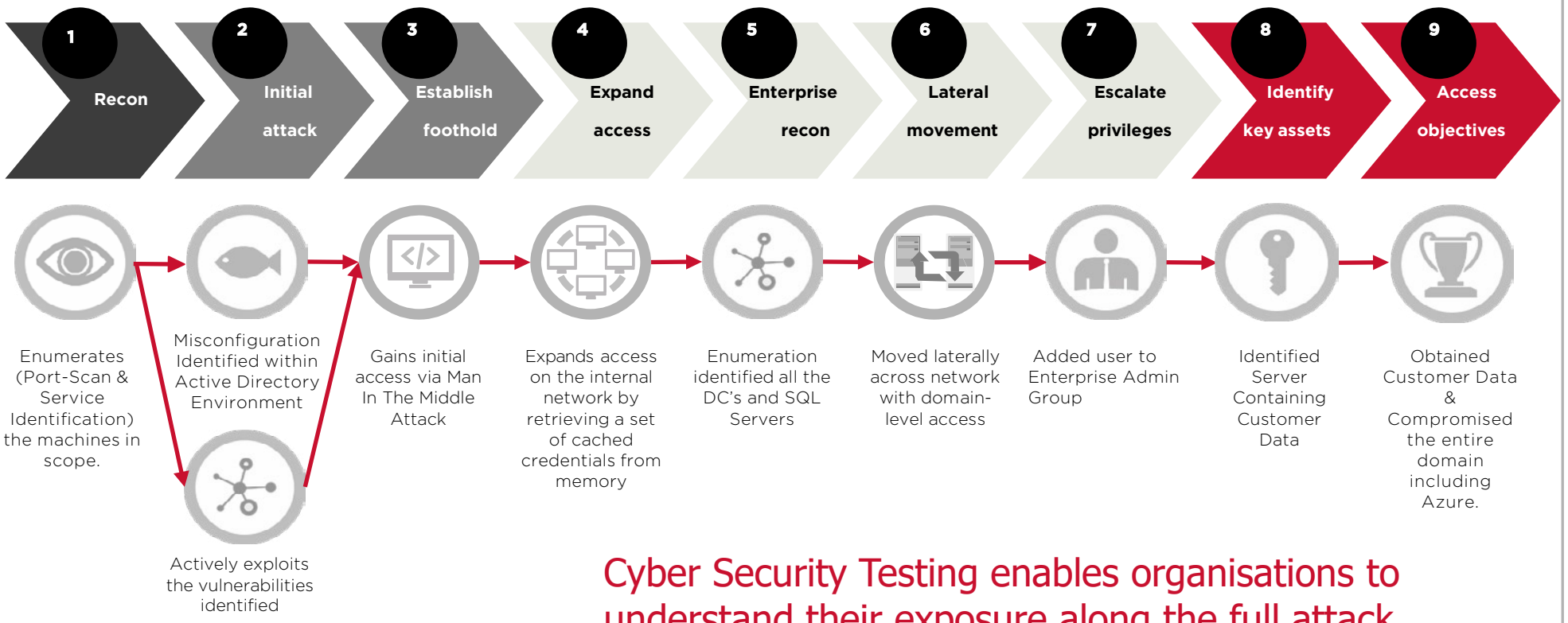
Source: Statista.com & nvd.nist.gov

Regularly testing your exposure and vulnerability to exploit by bad actors is critical for security – as mandated by many Standards and Frameworks such as ISO 27001, PCI DSS, NIST CSF, CIS Controls, Cyber Essentials, HIPAA, and more.

Why do Cyber Security Testing?

Attackers chain exposures to build attack paths

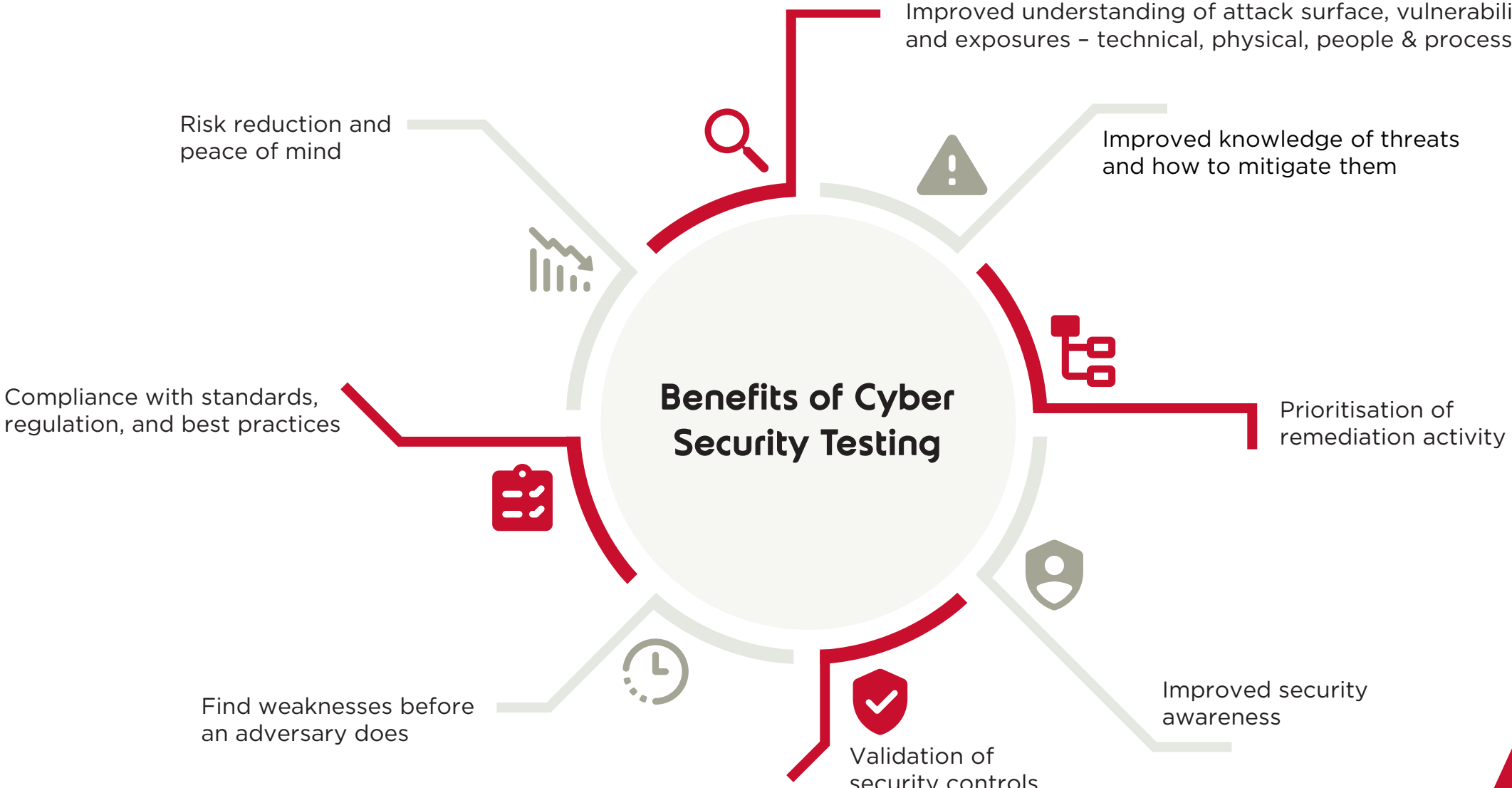
ATTACK PATH



Cyber Security Testing enables organisations to understand their exposure along the full attack path and how they can be addressed

Why do Cyber Security Testing?

Benefits of Cyber Security Testing



Integrity360

your **security** in mind

Cyber Security Testing Portfolio

CST Portfolio

Integrity360
your security in mind

Cyber Security Testing Service Categories

	Auditing	Vulnerability Scanning	Vulnerability Assessment	Penetration Testing	Red Teaming	User Testing & Awareness
Description	Formal review against a standard	Discovery, analysis and reporting on known vulnerabilities	Augmentation of Scanning with human review and interpretation	Authorised simulated attack to evaluate security	Authorised simulated attack using all methods possible	Tests focusing on people and human response to cyber attack methods
Tests Security of..	Infrastructure & Applications (incl source code)	Infrastructure & Applications	Infrastructure & Applications	Infrastructure & Applications	Infrastructure & Applications, People & physical assets	People
Methods	Manual inspection and some tools	Tool-based	Expert review of tool outputs	Human led with use of reconnaissance & extensive tooling	Use of technical, social engineering, and physical exploit methods	Phishing simulation and social engineering
Exploitation	Does not include exploitation	Does not include exploitation	Does not include exploitation	Includes exploitation	Includes exploitation	Includes exploitation
Benefits	Can be conducted pre or ex production	Low cost, can be frequent, finds known vuls, low-hanging fruit	Provides more context and accuracy with human input	Deeper insight into exploitable exposures	Tests the full range of what's exploitable	Tests and improves human security & Awareness

CST Portfolio

Cyber Security Testing Services Portfolio Overview

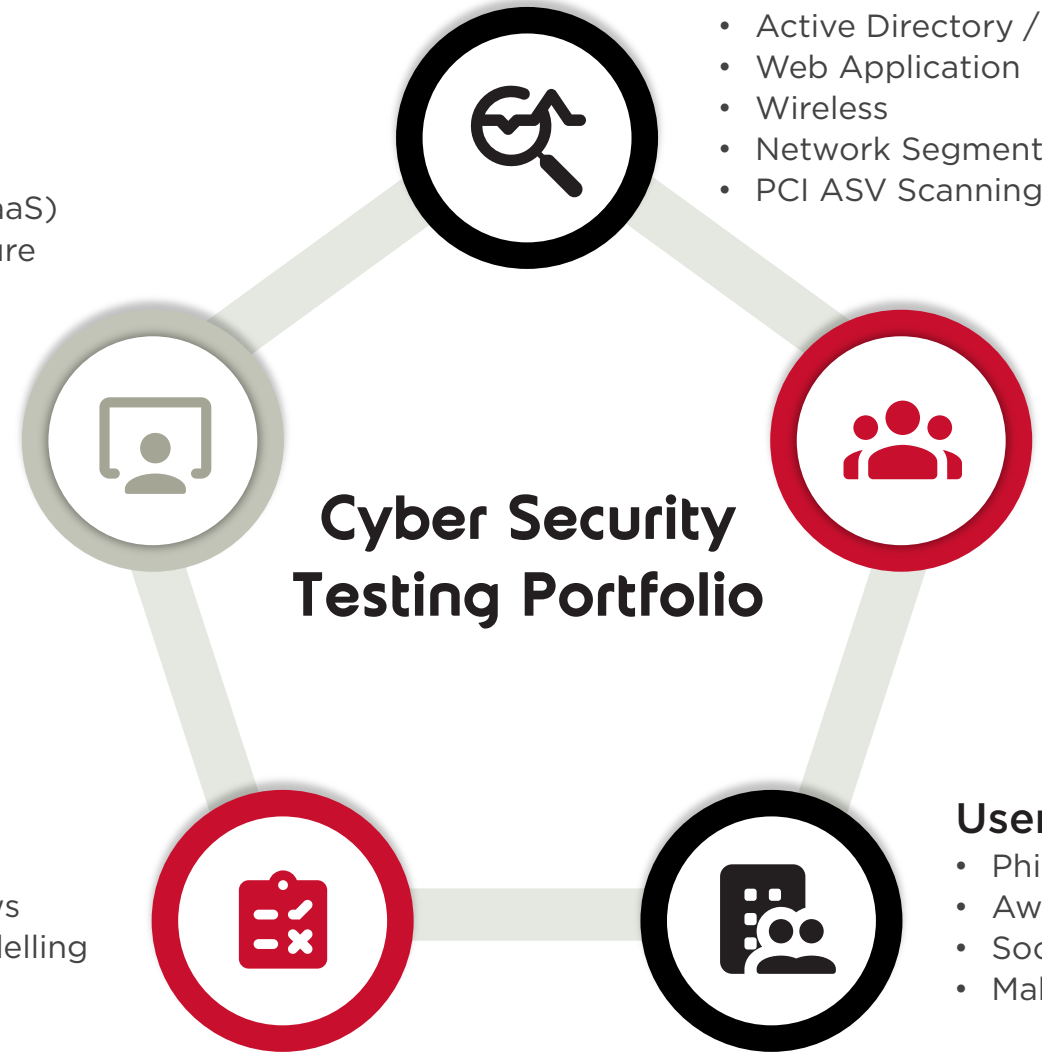
Integrity360
your security in mind

Vulnerability Scanning & Assessment

- Internal/External Infrastructure
- Active Directory / Entra ID
- Web Application
- Wireless
- Network Segmentation
- PCI ASV Scanning

Penetration Testing

- Pen Testing as a Service (PTaaS)
- Internal/External Infrastructure
- Web Application
- API
- Mobile
- Cloud
- Active Directory / Entra ID
- Wireless
- IoT



Red Team Services

- Red Team Exercise
- Physical Red Teaming
- Social Engineering
- Purple Teaming
- Atomic Red Teaming
- Open-Source Intelligence Test
- Targeted Threat Intelligence
- Threat Led Penetration Testing

Audit Services

- Config and build reviews
- Application Threat Modelling

User Testing & Training

- Phishing Campaign
- Awareness Training
- Social Engineering Testing
- Malware defence test

Integrity360

your **security** in mind

CST Portfolio – Scanning & Assessment Services

Scanning and Assessment Services

Integrity360
your security in mind

External Infrastructure Vulnerability Scan/Assessment

Description

An external vulnerability scan of the organisation's public infrastructure for vulnerabilities and security issues. This type of scan checks for weaknesses in your network's firewall(s), routers, and servers that could allow outside attackers to access and harm the network. Can be authenticated or unauthenticated scans.

Service Goals

- Identifying common vulnerabilities and exposures (CVEs) on external-facing systems
- Evaluating the security of external-facing infrastructure, such as load balancers and firewalls
- Checking for unauthorised open ports and services that may be accessible from the Internet
- Addressing vulnerabilities identified during the scan and verifying that proper controls are in place to protect against exploits, e.g. such as remote code execution (RCE)

Process

Scoping → Scanning → Validation → Reporting → Support & Remediation Check

Scoping: Work with our expert security consultants and technical team to determine the scope of the scanning exercise.

Scanning: Identify whether the target systems are affected by one of the thousands of potential vulnerabilities

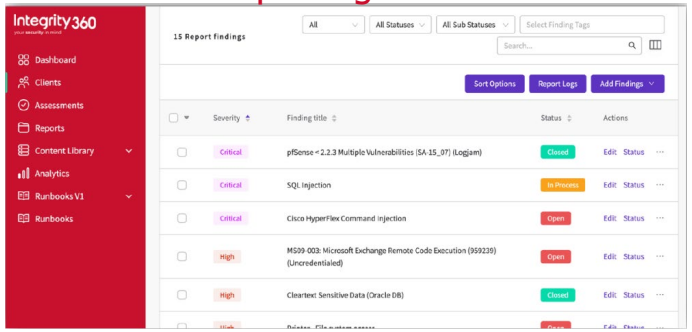
Validation (performed as a part of Vulnerability Assessment only): Manual validation to confirm legitimacy of detected vulnerabilities, crucial to differentiate between genuine security issues and false positives

Reporting: Report with key findings and remediation guidance

Support & Remediation Check: Technical support to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions.

Service Deliverables	Scanning Service	Assessment Service
Target infrastructure Scanning to identify Vulnerabilities and Misconfigurations	✓	✓
Report - Executive Summary, Detailed Technical Report, and Remediation Plan	✓	✓
Access to comprehensive reporting portal	✓	✓
Advanced Manual Verification		✓
In-Depth Analysis and expert insights		✓
Customised, actionable Remediation Strategies		✓

Reporting Portal



Service Benefits

- Identify security weaknesses before and attacker can exploit them
- Minimise false positives and reduce remediation effort
- Satisfy compliance standards
- Validate security policies
- Address customer concerns
- Improve posture
- Reduce risk
- Peace of mind

Scanning and Assessment Services

Integrity360
your security in mind

Internal Infrastructure Vulnerability Scan/Assessment

Description

An internal vulnerability scan focuses on the assets located behind corporate firewalls. The goal of this type of scan is to identify vulnerabilities that could be exploited from the inside of a corporate network and interfere with its confidentiality, availability, and integrity. Can be authenticated or unauthenticated scans.

Service Goals

- Identification of all devices that are connected to the network and verify that they are properly configured and secured.
- Testing access controls to ensure that only authorised users have access to sensitive data.
- Checking for outdated or vulnerable software and ensuring that it is properly patched.
- Detection of the misconfigurations that can lead to security vulnerabilities, such as weak passwords or exposed sensitive data.

Process

Scoping → Scanning → Validation → Reporting → Support & Remediation Check

Scoping: Work with our expert security consultants and technical team to determine the scope of the scanning exercise.

Scanning: Identify whether the target systems are affected by one of the thousands of potential vulnerabilities

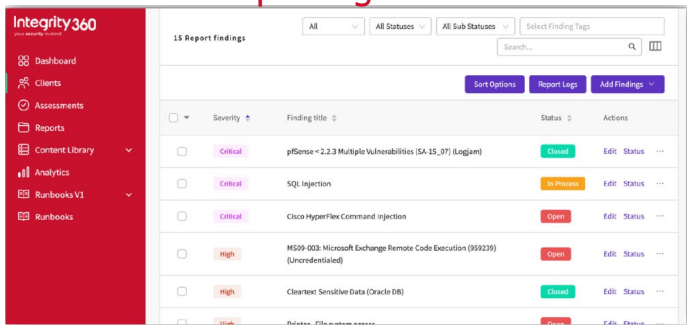
Validation (performed as a part of Vulnerability Assessment only): Manual validation to confirm legitimacy of detected vulnerabilities, crucial to differentiate between genuine security issues and false positives

Reporting: Report with key findings and remediation guidance

Support & Remediation Check: Technical support to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions.

Service Deliverables	Scanning Service	Assessment Service
Target infrastructure Scanning to identify Vulnerabilities and Misconfigurations	✓	✓
Report - Executive Summary, Detailed Technical Report, and Remediation Plan	✓	✓
Access to comprehensive reporting portal	✓	✓
Advanced Manual Verification		✓
In-Depth Analysis and expert insights		✓
Customised, actionable Remediation Strategies		✓

Reporting Portal



Service Benefits

- Identify security weaknesses before and attacker can exploit them
- Minimise false positives and reduce remediation effort
- Satisfy compliance standards
- Validate security policies
- Address customer concerns
- Improve posture
- Reduce risk
- Peace of mind

Scanning and Assessment Services

Integrity360
your security in mind

Active Directory/Entra ID Vulnerability Scan/Assessment

Description

An Active Directory scan focuses on the security of your identity and access management configuration in Active Directory and/or Entra ID (formerly Azure active Directory). Includes internal scans of your company's Active Directory domain and can be customised or use pre-defined settings. These scans can be performed as authenticated or unauthenticated.

Service Goals

- The goal of this type of scan is to identify vulnerabilities in your identity and access management configuration in Active Directory or Entra ID (formerly Azure AD)
- Evaluate the security of your domain policies and user permissions and detect unsafe trust relationships and unauthorised changes to your AD/Entra ID
- Prevent exposure to lateral movement, privilege escalation and eliminate other attack paths.

Process

Scoping → Scanning → Validation → Reporting → Support & Remediation Check

Scoping: Work with our expert security consultants and technical team to determine the scope of the scanning exercise.

Scanning: Identify whether the target systems are affected by one of the thousands of potential vulnerabilities

Validation (performed as a part of Vulnerability Assessment only): Manual validation to confirm legitimacy of detected vulnerabilities, crucial to differentiate between genuine security issues and false positives

Reporting: Report with key findings and remediation guidance

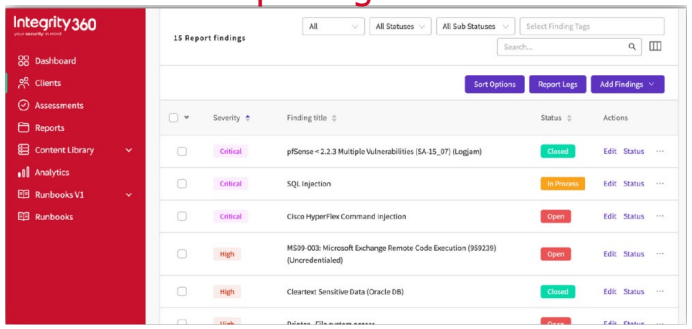
Support & Remediation Check: Technical support to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions.

Microsoft Entra ID

Active Directory

Service Deliverables	Scanning Service	Assessment Service
Target infrastructure Scanning to identify Vulnerabilities and Misconfigurations	✓	✓
Report - Executive Summary, Detailed Technical Report, and Remediation Plan	✓	✓
Access to comprehensive reporting portal	✓	✓
Advanced Manual Verification		✓
In-Depth Analysis and expert insights		✓
Customised, actionable Remediation Strategies		✓

Reporting Portal



Service Benefits

- Identify security weaknesses before and attacker can exploit them
- Minimise false positives and reduce remediation effort
- Satisfy compliance standards
- Validate security policies
- Address customer concerns
- Improve posture
- Reduce risk
- Peace of mind

Scanning and Assessment Services

Integrity360
your security in mind

Web Application Vulnerability Scan/Assessment

Description

The web application vulnerability scanning service uses automated tools to scan web application for vulnerabilities, insecure server configurations, and other potential security issues. The service provides a detailed report of the vulnerabilities found and provides guidance on how to address them. Options available for once-off or scheduled at regular intervals, authenticated or not authenticated.

Service Goals

- To identify potential security risks that could compromise the confidentiality, integrity, or availability of the web application, and how to address them
- These include vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), insecure server configurations, and other potential security issues.
- The scan may also identify outdated software, plugins or third-party libraries with known vulnerabilities

Process

Scoping → Scanning → Reporting → Support & Remediation Check

Scoping: Work with our expert security consultants and technical team to determine the scope of the website and application, as well as the best testing solution for your needs.

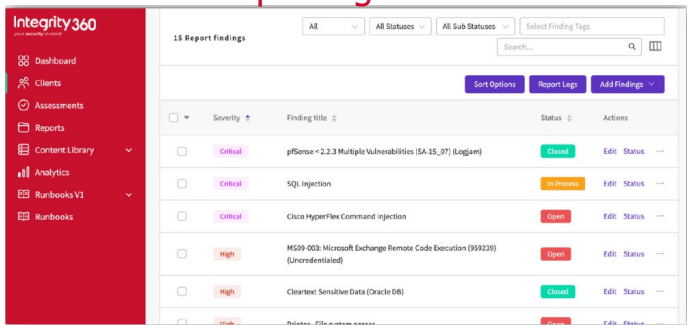
Scanning: The most crucial part of the scanning process, is that it attempts to identify whether the target systems are affected by one of the thousands of potential vulnerabilities, which could include misconfiguration or an unpatched service.

Reporting: Upon completion of the technical procedures, our testing team produces a report containing key findings and remediation guidance to address any discovered vulnerabilities.

Support & Remediation Check: We will provide you with all the technical support you need to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions.

Service Deliverables	Scanning Service	Assessment Service
Web Application Scanning to identify Vulnerabilities and Misconfigurations	✓	✓
Report - Executive Summary, Detailed Technical Report, and Remediation Plan	✓	✓
Access to comprehensive reporting portal	✓	✓
Advanced Manual Verification		✓
In-Depth Analysis and expert insights		✓
Customised, actionable Remediation Strategies		✓

Reporting Portal



Service Benefits

- Identify security weaknesses before and attacker can exploit them
- Minimise false positives and reduce remediation effort
- Satisfy compliance standards
- Validate security policies
- Address customer concerns
- Improve posture
- Reduce risk
- Peace of mind

Scanning and Assessment Services

Wireless Vulnerability Scan/Assessment

Description

The wireless vulnerability scanning and assessment service uses automated tools to scan the wireless network for security issues such as rogue access points, weak encryption, and misconfigurations that could leave the network open to attack. The service provides a detailed report of the vulnerabilities found and provides guidance on how to address them.

Service Goals

- The goal of a wireless scan service is to identify and assess potential vulnerabilities and threats within an organization's wireless network infrastructure
- Uncover security issues such as rogue access points, weak encryption, and general misconfigurations that could leave the network open to attack
- Help organizations protect sensitive data, maintain their operations, and comply with industry regulations

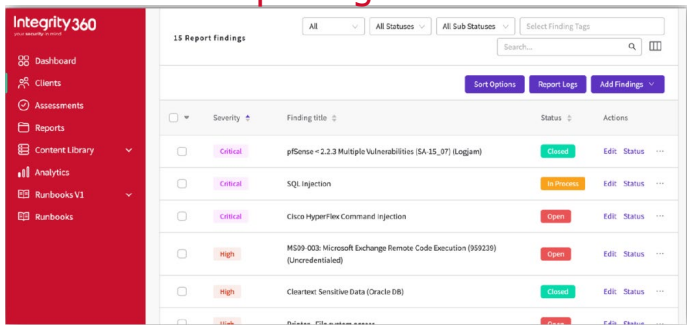
Process

Scoping → Preparation → Scanning → Analysis and Reporting → Support

Scoping: Work with our expert security consultants and technical team to determine the scope of the scanning: physical locations, buildings, floors, rooms, etc.
Preparation: Our experts should get from your information required for scanning: offices addresses, floor plans, list of authorized Wi-Fi networks.
Scanning: This is the execution of the scanning activity. Our experts go onsite to perform the scan and collect all required information.
Analysis and Reporting: Our experts analyze the collected data and produce a report containing key findings and remediation guidance to address any discovered threats.
Support: We will provide you with all the technical support you need to better understand the discovered threats and validate the effectiveness of implemented solutions.

Service Deliverables	Scanning Service	Assessment Service
Scanning to identify Vulnerabilities and Misconfigurations	✓	✓
Report - Executive Summary, Detailed Technical Report, and Remediation Plan	✓	✓
Access to comprehensive reporting portal	✓	✓
Advanced Manual Verification		✓
In-Depth Analysis and expert insights		✓
Customised, actionable Remediation Strategies		✓

Reporting Portal



Service Benefits

- Identify exploitable vulnerabilities and threats within wireless network
- Improve security posture of your wireless network
- Validate security policies
- Providing evidence to customers, regulators, and auditors that your organization takes security seriously by taking steps to protect sensitive data.
- Reduce risk of successful cyber attack
- Peace of mind

Scanning and Assessment Services

Network Segmentation Test

Integrity360
your security in mind

Description

This service validates the effectiveness of segmentation controls between network segments, for example, VLANs. A thorough scan and analysis of your network infrastructure will be performed to identify any unauthorised communication. Uses ICMP scans, port scans and variety of techniques and scripts to bypass segmentation controls and identify weaknesses.

Service Goals

- Evaluate the effectiveness of network segmentation strategies
- Identify potential vulnerabilities or misconfigurations that could be exploited by attackers
- Minimise the possibility of lateral movement by threat actor inside the environment
- Comply with mandatory standards and regulations (e.g., PCI-DSS, SOX, country-specific banking laws / regulations, HIPAA, SSAE16 / ISAE 3902, etc.)

Process

Scoping → Scanning → Validation → Reporting → Support & Remediation Check

Scoping: Work with our expert security consultants and technical team to determine the scope of the scanning exercise.

Scanning: Identify whether the target network segments are vulnerable to unauthorised traffic

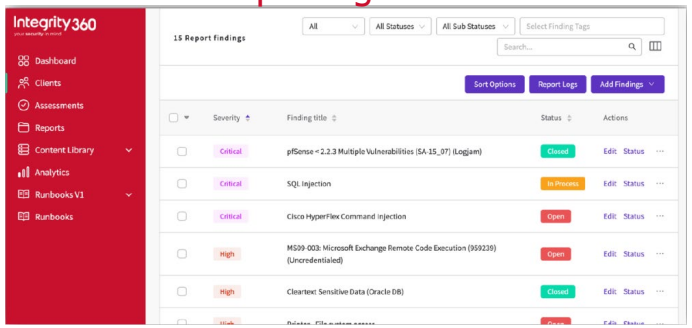
Validation (performed as a part of Vulnerability Assessment only): Manual validation to confirm legitimacy of detected vulnerabilities, crucial to differentiate between genuine security issues and false positives

Reporting: Report with key findings and remediation guidance

Support & Remediation Check: Technical support to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions.

Service Deliverables	Scanning Service	Assessment Service
Web Application Scanning to identify Vulnerabilities and Misconfigurations	✓	✓
Report - Executive Summary, Detailed Technical Report, and Remediation Plan	✓	✓
Access to comprehensive reporting portal	✓	✓
Advanced Manual Verification		✓
In-Depth Analysis and expert insights		✓
Customised, actionable Remediation Strategies		✓

Reporting Portal



Service Benefits

- Reduces risk by isolating less-secure networks from high-security networks
- Limits the possibility of lateral movement by threat actors in the environment
- Reduces the time and cost to become PCI compliant
- Tests the effectiveness of your security controls, such as firewalls and third-party services management.
- Evidence to customers, regulators, and auditors that your organization takes security seriously
- Reducing the likelihood of a successful cyber-attack.

Integrity360

your **security** in mind

CST Portfolio – Penetration Testing Services

Penetration Testing Services

External Infrastructure Penetration Test

Description

This test simulates real-world attacks on external devices, internet networking, cloud computing, and virtualization, focusing on Internet-facing infrastructure, including firewall, VPN endpoints, web servers, and mail servers. The level of access is like that of an external hacker trying to enter your company environment remotely.

Service Goals

- Identify and validate vulnerabilities in the infrastructure and systems that could be exploited by malicious actors
- Determine the impact and likelihood of each identified vulnerability, demonstrate impact through detailed descriptions and exploitation proof-of-concept (PoCs)
- Provide recommendations for remediation of identified vulnerabilities, best practices and improvements

Process

Scoping → Recon → Vulnerability Discovery → Exploitation → Reporting → Support & Remediation Check

Scoping: Work with our expert security consultants and technical team to determine the scope of the test

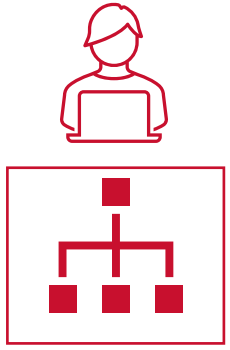
Reconnaissance: Our team employs all modern intelligence gathering techniques to uncover security & technical information about the targets under assessment.

Vulnerability Discovery: Our team utilizes years of offensive security experience, testing expertise and knowledge of the latest hacking tools to uncover exploitable exposures and vulnerabilities

Exploitation: Devise and carry out a plan to exploit what has been discovered while minimizing disruption of services.

Reporting: Documentation of key findings and remediation guidance to address any discovered vulnerabilities/exposures

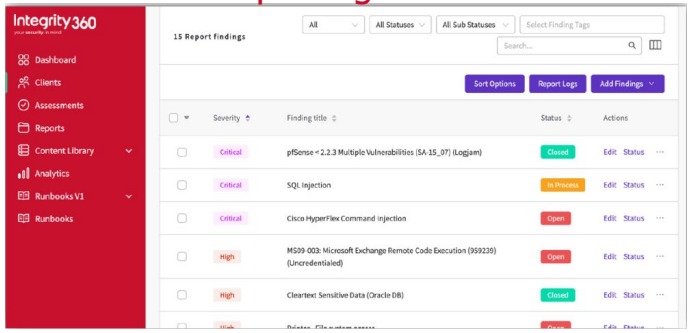
Support & Remediation Check: All the technical support you need to better understand the discovered vulnerabilities and validate the effectiveness of their remediation



Service Deliverables
Reconnaissance, discovery and exploitation to identify security weaknesses in infrastructure, processes and security controls
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan
Access to comprehensive reporting portal
In-Depth Analysis and expert insights
Customised, actionable Remediation Strategies

Service Options	
Black Box	The tester has no knowledge of the system being tested.
Grey Box	The tester has some knowledge, e.g. OS version, some access, etc.
White Box	The tester has full knowledge of system being tested, design, specs, etc.

Reporting Portal



Service Benefits

- Identify security weaknesses before an attacker can exploit them
- Identifying overlooked software patches, firewall misconfigurations, and encryption protocols
- Insight into security posture, including policies and controls
- Demonstrate compliance with standards/regulation
- Guidance for prioritisation of remediation actions
- Reduced risk of a breach
- Peace of mind

Penetration Testing Services

Internal Infrastructure Penetration Test

Description

This test simulates real-world attacks on the organisation's network devices and servers from the perspective of someone inside the environment with the same physical access as someone in the facility.

Service Goals

- Identify and validate vulnerabilities in the infrastructure and systems that could be exploited by malicious actors with physical access in the environment
- Identify susceptibility to insider threat and external threat actor post-access lateral movement
- Determine the impact and likelihood of each identified vulnerability, demonstrate impact through detailed descriptions and exploitation proof-of-concept (PoCs)
- Provide recommendations for remediation of identified vulnerabilities, best practices and improvements

Process

Scoping → Recon → Vulnerability Discovery → Exploitation → Reporting → Support & Remediation Check

Scoping: Work with our expert security consultants and technical team to determine the scope of the test

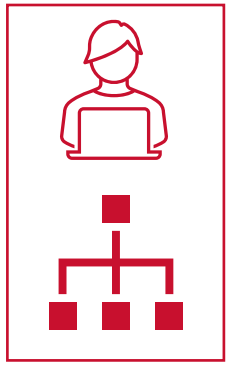
Reconnaissance: Our team employs all modern intelligence gathering techniques to uncover security & technical information about the targets under assessment.

Vulnerability Discovery: Our team utilizes years of offensive security experience, testing expertise and knowledge of the latest hacking tools to uncover exploitable exposures and vulnerabilities

Exploitation: Devise and carry out a plan to exploit what has been discovered while minimizing disruption of services.

Reporting: Documentation of key findings and remediation guidance to address any discovered vulnerabilities/exposures

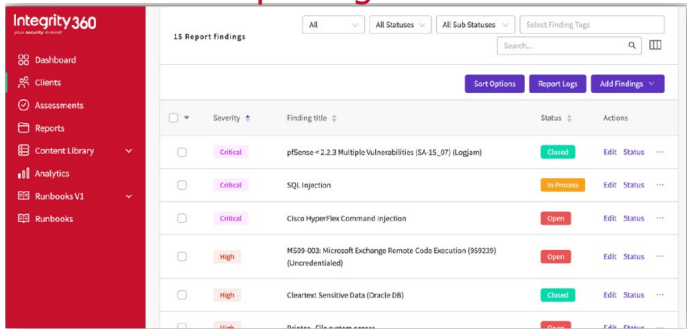
Support & Remediation Check: All the technical support you need to better understand the discovered vulnerabilities and validate the effectiveness of their remediation



Service Deliverables
Reconnaissance, discovery and exploitation to identify security weaknesses in internal infrastructure, processes and security controls
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan
Access to comprehensive reporting portal
In-Depth Analysis and expert insights
Customised, actionable Remediation Strategies

Service Options	
Black Box	The tester has no knowledge of the system being tested.
Grey Box	The tester has some knowledge, e.g. OS version, some access, etc.
White Box	The tester has full knowledge of system being tested, design, specs, etc.

Reporting Portal



Service Benefits

- Identify internal security weaknesses before an attacker or insider can exploit them
- Identifying overlooked software patches, firewall misconfigurations, and encryption protocols
- Insight into security posture, including policies and controls
- Demonstrate compliance with standards/regulation
- Guidance for prioritisation of remediation actions
- Reduced risk of a breach
- Peace of mind

Penetration Testing Services

Web Application Penetration Test

Description

With web application penetration testing, our technical team will be able to identify potential threats and vulnerabilities within your web application, using frameworks like the OWASP Top 10 and Web testing Guide and NIST Cybersecurity Framework, we can identify common vulnerabilities and best practices for secure development. Through simulated web attacks, we will uncover the weaknesses in your application and provide detailed information and actionable guidance for remediation.

Service Goals

- Identify and validate vulnerabilities in web applications that could be exploited by malicious actors
- Determine the impact and likelihood of each identified vulnerability, demonstrate impact through detailed descriptions and exploitation proof-of-concept (PoCs)
- Understand exposures per user type (authenticated, unauthenticated, privileged, unprivileged)
- Provide recommendations for remediation of identified vulnerabilities, best practices and improvements

Process

Scoping → Recon → Vulnerability Discovery → Exploitation → Reporting → Support & Remediation Check

Scoping: Determine the scope of the website and application, as well as the best testing solution for your needs.

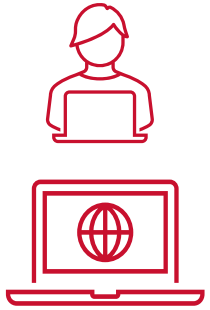
Reconnaissance: Team employs all modern intelligence gathering techniques to uncover security and technical information about the websites and applications under assessment.

Vulnerability Discovery: To identify exploitable security vulnerabilities, our penetration testing team utilizes their years of offensive security experience, testing expertise and knowledge of the latest hacking tools.

Exploitation: Once vulnerabilities have been found, our technical team devises and carries out a plan to exploit them while minimizing disruption of services.

Reporting: Upon completion of the technical procedures, our penetration testing team produces a report containing key findings and remediation guidance to address any discovered vulnerabilities.

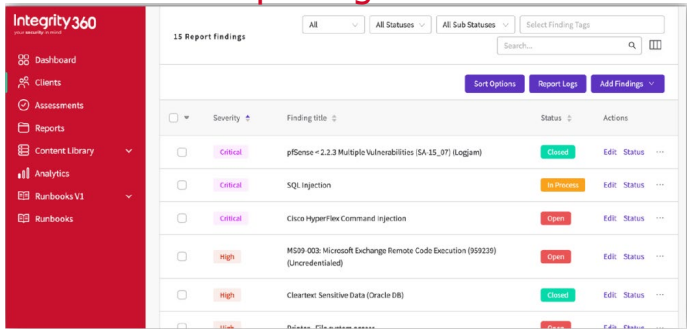
Support & Remediation Check: All the technical support you need to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions



Service Deliverables
Reconnaissance, discovery and exploitation to identify security weaknesses in internal infrastructure, processes and security controls
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan
Access to comprehensive reporting portal
In-Depth Analysis and expert insights
Customised, actionable Remediation Strategies

Service Options	
Black Box	The tester has no knowledge of the system being tested.
Grey Box	The tester has some knowledge, e.g. OS version, DB, authenticated access
White Box	The tester has full knowledge of application being tested, design & code

Reporting Portal



Service Benefits

- Identify web application weaknesses such as SQL injection, Cross-site scripting, insecure configuration, access controls and management
- Satisfy compliance requirements (ISO, PCI)
- Validate security policies and controls
- Assist with prioritisation
- Avoid the negative impact of a cyber attack
- Peace of mind

Penetration Testing Services

API Penetration Test

Integrity360
your security in mind

Description

API penetration testing is a comprehensive security evaluation of an application's API (Application Programming Interface) to identify and mitigate vulnerabilities and potential risks. Testing focuses on the logic and functionality of the API, identifying and exploiting any weaknesses or errors in its programming.

Service Goals

- Evaluate the security and functionality of an application's API
- Ensure API is compliant with industry standards and best practices
- Help prevent unauthorized access, data breaches, denial of service attacks, and other forms of malicious activity

Process

Scoping → Recon → Vulnerability Discovery → Exploitation → Reporting → Support & Remediation Check

Scoping: Determine the scope of the Application and its APIs, as well as the best testing solution for your needs.

Reconnaissance: Team employs all modern intelligence gathering techniques to uncover security and technical information about the applications/APIs under assessment.

Vulnerability Discovery: To identify exploitable security vulnerabilities, our penetration testing team utilizes their years of offensive security experience, testing expertise and knowledge of the latest hacking tools.

Exploitation: Once vulnerabilities have been found, our technical team devises and carries out a plan to exploit them while minimizing disruption of services.

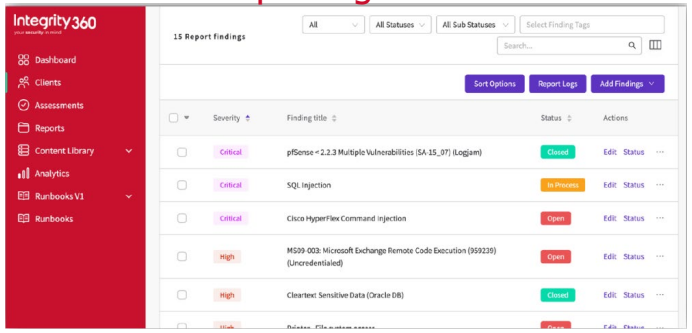
Reporting: Upon completion of the technical procedures, our penetration testing team produces a report containing key findings and remediation guidance to address any discovered vulnerabilities.

Support & Remediation Check: All the technical support you need to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions

Service Deliverables
Reconnaissance, discovery and exploitation to identify API security weaknesses and issues
Test: Input/output data, authentication, authorisation, insecure session management (cookies, access tokens, etc.), common attacks (injection, tampering, DoS), other test input scenarios
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan, Portal access
In-Depth Analysis, expert insight, remediation advice

Service Options	
Black Box	The tester has no knowledge of the system being tested.
Grey Box	The tester has some knowledge, e.g. OS version, DB, authenticated access
White Box	The tester has full knowledge of application being tested, design & code

Reporting Portal



Service Benefits

- Identify security loopholes, misconfigs, & other exploitable weaknesses in API
- Improved security, performance and reliability
- Reduced the likelihood of security breaches
- Demonstrate compliance with standards/regulation

Penetration Testing Services

Mobile Application Penetration Test

Description

Mobile Penetration Testing is a method used to identify vulnerabilities in both IOS and Android applications and reduce the risks of attacks such as jailbroken and root device check bypass, pinning bypass, data exfiltration through the exportable backup, and data tampering. With this service our technical team will simulate various attacks to identify vulnerabilities and provide detailed recommendations for improving security.

Service Goals

- Evaluate the security and functionality of a mobile applications
- Ensure application is compliant with industry standards and best practices
- Help prevent unauthorized access, data breaches, and other forms of malicious activity
- Prevent communications being intercepted or retrieved or leakage of data
- Avoid insecure use of camera and microphone use by attackers

Process

Scoping → Recon → Vulnerability Discovery → Exploitation → Reporting → Support & Remediation Check

Scoping: Determine the scope of the Mobile Application, as well as the best testing solution for your needs.

Reconnaissance: Team employs all modern intelligence gathering techniques to uncover security and technical information about the Mobile application under assessment.

Vulnerability Discovery: To identify exploitable security vulnerabilities, our penetration testing team utilizes their years of offensive security experience, testing expertise and knowledge of the latest hacking tools.

Exploitation: Once vulnerabilities have been found, our technical team devises and carries out a plan to exploit them while minimizing disruption of services.

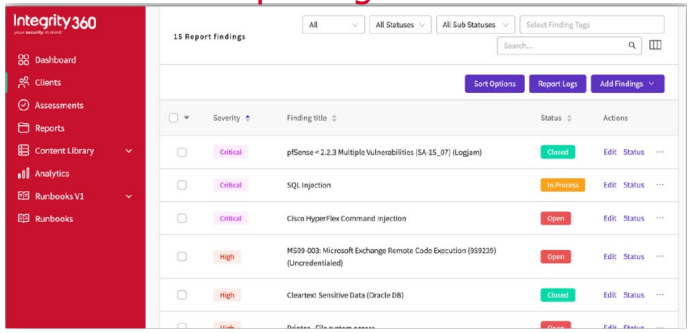
Reporting: Upon completion of the technical procedures, our penetration testing team produces a report containing key findings and remediation guidance to address any discovered vulnerabilities.

Support & Remediation Check: All the technical support you need to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions

Service Deliverables
Reconnaissance, discovery and exploitation to identify mobile application security weaknesses and issues
Test: Jailbreak and root detection algorithms, pinning algorithms, login security, authentication, brute force attacks, privilege escalation, sensitive data disclosure, handling of malicious files permissions, input testing
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan, Portal access
In-Depth Analysis, expert insight, remediation advice

Service Options	
Black Box	The tester has no knowledge of the system being tested.
Grey Box	The tester has some knowledge of the application and access permissions
White Box	The tester has full knowledge of the application being tested, design & code

Reporting Portal



Service Benefits

- Identify exploitable weaknesses in Mobile Application security
- Improved security, performance and reliability
- Demonstrate compliance with standards/regulation
- Improve mobile application development security standards
- Assist with remediation prioritisation
- Reduced the likelihood of security breaches

Penetration Testing Services

Cloud Penetration Test

Integrity360
your security in mind

Description

A specialised service designed to assess the security of cloud-based systems, configurations, applications, and infrastructure. Support for AWS, Azure, Google Cloud Platform, and others. Our methodology aligns with industry-standard frameworks like OWASP, NIST, CIS, and PCI DSS. Focusses on security of organisation's components within the cloud rather than the CSP infrastructure and in line with CSP guidelines.

Service Goals

- Evaluate the security of the Cloud environment under your control
- Understand where there is misconfiguration, weak access control, improper use, weak identity and access management, or inappropriate exposure of sensitive data
- Support remediation and continuous security improvement

Process

Scoping → Recon → Vulnerability Discovery → Exploitation → Reporting → Support & Remediation Check

Scoping: Work with our expert security consultants and technical team to determine the scope of the Cloud test, as well as the best testing solution.

Reconnaissance: Our penetration testing team employs all modern intelligence gathering techniques to uncover security and technical information about the cloud infrastructure under assessment.

Vulnerability Discovery: To identify exploitable security vulnerabilities, our penetration testing team utilizes their years of offensive security experience, testing expertise and knowledge of the latest hacking tools.

Exploitation: Once vulnerabilities have been found, our technical team devises and carries out a plan to exploit them while minimizing disruption of services.

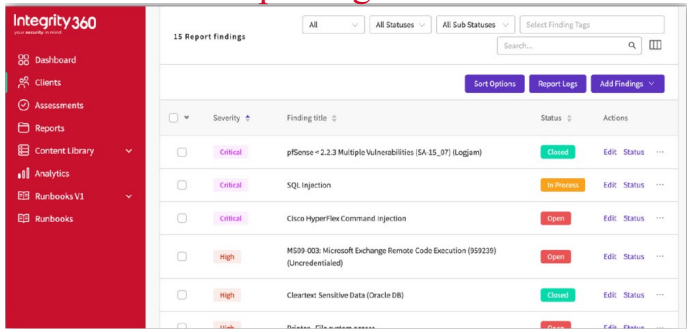
Reporting: Upon completion of the technical procedures, our penetration testing team produces a report containing key findings and remediation guidance to address any discovered vulnerabilities.

Support & Remediation Check: We will provide you with all the technical support you need to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions.

Service Deliverables
Reconnaissance, discovery and exploitation to identify cloud security weaknesses and issues
Test: publicly exposed & vulnerable cloud services, unpatched services and applications, access security & data security, leaked credentials/tokens, privilege escalation, storage methods, misconfigurations
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan, Portal access
In-Depth Analysis, expert insight, remediation advice

Service Options	
Black Box	The tester has no knowledge of the system being tested.
Grey Box	The tester has some knowledge such as open services, user access etc.
White Box	Tester has full knowledge of the system and admin level access

Reporting Portal



Service Benefits

- Gain understanding of Cloud security configuration
- Learn about the most common and effective Cloud attack vectors and how to detect, prevent, and mitigate
- Align best practices with business processes
- Receive a detailed report of the issues discovered, their impact, and recommended remediation.
- Obtain plan for remediation
- Demonstrate Compliance
- Move to the cloud with increased confidence

Penetration Testing Services

Active Directory/Entra ID Penetration Test

Description

Designed to ensure the security and integrity of systems and networks that utilize Active Directory for authentication and resource management within your infrastructure. Thorough analysis of your Active Directory infrastructure to identify and exploit potential vulnerabilities and weaknesses that could be exploited by malicious attackers.

Service Goals

- The goal of this type of test is to identify vulnerabilities in your identity and access management configuration in Active Directory or Entra ID (formerly Azure AD)
- Evaluate the security of your domain policies and user permissions and detect unsafe trust relationships and unauthorised changes to your AD/Entra ID
- Prevent exposure to lateral movement, privilege escalation and eliminate other attack paths.

Process

Scoping → Scanning → Validation → Reporting → Support & Remediation Check

Scoping: Work with our expert security consultants and technical team to determine the scope of the AD test, as well as the best testing solution for your needs.

Reconnaissance: Our penetration testing team employs all modern intelligence gathering techniques to uncover security and technical information about the AD infrastructure under assessment.

Vulnerability Discovery: To identify exploitable security vulnerabilities, our penetration testing team utilizes their years of offensive security experience, testing expertise and knowledge of the latest hacking tools.

Exploitation: Once vulnerabilities have been found, our technical team devises and carries out a plan to exploit them while minimizing disruption of services.

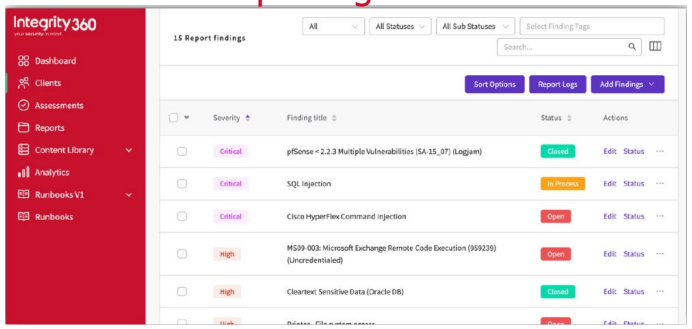
Reporting: Upon completion of the technical procedures, our penetration testing team produces a report containing key findings and remediation guidance to address any discovered vulnerabilities.

Support & Remediation Check: We will provide you with all the technical support you need to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions

Service Deliverables
Reconnaissance, discovery and exploitation to identify AD security weaknesses and issues
Enumeration and discovery of systems, services, domains and trusts, GPO, permissions & authentication protocols; Exploitation, lateral movements and privilege escalation through password cracking, ticket manipulation, hash manipulation, LDAP injection, exploit of insecure protocols, & use of zero-days
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan, Portal access
In-Depth Analysis, expert insight, remediation advice

Service Options	
Unprivileged user	Tester is unprivileged domain user
Local admin on domain joined system	Unprivileged domain user with local admin on domain joined system - tests lateral movement
Privileged User	Tester has full privileged access – ideal for most in-depth assessment

Reporting Portal



Service Benefits

- Gain an understanding of Active Directory security configuration
- Learn about most common and effective Active Directory attack vectors and how to detect, prevent, and mitigate
- Align Active Directory security best practices with your business processes and requirements
- Receive a detailed report of the issues discovered, & the impact
- Obtain a plan of action for resolving and mitigating any identified issues.
- Compliance
- Reduced risk of breach

Penetration Testing Services

Wireless Penetration Test

Description

Wireless penetration testing is a way to evaluate the security of your wireless networks, Wi-Fi-enabled devices such as laptops, smartphones, printers, security cameras, and IoT devices.

Service Goals

- Assessing the security posture of the wireless network and related systems
- Testing the effectiveness of security controls and policies related to wireless network security.
- Provide recommendations for remediation of identified vulnerabilities, best practices and improvements.

Process

Scoping → Recon → Vulnerability Discovery → Exploitation → Reporting → Support & Remediation Check

Scoping: Work with our expert security consultants and technical team to determine the scope of the scanning: physical locations, buildings, floors, rooms, etc. and appropriate test

Reconnaissance: Our penetration testing team employs all modern intelligence gathering techniques to uncover security and technical information about the wireless networks under assessment.

Vulnerability Discovery: To identify exploitable security vulnerabilities, our penetration testing team utilizes their years of offensive security experience, testing expertise and knowledge of the latest hacking tools.

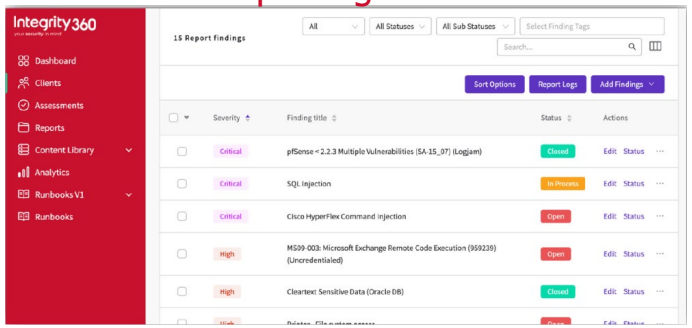
Exploitation: Our technical team devises and carries out a plan to exploit these while minimizing disruption of services.

Reporting: Upon completion of the technical procedures, our penetration testing team produces a report containing key findings and remediation guidance to address any discovered vulnerabilities.

Support & Remediation Check: We will provide you with all the technical support you need to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions.

Service Deliverables
Reconnaissance, discovery and exploitation to identify wireless security weaknesses and issues
On location testing of Wi-Fi networks; Thorough analysis of the wireless security controls and authentication mechanisms, such as WEP and WPA; Identifying weak encryption protocols; Capturing authentication handshakes; Cracking Pre-Shared Keys (PSK) to allow remote access; Authentication attacks against wireless devices and Access Points (APs); information disclosure when wireless clients connect to your network; Certificate spoofing attacks; Identify unconfigured or unsecured IoT devices that can be hijacked over Wi-Fi
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan, Portal access
In-Depth Analysis and expert insights, Customised, actionable Remediation Strategies

Reporting Portal



Service Benefits

- Thorough analysis of wireless security controls
- Understand risks and vulnerabilities and how to mitigate them
- Compliance with regulation and standards
- Understanding of remediation prioritisation
- Evidence of quality of wireless security controls
- Reducing the risk of a successful attack
- Peace of mind

Penetration Testing Services

IoT (Internet of Things) Penetration Test

Description

IoT penetration testing is a form of security evaluation focused on the Internet of Things (IoT) devices within a network. Includes examining smart devices, sensors, and other IoT components for vulnerabilities that could be leveraged by cyber attackers and involves testing for weaknesses in device firmware, wireless communication protocols, and the interaction between devices and their connected networks or cloud services.

Service Goals

- Emulate real-world cyber threats targeting IoT ecosystems to pinpoint security lapses and recommend enhancements
- Identify and validate vulnerabilities in the IoT devices, communication protocols, and associated systems susceptible to exploitation by malicious actors
- Determine the impact and likelihood of each identified vulnerability, demonstrate impact through detailed descriptions and exploitation proof-of-concept (PoCs)
- Provide recommendations for remediation of identified vulnerabilities, best practices and improvements

Process

Scoping → Recon → Vulnerability Discovery → Exploitation → Reporting → Support & Remediation Check

Scoping: Collaborate to outline the test's extent, targeting specific IoT devices, ecosystems, and communication protocols to tailor the most effective testing strategy for your organisation's needs.

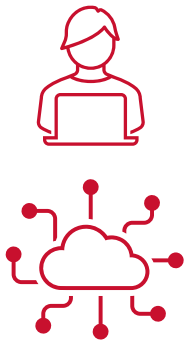
Reconnaissance: Our penetration testing team conducts comprehensive intelligence gathering on the IoT environment, leveraging advanced techniques to collect technical information that may impact the security of IoT devices and their network interfaces.

Vulnerability Discovery: Leveraging extensive offensive security experience, our testers probe for weaknesses using the latest tools and their deep understanding of IoT-specific vulnerabilities.

Exploitation: Once vulnerabilities have been found, our technical team devises and carries out a plan to exploit them while minimising disruption of services.

Reporting: Upon completion of the technical procedures, our penetration testing team produces a report containing key findings and remediation guidance to address any discovered vulnerabilities.

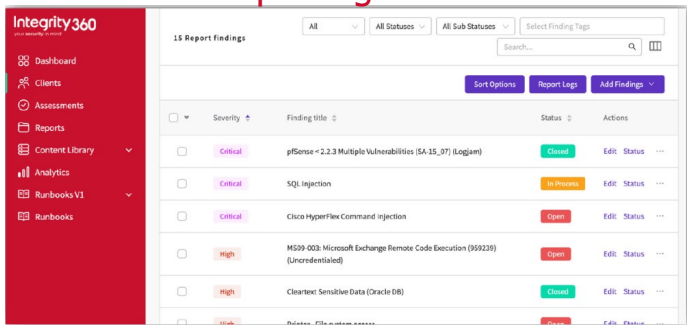
Support & Remediation Check: We will provide you with all the technical support you need to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions.



Service Deliverables

Reconnaissance, discovery and exploitation to identify IoT security weaknesses & issues
(Depending on scope): Firmware analysis and reverse engineering, IoT wireless security access, IoT connected network security assessment, IoT API security testing, mobile app IoT interface, IoT Web application test, IoT hardware security, compliance test, IoT configuration and Authentication review and test, IoT threat modelling
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan, Portal access
In-Depth Analysis and expert insights, Customised, actionable Remediation Strategies

Reporting Portal



Service Benefits

- Early Detection of IoT-related Vulnerabilities
- Protection Against Data Breaches
- Enhanced Device Reliability
- Compliance with Regulations & Standards
- Improved Customer Trust and Brand Reputation
- Cost Savings
- Support for Security by Design
- Enhanced Privacy Protection
- Adaptation to New Threats
- Remediation prioritisation

Integrity360

your **security** in mind

CST Portfolio – Red Teaming Services

Red Team Services

Red Team Exercise

Integrity360
your security in mind

Description

A red team is a group that pretends to be an enemy, attempts an intrusion against an organisation at their direction and then reports back so that the organisation can improve defenses. The Red Team will use a variety of techniques, including social engineering, network exploitation, and physical penetration testing, to gain and demonstrate non-destructive access to sensitive data and systems.

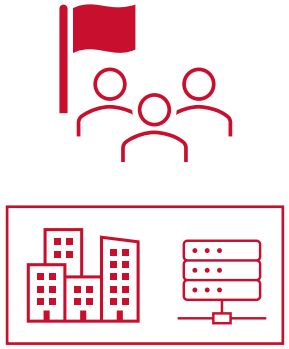
Service Goals

- Identify vulnerabilities and exposures in any of the following:
  - Technology – infrastructure, applications, routers, switches, appliances etc.
  - People – staff, independent contractors, departments, business partners etc.
  - Physical – offices, warehouses, substations, data centres, buildings, etc.
- Highlight the exposures that may be leveraged by a determined adversary in any form so they may be mitigated, hence reducing risk

Process

Scoping → Recon → Planning → Execution → Analysis → Reporting → Support

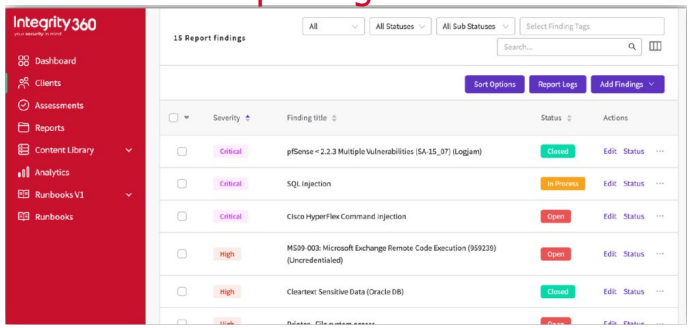
Scoping: Work with our expert security consultants and technical team to determine the scope of the assessment, including the target systems, network, and access points.
Information Gathering and Reconnaissance: Our Red Team employs all modern intelligence gathering techniques to uncover security and technical information about the targets under assessment.
Planning: Our Red Team will develop a customized plan that simulates realistic attack scenarios and objectives that align with the organization's threat model.
Execution: Our Red Team will use a combination of advanced techniques, tactics and procedures to infiltrate the organization's network, systems, and physical locations
Analysis: The Red Team will analyze and document the results of the assessment, including vulnerabilities identified, data exfiltration, and incident response capabilities
Reporting: Upon completion of the assessment, our team will produce a detailed report that includes a summary of the attack scenarios, the vulnerabilities identified, the impact of the vulnerabilities, and the recommendations for remediation.
Support: We will provide you with all the technical support you need to better understand the discovered vulnerabilities, validate the effectiveness of implemented solutions, and develop an incident response plan.



Service Deliverables
Reconnaissance, discovery and exploitation to identify security weaknesses & issues across technology, physical locations, & people
Methodologies may include: Security testing of external and internal fixed and wireless infrastructure and web applications, phishing and spear phishing, social engineering – email and/or telephone and in person, physical penetration testing, and any other attack vector that becomes apparent to achieve the goals of the exercise
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan, Portal access included
In-Depth Analysis and expert insights, Customised, actionable Remediation Strategies

RTA Package Options
Red Team Assessment (RTA)
RTA (Reduced Enumeration)
Simulated Compromise
Assumed Breach

Reporting Portal



Service Benefits

- Identify vulnerabilities and threats within overall security posture
- Use advanced techniques, tactics, and procedures to simulate real-world cyber-attacks
- Uncover security issues such as network infiltration, data exfiltration, staff awareness, and physical security
- Improve the organization's IR capability and procedures.
- Validate security controls and identify any weaknesses that need to be addressed before they can be exploited by attackers.
- Evidence of compliance and best practices
- Reduce the likelihood of a successful cyber-attack.

Red Team Services

Physical Security Test

Integrity360
your security in mind

Description

One of the steps of a Red Team engagement is an assessment of an organisation's physical security and security awareness with the aim of acquiring internal system access. It may also include an element of black-box spear phishing, unless specifically excluded. This test is available standalone or in conjunction with wider Red Team Exercise.

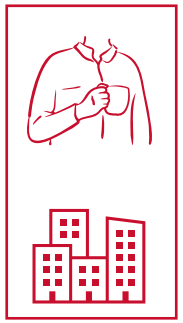
Service Goals

- Identify vulnerabilities and exposures in any of the following:
  - Physical – offices, warehouses, substations, data centres, buildings, etc.
  - People and security controls around physical access
- Gain access to physical areas, secure areas, networks and domains
- Highlight the exposures that may be leveraged by a determined adversary in any form so they may be mitigated, hence reducing risk

Process

Scoping → Recon → Planning → Execution → Analysis → Reporting → Support

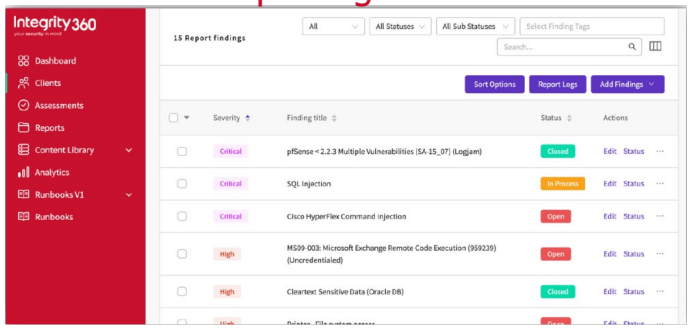
Scoping: Work with our expert security consultants and technical team to determine the scope of the assessment, including the target physical environment
Information Gathering and Reconnaissance: Our team employs all modern intelligence gathering techniques to uncover security and technical information about the targets under assessment.
Planning: Our team will develop a customized plan that simulates realistic attack scenarios and objectives that align with the organization's threat model.
Execution: Our team will use a combination of techniques, tactics and procedures to infiltrate the physical environment
Analysis: The team will analyze and document the results of the assessment, including vulnerabilities identified, data exfiltration, and incident response capabilities
Reporting: Upon completion of the assessment, our team will produce a detailed report that includes a summary of the attack scenarios, the vulnerabilities identified, the impact of the vulnerabilities, and the recommendations for remediation.
Support: We will provide you with all the technical support you need to better understand the discovered vulnerabilities, validate the effectiveness of implemented solutions, and develop an incident response plan.



Service Deliverables

Service Deliverables
Reconnaissance, discovery and exploitation
Bypassing of security controls through various means: Delivery, employee w/wo ID,ID cloning, visitor, smokers, physical attraction, vendor, bribe, lock picking, break in, tailgate
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan, Portal access included
In-Depth Analysis and expert insights, Customised, actionable Remediation Strategies

Reporting Portal



Service Benefits

- Identify physical vulnerabilities and threats within overall security posture
- Use advanced techniques, tactics, and procedures to simulate real-world cyber-attacks
- Uncover security issues such as staff awareness, and physical security gaps
- Test security culture
- Validate security controls and identify any weaknesses that need to be addressed before they can be exploited by attackers.
- Show evidence of compliance and best practices
- Reduce the likelihood of a successful physical cyber-attack

Red Team Services

Purple Team Exercise

Integrity360
your security in mind

Description

A purple team exercise is designed to help internal security teams (blue teams) to fine tune their incident response capabilities in the face of typical operations conducted by a red team, in this case Integrity360. Therefore this exercise is similar to a Red Team exercise, with the addition of collaboration and engagement with the client's operational security team during the process

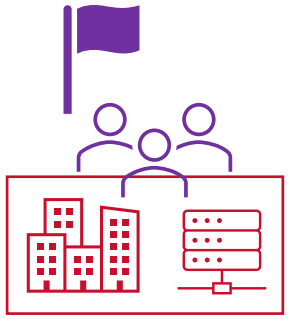
Service Goals

- Create intrusion events in collaboration with the Blue team
- Validate processes and procedures, protections in place, detection, response, and post-mortem activities.
- Improve the overall protective and response capabilities of the organisation

Process

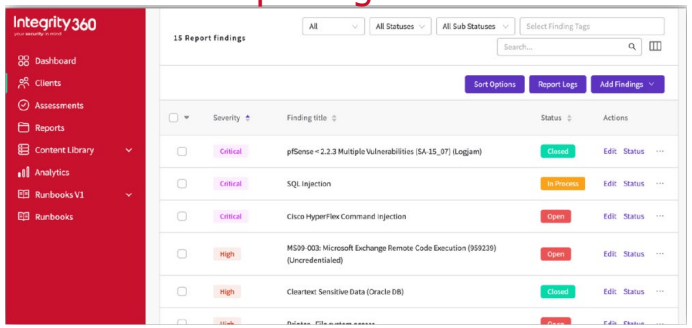
Scoping → Recon → Planning → Execution → Analysis → Reporting → Support

Scoping: Work with our expert security consultants and technical team to determine the scope of the assessment, including the target systems, network, and access points.
Information Gathering and Reconnaissance: Our Red Team employs all modern intelligence gathering techniques to uncover security and technical information about the targets under assessment.
Planning: Our Red Team will develop a customized plan that simulates realistic attack scenarios and objectives that align with the Blue Team's requirements
Execution: Our Red Team will use a combination of advanced techniques, tactics and procedures to infiltrate the organization's network, systems, and physical locations, in collaboration with the Blue team
Analysis: The Red Team will analyze and document the results of the assessment, including vulnerabilities identified, data exfiltration, and incident response capabilities and where the Blue team was/wasn't successful
Reporting: Upon completion of the assessment, our team will produce a detailed report that includes a summary of the attack scenarios, the vulnerabilities identified, the impact of the vulnerabilities, and the recommendations for remediation.
Support: We will provide you with all the technical support you need to better understand the discovered vulnerabilities, validate the effectiveness of implemented solutions, and develop a plan to improve security controls



Service Deliverables
Reconnaissance, discovery and exploitation to identify security weaknesses and issues across technology, physical locations, and people in line with Blue team
Replay of successful attacks performed to cover scanning, lateral movement, domain compromise, data exfiltration, phishing, web proxy bypass, malware via web browser, and other successful tactics and techniques
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan, Portal access included
In-Depth Analysis and expert insights, Customised, actionable Remediation Strategies

Reporting Portal



Service Benefits

- Identify vulnerabilities and threats within overall security posture that help Blue team improve posture
- Use advanced techniques, tactics, and procedures to simulate real-world cyber-attacks
- Uncover security issues such as network infiltration, data exfiltration, staff awareness, and physical security
- Improve the organization's IR capability and procedures.
- Validate security controls and identify any weaknesses that need to be addressed before they can be exploited by attackers.
- Evidence of compliance and best practices
- Reduce the likelihood of a successful cyber-attack.

Red Team Services

Open-Source Intelligence (OSINT) Penetration Testing

Description

OSINT (Open-Source Intelligence) activities involve the collection and analysis of publicly available information from a variety of sources such as the internet, social media, news outlets, and government documents, identifying potential risks, by gathering intelligence on organizations, people, management, and partners. Often used as part of Red Team exercise or can be procured independently.

Service Goals

- Gather information from public sources, such as search engines, social media, blogs, and forums that may represent a cyber security risk
- Identify and address any weaknesses or vulnerabilities in a target organization.
- This information is used to create a record of the case being reviewed and to reduce the risk of successful attacks from malicious actors.

Process

Scoping → Recon → Vulnerability Discovery → Exploitation → Reporting → Support & Remediation Check

Scoping: Work with our expert security consultants and technical team to determine the scope of the OSINT investigation

Reconnaissance: Our penetration testing team employs all modern intelligence gathering techniques to uncover security and technical information about the scope under assessment.

Vulnerability Discovery: To identify exploitable security vulnerabilities, our penetration testing team utilizes their years of offensive security experience, testing expertise and knowledge of the latest hacking tools.

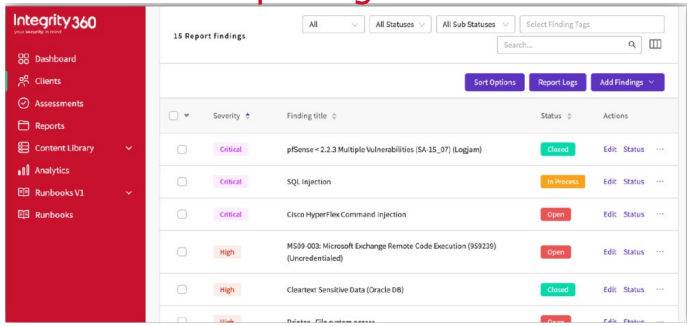
Exploitation: Once vulnerabilities have been found, our technical team devises and carries out a plan to exploit them while minimizing disruption of services.

Reporting: Upon completion of the technical procedures, our penetration testing team produces a report containing key findings and remediation guidance to address any discovered vulnerabilities.

Support & Remediation Check: We will provide you with all the technical support you need to better understand the discovered vulnerabilities and validate the effectiveness of implemented solutions.

Service Deliverables
Review and monitor information on the open, deep, and dark web, including sensitive data leaks
Identify social networks used by user or company and review content for sensitive information, and Examine availability of risky geographic information
Access old and cached online data for sensitive content
Explore DNS services, domains, subdomains and IP addresses
In-Depth Analysis and expert insights, Customised, actionable Remediation Strategies

Reporting Portal



Service Benefits

- Brand protection
- Detection of exposed sensitive information or credentials
- Identification of rogue or careless employees
- Overall security posture improvement
- Provide a valuable source of information for a variety of purposes
- Complement other forms of intelligence gathering to provide a more complete picture of a topic or event
- Cyber breach risk reduction
- Deter threat actors from targeting you

Integrity360

your **security** in mind

CST Portfolio – Audit Services

Audit Services

Build and Configuration Reviews

Description

Who better to evaluate the configuration of your infrastructural assets and systems than the people who know who to exploit any vulnerabilities, misconfigurations, and exposures? This service offers a detailed review of the configuration and build of these critical assets against best-practices with actionable recommendations for how to better secure your environment.

Service Goals

- Identify and validate security misconfigurations on a wide variety of asset types
- Provide recommendations for remediation of identified vulnerabilities, misconfigurations in line with best practices and improvements.

Service Options

Server, Desktop, and Laptop Build Reviews: Dive deep into the operating system configurations and security settings from an authenticated perspective. We scrutinise patch levels, security policies, user accounts, password practices, antivirus defences, file permissions, sensitive data, and logging capabilities to identify and remedy potential vulnerabilities.

Mobile Device and Citrix Breakout Tests: Assess the security integrity of mobile devices and Citrix remote access services, including device encryption, authentication mechanisms, data leakage risks, and breakout testing to ensure robust security against unauthorised access and data breaches.

Active Directory and Cloud Security Audits: Conduct comprehensive reviews of Active Directory environments and cloud configurations against best practices and industry standards. Our audits focus on domain configurations, trust relationships, patch management, password policies, and cloud component configurations to safeguard against unauthorised access and ensure data integrity.

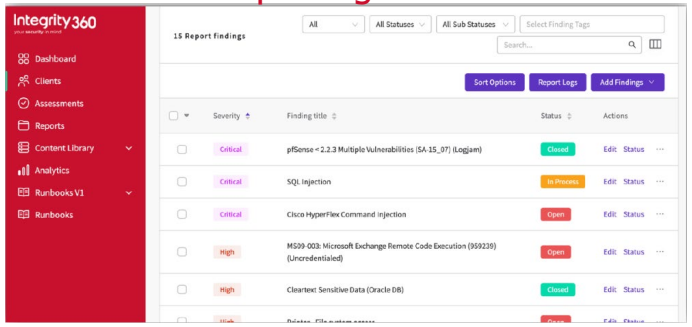
Web Server, Database, and Firewall Configuration Reviews: Evaluate the security setup of application servers, databases, and firewalls. We analyse installation, access controls, encryption, logging, and vulnerability to DoS attacks, ensuring your defences are resilient against intrusion and data exploitation.

VPN and Office 365 Configuration Reviews: Examine VPN endpoints and Office 365 setups for compliance with best practices, including encryption, authentication, data management, and email security. Our assessments identify configuration lapses and provide actionable recommendations for enhancement.

Network Device Configuration Review: Analyse routers and switches against security best practices to identify misconfigurations and insecure rules that could expose your network to cyber threats.

Service Deliverables
Identify misconfigurations and insecure system settings
Detecting outdated or unpatched software and firmware, including third-party components
Evaluating the security of communication protocols and encryption standards.
Testing for weak, default, or compromised credentials; Investigating possibilities for privilege escalation and lateral movements within the network.
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan, Portal access included

Reporting Portal



Service Benefits

- Proactively understand vulnerabilities & misconfigurations of critical assets
- Streamline patch management
- Uncover insecure configurations
- Risk-based prioritisation
- Alignment with best practice
- Compliance with standards and regulation
- Protection of sensitive data
- Enhance security and resilience
- Reduced risk of cyber breaches

Audit Services

Threat Modelling Service for Applications

Description

Our Threat Modelling Service is designed to identify, assess, and prioritise potential threats due to your organisation's new or even existing applications. By simulating attacker behaviours and analysing possible vulnerabilities, we provide a comprehensive framework that not only identifies but also mitigates risks to the applications even before they are released and can be exploited.

Service Goals

- Lower cyber risk by systematically identifying and mitigating threats to new applications proactively
- Enhance the organisation's ability to respond to and recover from security incidents more efficiently through early identification of potential attack vectors and preparation of effective mitigation strategies
- Improved application security for new developments

Threat Modelling Process

Interviews with key stakeholders → Data flow diagram (DFD) → Threat Identification → Risk Analysis → Security Requirements

Interviews with key stakeholders: This phase involves talking through the system with asset owners, engineers or developers that can provide insights on the low-level functionalities of the system, the key components involved in the intended deployment and understanding the system's security goals.

Data flow diagram (DFD): With information gathered from stakeholders, design documents and deployment architecture, we build a data flow diagram model of the system involving various components and their respective trust boundaries. The DFD will then be reviewed and finalised by the stakeholders to confirm understanding.

Threat Identification: Based on the DFD and design documents, Integrity360 will then identify possible threats that apply to the system. These threats depend on the deployment context and the technology stack used for developing the system.

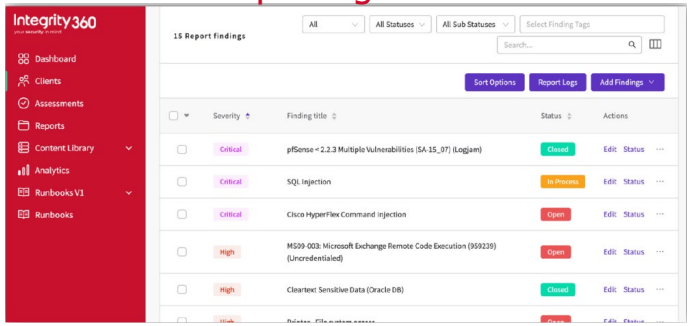
Risk Analysis: With the threats identified, a risk analysis will be performed to determine their risk based on technical, business impacts and the likelihood of a threat materialising. [{Business Impact + Technical Impact} * Likelihood = Overall Risk], or a standard CVSS 3.0 score could be used.

Security Requirements: Security requirements are the outcome of a threat modelling exercise and are designed to address threats identified to the system and risk reduction to be applied to the system. Once addressed, the system should undergo requirement testing and cyber security testing to identify any implementation pitfalls/gaps.

Service Deliverables

Service Deliverables
Stakeholder interviews and input collection
Data flow mapping and threat identification
Risk analysis and identification of security requirements
Identification of risks across Design phase, development phase, coding errors, misconfigurations, or insecurities, test phase coverage gaps, unidentified threat vectors, deployment, maintenance, compliance, regulation and continuous monitoring.
Comprehensive Report - Executive Summary, Detailed Technical Report, and Remediation Plan, Portal access included

Reporting Portal



Service Benefits

- Requirements and Design gaps detected early in the development process
- SDLC maturity improved
- Threats are addressed and security posture improved at an early stage
- Development effort is reduced by considering security at the design stage to avoid costly code rewrites, & design changes
- Prevention of security incidents
- Improved developer security awareness

Audit Services

Secure Code Review

Description

This service is designed to reinforce the security of your software development process. By rigorously analysing the source code of applications, it identifies and addresses vulnerabilities, ensuring adherence to the best coding practices. Tailored for diverse IT environments, it scrutinises every aspect of the code, covering servers, desktops, mobile devices, and cloud-based applications.

Service Goals

- To detect and confirm vulnerabilities in application source code that could be exploited by cybercriminals to allow unauthorised access, data breaches, or other security threats
- Evaluate the potential impact and probability of identified vulnerabilities, provide detailed descriptions and, where applicable, proof-of-concept examples to demonstrate how they might be exploited
- Provide guidance on how to rectify identified vulnerabilities, including best practices for secure coding, improvements to existing code, and strategies to prevent similar vulnerabilities in future development

Services Available

- Best Practices Adherence
- Input Validation Assessment
- Error Handling Assessment
- Session Management Assessment
- Authentication Assessment
- Cryptographic Assessment
- Logging Assessment
- Denial of Service Assessment
- Deployment Review
- Secure Software Development Consultancy

Service Deliverables
Identifying code mis practices and non-adherence to secure coding standards
Detecting the use of outdated or vulnerable libraries and dependencies
Assessing the robustness of error handling and input validation mechanisms
Evaluating authentication, authorisation, and session management security
Testing for security weaknesses in data encryption and storage practices
Investigating secure integration of code within the broader IT and cloud infrastructure
Detailed report and remediation recommendations

Service Benefits

- Early detection and resolution of vulnerabilities in code
- Alignment with best practice
- Streamlined maintenance
- Identification of insecure coding practices
- Compliance
- Prevention of exploitation and data leakage
- Improved security posture
- Continuous learning and development

Integrity360

your **security** in mind

CST Portfolio – User Testing and Training

User Testing and Training Services

Phishing Campaign

Integrity360
your security in mind

Description

Cybercriminals use phishing, the fraudulent attempt to obtain sensitive information such as credit card details, login credentials, and other valuable data by disguising as a trustworthy organization or reputable person in an email communication. This service simulates a phishing campaign to test the security awareness of your organisation's staff.

Service Goals

- Identification of vulnerabilities in email security controls
- Measurement of staff awareness
- Improved targeting of training
- Increased staff awareness of phishing attacks

Process

Scoping → Recon → Pretexting → Execution → Analysis → Reporting → Support

Scoping: Defining the scope of the target organisation, including specific areas of interest and the type of information to be gathered

Reconnaissance: Gathering publicly available information about the target organization, such as searching through search engines, social media, and forums. Identifying and collecting relevant information such as e-mails, telephone numbers, usernames, given names, addresses, etc.

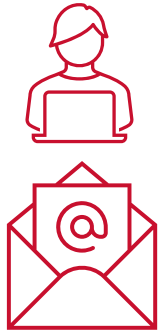
Pretexting: The testing team will develop a pretext, or a believable scenario, to use when attempting to manipulate employees, designed to elicit the desired response from the employee, such as providing sensitive information or opening a malicious attachment

Execution: Sending developed phishing emails and recording reactions on these emails

Analysis: Analyzing the gathered information to identify potential vulnerabilities and areas of interest

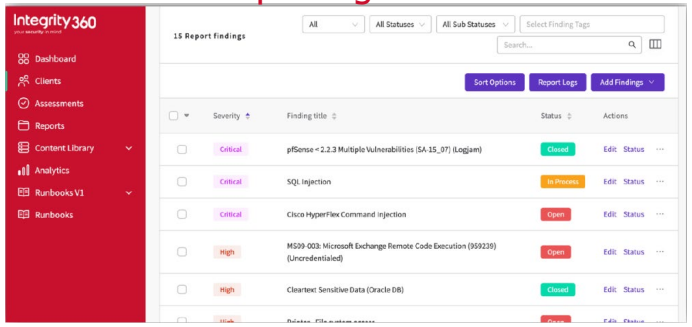
Reporting: Compiling a report of findings and recommendations for further investigation or action

Support: Providing additional guidance and support to help the client understand and utilize the gathered information



Service Deliverables	Basic	Intermed-iate	Advanced
Campaign with Basic phishing email templates	✓		
Campaign with Intermediate templates, more elaboration more complex to detect		✓	
Campaign with Advanced custom templates, targeted user accounts. Use of OSINT sources			✓
Detailed report on nr of employees who fell for the phishing attempt, failure of controls, recommendations, with portal access	✓	✓	✓

Reporting Portal



Service Benefits

- Identify vulnerabilities in email security controls
- Measuring and raising staff awareness
- Improving training
- Testing reporting and incident response
- Increased Compliance
- Reduced risk
- Improved resilience

User Testing and Training Services

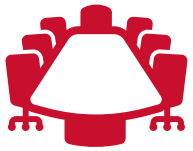
Cyber Security Awareness Training

Description

A Security Awareness Course is a way to empower employees with all the needed knowledge about some basic but comprehensive security concepts. Throughout the course, learners will be introduced to best practices for protecting their personal and professional information, including password management, safe browsing habits, and secure communication practices. Basic, Intermediate, and Advance Options available.

Target Audience

- Large enterprises that have complex networks and numerous IT assets that require protection from cyber threats
- Small and medium-sized businesses that may not have dedicated security personnel or resources to manage and maintain their infrastructure and application security
- Government agencies that have sensitive information and systems that need to be secured against unauthorized access
- Service providers that manage critical infrastructure and applications, such as energy or financial services, and need to ensure the security of their systems to prevent disruptions to their services
- Organizations that are subject to compliance regulations, such as PCI DSS, HIPAA, or GDPR, and require regular security assessments to maintain compliance



Service Goals

- Educate technical and non-technical audiences about the underlying risks & consequences of cyber-attacks
- Train employees on how to identify and how to respond to security threats
- Foster a culture of security within the organization
- Empower employees to take ownership of their personal information and safeguard information Ensure compliance with industry and regulatory standards for data privacy and security
- Minimize the potential risk caused by human error and insider threats

Service Deliverables
A comprehensive security awareness training program that covers a variety of topics, such as phishing, social engineering, password management, and safe browsing practices.
Training sessions for audiences of all types: novices, intermediates or professionals.
Training materials including visual presentations, sources of reference, live mockup demonstration of attacks and handouts that employees can access and refer to as needed.
Measurement of the effectiveness of the course and identify areas for improvement.
Incident response plans and procedures what to do in the event of a security incident
Metrics and reporting to track employee participation and monitor the overall effectiveness

Service Benefits

- By regularly delivering/attending Cybersecurity Awareness Courses, organizations can protect their reputation and maintain customer trust
- Enhance overall security posture through heightened knowledge and awareness and ultimately reducing the risk of social engineering attacks and data breaches
- By utilizing the Advanced Level Course, organizations can enhance their applications and infrastructures.

User Testing and Training Services

Social Engineering Testing

Integrity360
your security in mind

Description

Social engineering test methodology involves simulating real-world social engineering attacks to assess an organisation's susceptibility to these attacks. This service assesses your organisation's people, processes, and procedures through a combination of email phishing, vishing, smishing and onsite physical assessments. By simulating real-world scenarios, we can identify weaknesses in your security and provide recommendations for improvements.

Service Goals

- Identify vulnerabilities in security controls and processes
- Assessing employee awareness of security risks and best practices
- Testing effectiveness of security controls, access controls, password controls and intrusion detection
- Meeting compliance standards

Process

Scoping → Recon → Pretexting → Execution → Analysis → Reporting → Support

Scoping: Defining the scope of the target organisation, including specific areas of interest and the type of information to be gathered

Reconnaissance: Gathering publicly available information about the target organization, such as searching through search engines, social media, and forums. Identifying and collecting relevant information such as e-mails, telephone numbers, usernames, given names, addresses, etc

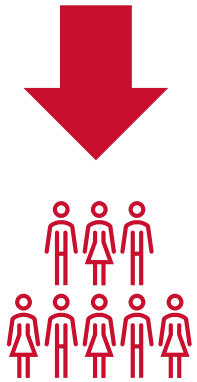
Pretexting: The social engineering team will develop a pretext, or a believable scenario, to use when attempting to manipulate employees. The pretext should be designed to elicit the desired response from the employee, such as providing sensitive information or opening a malicious attachment.

Execution: Contact, manipulation and exploitation. Manipulate and deceive targets using psychological tactics to gain access to sensitive information or systems, exploit the acquired data for launching further attacks, and cover tracks to avoid detection.

Analysis: Analyzing the gathered information to identify potential vulnerabilities and areas of interest

Reporting: Compiling a report of findings and recommendations for further investigation or action

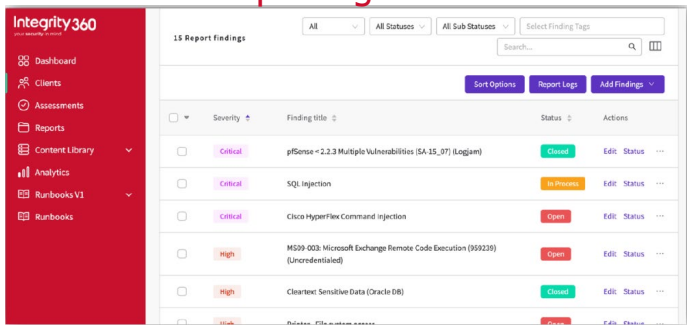
Support: Providing additional guidance and support to help the client understand and utilize the gathered information



Service Deliverables

Service Deliverables
Social Engineering tests aligned with specific areas of interest defined in scope
Executive summary: A high-level overview of the test, including the scope, severity level and key findings.
Detailed technical report: A more in-depth look at the issue identified, including descriptions, potential impact, severity level, screenshot captures and recommendations for remediation.
Online access to reporting portal

Reporting Portal



Service Benefits

- Protect brand and reputation from ransomware and spear phishing attacks
- Ensure members of organisation do not get tricked and disclose sensitive information
- Validate that policies and procedures are understood and followed
- Raise awareness among employees and management about the dangers of social engineering attacks
- Minimise the risk of a successful attack

User Testing and Training Services

Malware Defence Test

Description

A Malware Defence Test aims to determine the organisation's vulnerability to infection by malicious software. It verifies that security controls, such as mail filtering, anti-virus and physical media restrictions, are in place and are effective in protecting users from malicious content.

Service Goals

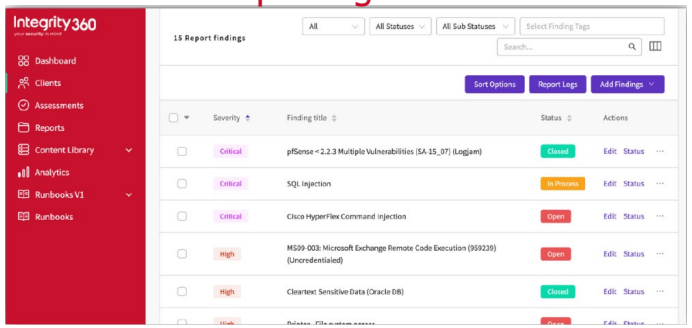
- Identify and mitigate vulnerabilities
- Enhance overall security posture against evolving threats, including phishing and web proxy bypass
- Assess and fortify endpoint security against various attack vectors
- Mitigate the impact of potential risks, including those associated with zero-day vulnerabilities

Target Audience

- Large enterprises with complex IT environments.
- Enterprises across various sectors, including finance, healthcare, government, and education.
- SMEs seeking to enhance their cybersecurity measures.
- Government entities requiring secure public service delivery.
- Healthcare, utilities, and other sectors dependent on robust security.

Service Deliverables
Malware Defence tests aligned with specific areas of interest defined in scope
Executive summary: A high-level overview of the test, including the scope, severity level and key findings.
Detailed technical report: A more in-depth look at the issue identified, including descriptions, potential impact, severity level, screenshot captures and recommendations for remediation.
Online access to reporting portal

Reporting Portal



Service Benefits

- Fortify organisation's security stance against evolving threats like phishing and endpoint attacks
- Meet industry standards by continually assessing and enhancing malware defence capabilities
- Actively identify and resolve vulnerabilities
- Strengthen against social engineering tactics
- Enhance defences against malware infiltrations through browser-based exploits

Integrity360

your **security** in mind

Why Integrity360 for Cyber Security Testing Services?

Integrity360
your security in mind

Why Integrity360 for Cyber Security Testing Services?

People

>30 Pentesters

Activity

>500 tests completed in last 12 months

Methodology

Industry-leading methodology with 100% exploit success rate

The Integrity360 Difference

- Providing high-quality security testing services since 2005
- Extensive experience with the latest tools and technologies
- Breadth of support - small business to large enterprise
- We prioritise manual testing as a critical component
- Flexible working schedules, including night shift options
- Services in multiple languages
- Industry-leading cybersecurity training & certifications
- Post-testing support excellence
- Full suite of complementary security services available
- All results in portal maintained for 1 year

Heavily Certified and Accredited

OFFENSIVE security OSCP
OFFENSIVE security OSCE
CISSP ISC2
GIAC www.giac.org
EC-Council
CREST
PEN TEST
STAR Intelligence-led PT
CSIR
National Cyber Security Centre a part of GCHQ
CHECK – *in progress*

Pan European Coverage

Why Integrity360

Integrity360
your security in mind

Expert testers + Advanced tools + Proven Methodology= Success

nessus Professional

Grapefruit

Burp Suite Professional

FOCA

ReadyAPI

SHODAN

CORE IMPACT
CORE SECURITY

FRIDA

DataSploit

theHarvester

cobaltstrike
by HelpSystems

spiderfoot

MALTEGO

OBJECTION
RUNTIME MOBILE EXPLORATION
GIT.IO/OBJECTION

Wireshark

KALI LINUX

SoapUI

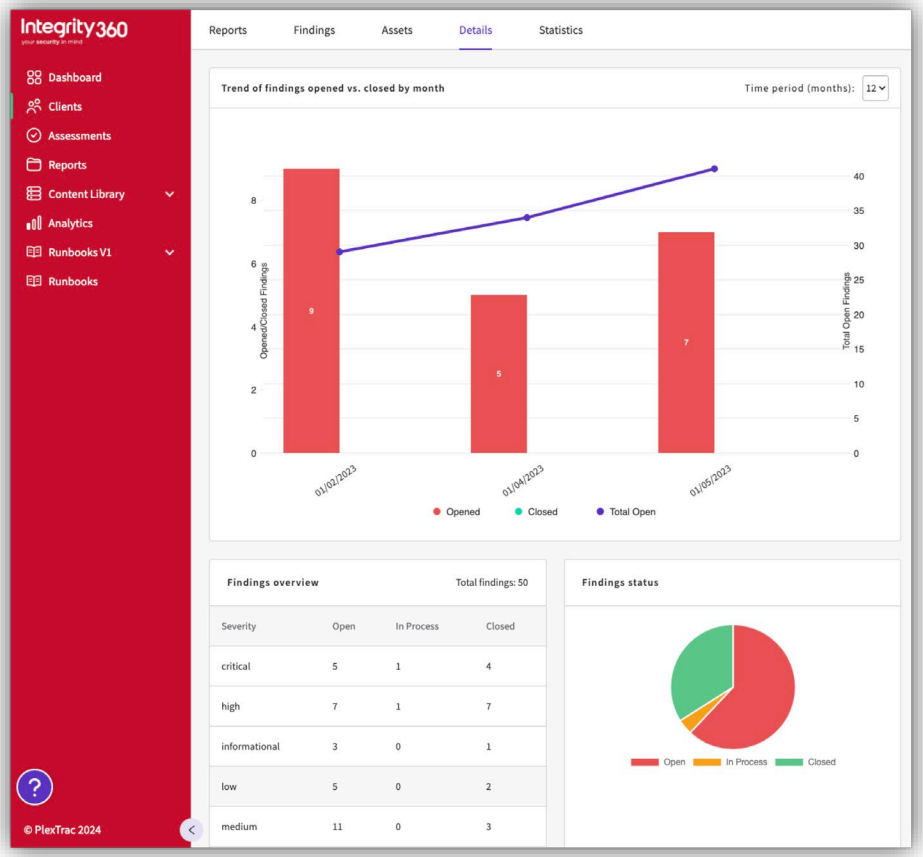
MOBSF

Why Integrity360

Vulnerability Portal

Through the Integrity360 Vulnerability Portal, clients will receive a comprehensive report outlining the security issues discovered in the targeted applications.

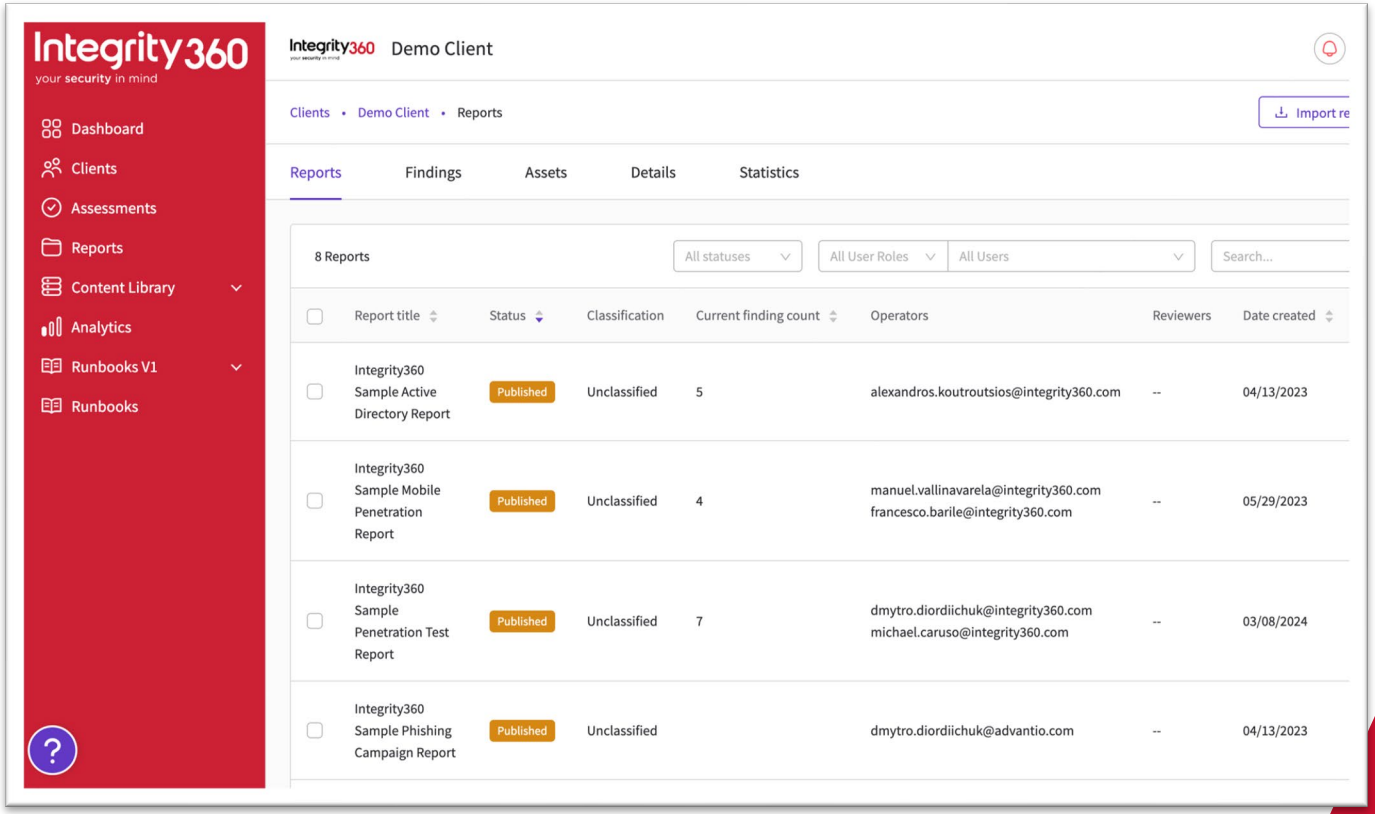
- All reports and vulnerabilities in one place
- Included in each CST service as a complimentary service
- Remediation tracker with the history of remediation
- Vulnerabilities assignment
- Assets inventory
- Email notifications



Why Integrity360

Vulnerability Portal - Client Access

- Each client has dedicated space
- Permissions doesn't allow to access other spaces and findings
- Clients can have several tenants in the console
- 24/7 on-line access for 3 users

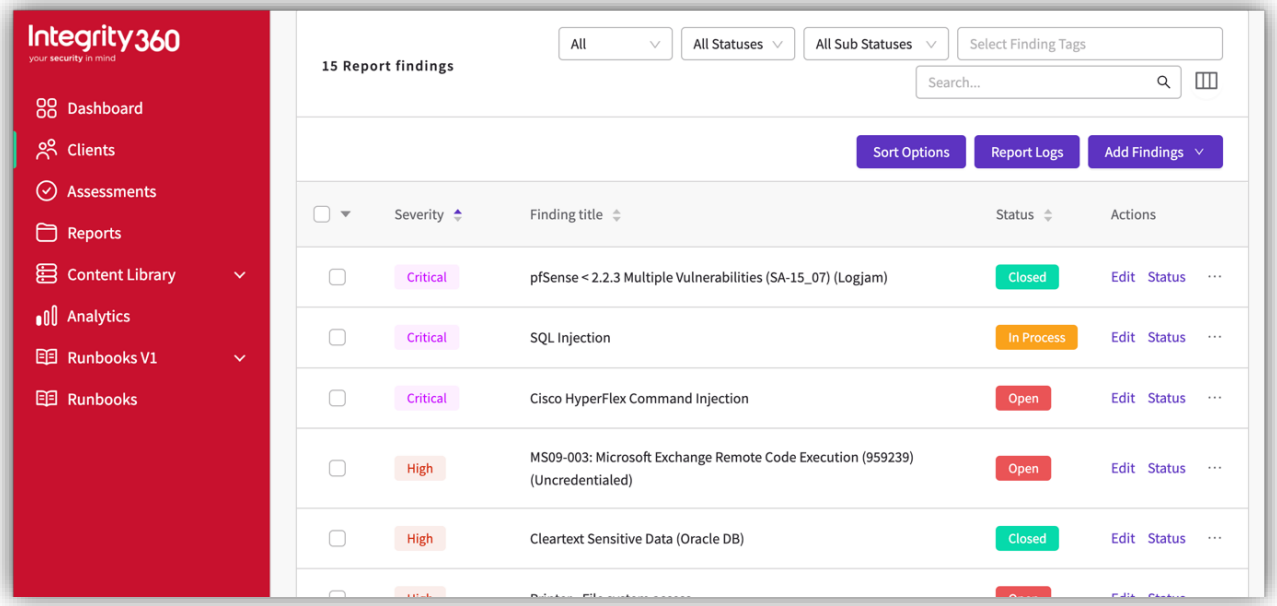


Why Integrity360

Vulnerability Portal – online report details

Each finding is assigned a risk rating and includes evidence that the stated flaws exist, as well as examples and best practices that developers can use to identify and resolve the stated issue.

- Title
- Risk score
- Remediation status
- Exploitation status
- Technical description
- Steps to reproduce and evidence of exploitation
- Remediation actions and references



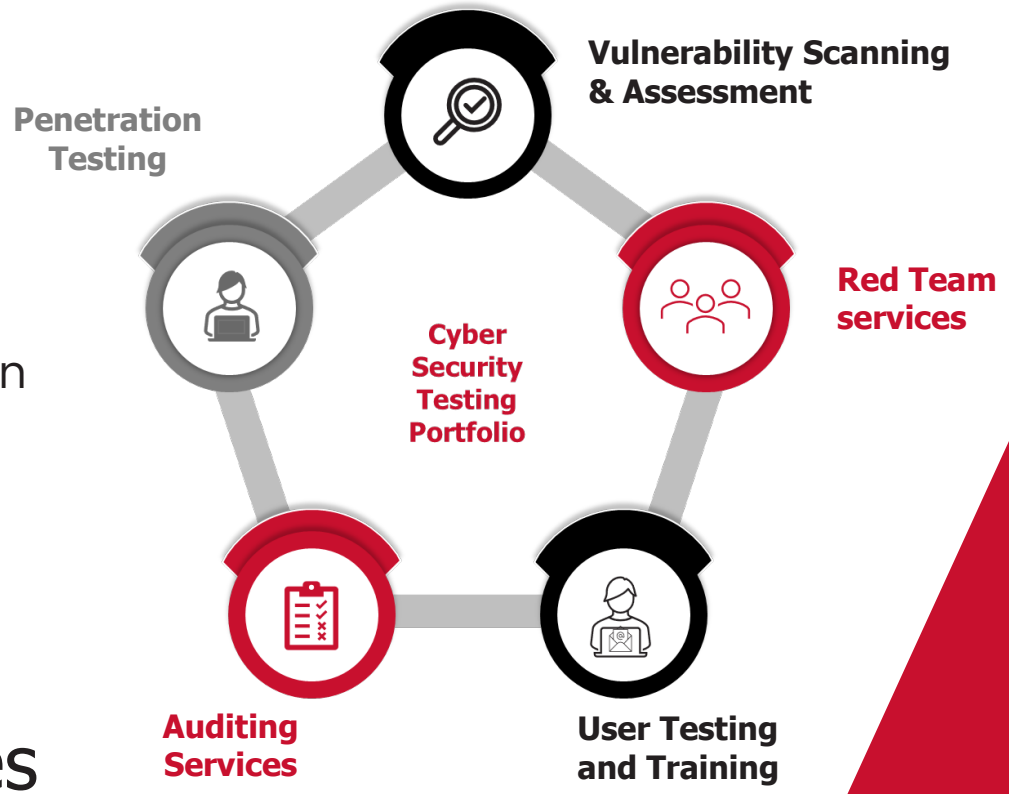
Integrity360

your **security** in mind

Summary and Next Steps

Summary and Next Steps

- Cyber Security testing is essential for
  - Identification of risks and exposures
  - Assisting with remediation planning and execution
  - Addressing Technical, Human, and Physical security
  - Complying with standards and regulation
- Integrity360 is a leading provider of full suite cyber security testing services
- Consider you needs, scope and cadence requirements, or ask us for guidance
- Request a Proposal



Integrity360

your **security** in mind

Thank you

Your Name Position

your.email@integrity360.com