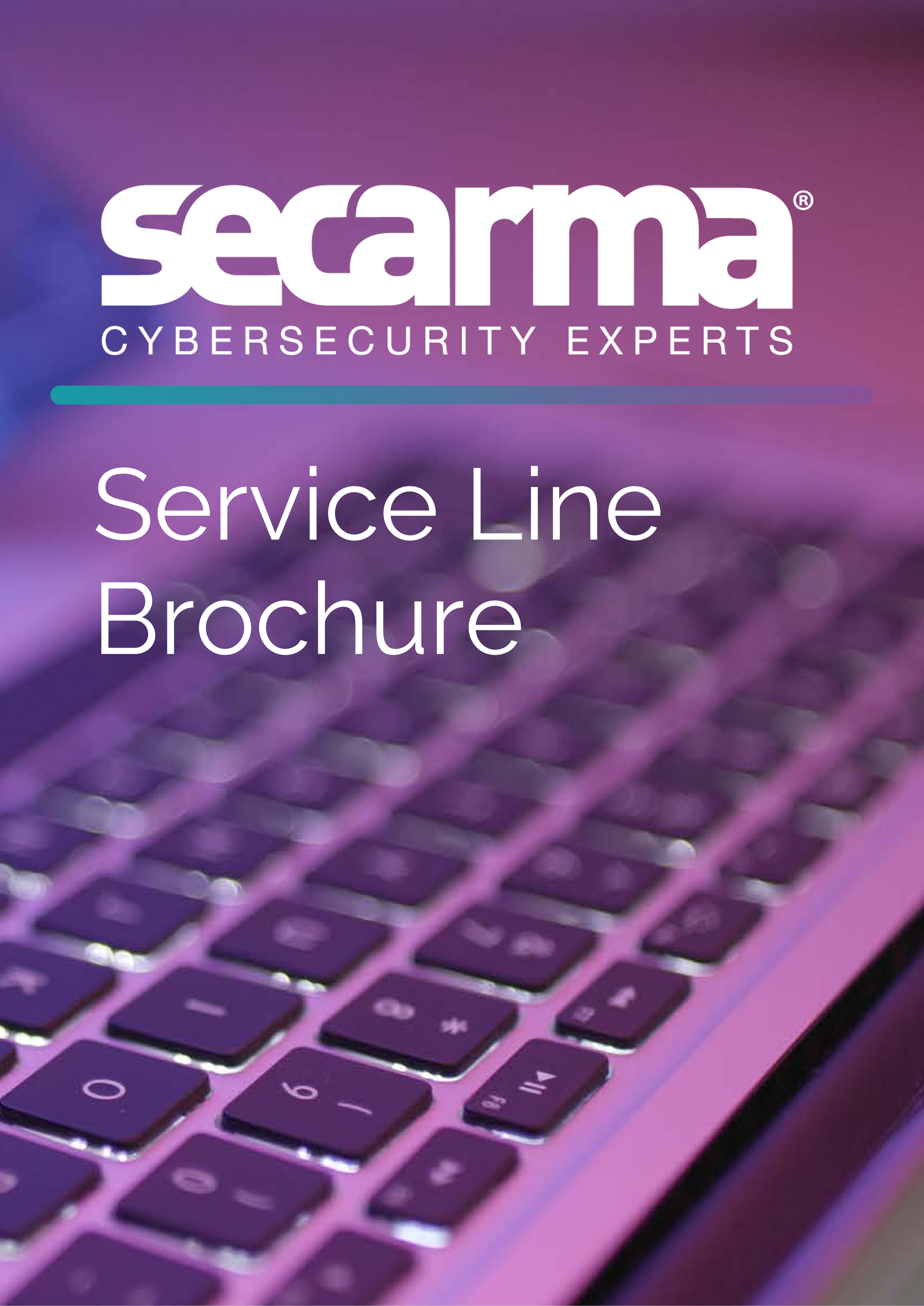
secarma®

CYBERSECURITY EXPERTS

Service Line Brochure



Why Secarma?

Secarma is an independent cybersecurity consultancy that utilises ethical hacking methods to test the strength of your organisation's existing security posture.

Drawing on almost 20 years in business, and with a strong reputation to match, Secarma is the best choice for your cybersecurity needs; we're continuously investing in research, training, and technical development to ensure we provide our customers with the best service.

.Our consultative approach is how we stand out from the competition; we put you in touch with one of our experienced testers from the get-go, meaning you'll have an expert by your side throughout the process. Our consultants are all highly accredited, passionate, and proficient not just at hacking into your systems, but also communicating to senior management and security teams how they achieved this.

By working with us, you can give your security team a better idea of what to expect, and prepare your business for real-world attacks.

Accreditations

At Secarma, our experts pride themselves on their up to date certifications. Your organisation's security and compliance are of top importance to us, which is why we've achieved the following accreditations:

CYBER ESSENTIALS CERTIFIED PLUS

CREST ACCREDITED

bsi. UKAS MANAGEMENT SYSTEMS 0003

nqa. ISO 9001 QUALITY MANAGEMENT UKAS MANAGEMENT SYSTEMS 015

CHECK
IT Health Check Service

secarma®
CYBERSECURITY EXPERTS

Our Services

With an ever expanding threat landscape, remote working, and GDPR regulations, cybersecurity services have never been more crucial for businesses.

Cybersecurity isn't a one size fits all process, and there are a number of options available to suit your needs and company objectives. Here are a few of ours:

Penetration Testing

A human-led simulation of a real cyberattack, designed to exploit your system's previously undetected vulnerabilities and determine the real-world risk to your business.

Security Training

Hands-on courses that teach you about security vulnerabilities and how to exploit them. We teach you how to break systems, then build them in a more resilient way.

Consultancy

We work with you to help you meet security objectives, develop your understanding of your organisation's security posture, test its defences, and prepare for worst-case scenarios.

Vulnerability Scanning

24/7 intelligent scanning that gives you a full overview of your current security posture, allowing you to track remediation, spot issues, and identify your areas of risk.

secarma®
CYBERSECURITY EXPERTS

Penetration Testing

The threat of cybercrime continues to loom large over organisations, but is your business fully prepared to fight back? The need to test the strength of your security is no longer just a ‘nice to have,’ it’s a must.

We utilise human intelligence to gain access to your organisation’s environment. The goal is to locate vulnerabilities by simulating a cyber-attack, but instead of breaching your data or injecting malware, we review your security posture from the inside and help you make it stronger.

Why Invest in Offensive Security?

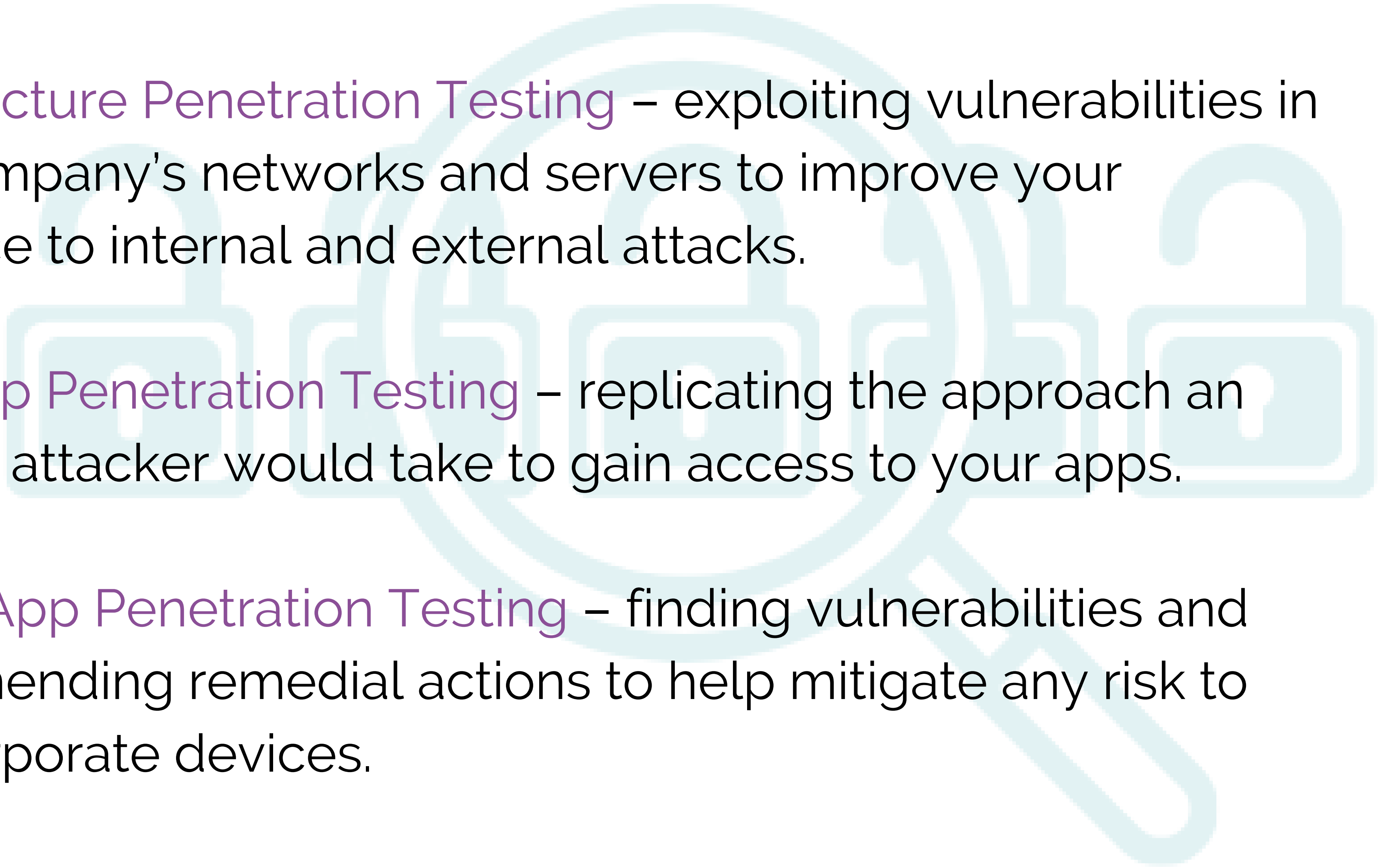
How do you know your systems are secure if you don’t test them regularly? In an ideal world for our customers, we wouldn’t find any way to break their systems, but that’s rarely the case. And isn’t it better that we find our way into your systems ethically, rather than a cybercriminal hacking in and causing havoc?

Our in-depth reviews give you an overview of your security from a hacker’s perspective, helping you reach the next level of cybersecurity maturity.

secarma®
CYBERSECURITY EXPERTS

Services

Our experienced consultants utilise similar tools and techniques to real-world threat actors, meaning we can simulate realistic exploits without harming your systems in any way. These services include:



Infrastructure Penetration Testing – exploiting vulnerabilities in your company's networks and servers to improve your resilience to internal and external attacks.

Web App Penetration Testing – replicating the approach an external attacker would take to gain access to your apps.

Mobile App Penetration Testing – finding vulnerabilities and recommending remedial actions to help mitigate any risk to your corporate devices.

Wireless Penetration Testing – a full review of your wireless network to help you provide secure remote working for your staff.

Vulnerability Scanning – 24/7 intelligent scanning that gives you a full overview of your current security posture in real time.

Infrastructure Penetration Testing

Infrastructure Penetration Testing exploits vulnerabilities in your company's networks and servers to improve your resilience to attacks. We provide context around the vulnerability, threat and impact, as well as tailored advice on how to protect your critical operating systems and networks.

.

WHO IS IT FOR?

Infrastructure testing is for organisations who wish to gain a real-world view of their security posture.

For example, you may want to know if your customer data or staff payroll information is being stored and transmitted in a secure manner.

Alternatively, you might need to know the security weaknesses in your Internet-facing IT systems — such as email servers, routers, and web servers that host e-commerce websites.

If you've changed your systems, vulnerabilities could have been introduced. We may also find services that you didn't know you had exposed.

HOW CAN WE HELP?

We use a range of manual techniques, automated security tools and a proprietary methodology, to identify, validate, and exploit security vulnerabilities. Each test we conduct is individually tailored to your company's requirements, and the specific systems to be tested.

We're able to test individual systems right through to complex and extensive enterprise-wide infrastructures. We can also focus our investigation on your company's responsiveness to a particular type of attack, such as social engineering or ransomware.

WHAT WE TEST

By utilising similar tools and techniques to real-world threat actors, our team will identify, verify and priorities exploitable weaknesses within your infrastructure. Our tests include:

- **Known Vulnerabilities** - Missing security updates is a common weakness that can lead to services, operating systems and applications being compromised.
- **Default Misconfiguration** - Systems are often configured by default with compatibility in mind which can lead to insecurities such as weak encryption being used
- **Access Control** - Authentication systems often have weaknesses such as username enumeration, lack of bruteforce protection, or even just common and weak passwords.
- **Service Flaws** - Services accounts may have weaknesses that allow a threat actor to leverage the service for privilege escalation, such as insecure permissions or executable storage.

secarma®
CYBERSECURITY EXPERTS

Web App Penetration Testing

As a direct interface with clients, applications are usually designed with functionality and aesthetics in mind, with security considerations coming in second place. However, web app security risks can be significant, so by investing in web application penetration testing, you can stay one step ahead.

.

WHO IS IT FOR?

With fewer companies operating on a purely local scale, remote working and flexible office hours remove the geographical barrier to business. To enable such flexible working for your staff, your clients and external partners, the typical solution is a combination of hot-desking and wireless networking.

WiFi networks are not generally afforded the same level of physical network access controls as they are with traditional Ethernet implementations. Furthermore, it is commonplace to provide 'guest' or Bring Your Own Device 'BYOD' access to wireless networks, which create an increased risk of rogue devices being introduced.

Whilst this provides opportunities for growth, you may also be opening new avenues for compromise by attackers.

HOW CAN WE HELP?

We are able to conduct a full review of your wireless network either as a standalone assessment or as part of a larger scale investigation into your infrastructure security posture.

We will often deliver a standalone wireless assessment from a black-box perspective, but we may also combine with an architecture review (thereby utilising a white-box approach), enabling a more thorough analysis.

WHAT WE TEST

We check the configuration of your wireless technologies, test for rogue access points that may have been installed, and determine whether less secure Wi-Fi networks can provide an avenue to the corporate network. We will also check that wireless security standards around SSIDs, encryption and authentication are all in place. We most commonly find flaws relating to:

› Encryption protocols

The first line of defence for a wireless network. If an attacker can crack the encryption then they can gain access to the network.

› Authentication

As an example the PSK acts as a password to authenticate a user to the network. Passwords that are weak, or not stored securely, offer an easy avenue onto the network for an attacker.

› Segmentation

Weak or absent network segregation can lead to the disclosure of sensitive data, access to (or compromise of) internal systems, and the targeting of internal users.

Mobile App Penetration Testing

Attacks against mobile apps are having devastating effects on organisations. Mobile devices, and the applications they use, have quickly become a core part of everyday life, which is why mobile application security testing is a must when looking to fortify your business against cyberattacks.

.

WHO IS IT FOR?

This service is for organisations who develop mobile applications, that handle sensitive data or interact with backend systems. Just as bespoke web applications can create paths in for malicious users, so can mobile applications.

Whether it's an application developed for public use or something internal for you team, we can give an independent view to the risk exposure it causes for your business.

HOW CAN WE HELP?

Our Mobile Application Security Testing service will find vulnerabilities, prioritise them and recommend remedial actions. This will help you to understand and then mitigate your risks.

For development teams, we will also help you integrate secure development practices into your development lifecycle, baking in security-by-design and improving the security of subsequent applications.

In addition to penetration testing applications, we can also provide code-assisted penetration testing – where we review the code alongside the penetration testing activities to allow for a more efficient security assessment or to allow for a higher level of assurance.

WHAT WE TEST

Our mobile application testing methodology looks at the system as a whole. We review the application itself, but also the interactions with backend systems such as APIs and data stores.

Using the OWASP Mobile Top 10 as a foundation, we review all areas of application functionality, such as:

- **Application logic**
  Abuse of functionality and logical flaws within applications.
- **Authentication**
  Username enumeration, brute force attacks, and credential stuffing.
- **Authorisation**
  Insufficient credential and session management.
- **Cryptography**
  A review of the cryptographic configuration of sensitive data in storage and transit.
- **Code Review**
  We can review code for deprecated or vulnerable functions, as well as reviewing the quality of security implementations.

secarma®
CYBERSECURITY EXPERTS

Wireless Penetration Testing

Wireless networks are a potential weak point in the corporate perimeter and an enticing entry point for cybercriminals. If an attacker gains access to your wireless networks, they can begin to target internal systems. Stay one step ahead with wireless penetration testing – a vital step in keeping your wireless access points, production applications, and data repositories secure.

WHO IS IT FOR?

With fewer companies operating on a purely local scale, remote working and flexible office hours remove the geographical barrier to business. To enable such flexible working for your staff, your clients and external partners, the typical solution is a combination of hot-desking and wireless networking.

WiFi networks are not generally afforded the same level of physical network access controls as they are with traditional Ethernet implementations. Furthermore, it is commonplace to provide 'guest' or Bring Your Own Device 'BYOD' access to wireless networks, which create an increased risk of rogue devices being introduced.

Whilst this provides opportunities for growth, you may also be opening new avenues for compromise by attackers.

HOW CAN WE HELP?

We are able to conduct a full review of your wireless network either as a standalone assessment or as part of a larger scale investigation into your infrastructure security posture.

We will often deliver a standalone wireless assessment from a black-box perspective, but we may also combine with an architecture review (thereby utilising a white-box approach), enabling a more thorough analysis.

WHAT WE TEST

We check the configuration of your wireless technologies, test for rogue access points that may have been installed, and determine whether less secure Wi-Fi networks can provide an avenue to the corporate network. We will also check that wireless security standards around SSIDs, encryption and authentication are all in place. We most commonly find flaws relating to:

Encryption protocols

The first line of defence for a wireless network. If an attacker can crack the encryption then they can gain access to the network.

Authentication

As an example the PSK acts as a password to authenticate a user to the network. Passwords that are weak, or not stored securely, offer an easy avenue onto the network for an attacker.

Segmentation

Weak or absent network segregation can lead to the disclosure of sensitive data, access to (or compromise of) internal systems, and the targeting of internal users.

secarma®
CYBERSECURITY EXPERTS

Vulnerability Scanning

Vulnerability Scanning is a 24/7 intelligent scanning service that gives you a full overview of your current security posture, allowing you to track remediation, spot vulnerabilities, and identify your areas of risk.

WHO IS IT FOR?

Vulnerability scanning software is for organisations who want to continually (or as and when required) test their applications and infrastructure to catch vulnerabilities before they cause an issue.

For organisations who need a quick, easy, flexible and affordable way to respond to and manage vulnerabilties, AppCheck offers unlimited testing 24 hours a day, 365 days a year. Its dashboard presents a fully configurable view of your current security posture, allowing you to track remediation, spot vulnerabilities

HOW CAN WE HELP?

An effective solution for identifying and reporting vulnerabilities throughout the year. Whilst it can't reach the same depth as a manual penetration test, it works particularly well alongside Penetration Testing to achieve a balance of depth and frequency. AppCheck can help with:

- **Quick & frequent vulnerability scanning:** Scans only take seconds to configure and start, and can be performed 24 hours a day, 365 days a year.
- **Security by design:** Perform scans throughout an applications lifecycle, ensuring it's secure before launching, and in the future.
- **Reporting & remediation:** Provides detailed reports with easy to follow remediation advice.
- **Vulnerability management dashboard:** A fully configurable view of your current security posture.

WHAT WE TEST

AppCheck has two distinct scanning engines designed to test web applications and computer systems for vulnerabilities:

Applications

For each URL configured with the scan, AppCheck will map out the application and mimic a typical application user. Methodical security testing will be performed to confirm the vulnerabilities

Common vulnerabilities detected during the web application scan include; Injection flaws such as SQL, NoSQL, XML, Code, and command injection, cross-site scripting and hundreds of other vulnerability classes arising from insecure code.

Internal & External Infrastructure

The infrastructure scan identifies accessible services which are then probed for vulnerabilities.

Common vulnerabilities detected during the infrastructure scanning phase include; missing operating systems patches, weak administrative passwords and access control vulnerabilities.

Vulnerability Scanning

POWERED BY AppCheck
ACCURACY IS EVERYTHING

secarma®
CYBERSECURITY EXPERTS

Security Training

Our Security Training courses allow practical experience breaking security systems, before teaching attendees how to build systems in a more resilient way.

Our labs are designed to educate IT professionals on different security vulnerabilities by taking them through the process of a penetration test, step by step. We'll show attendees the tools and techniques we use during real-world engagements, so they know what to expect should an attack on their organisation occur.

Why Invest in Security Training?

Many security flaws can be subtle or difficult to spot if you're not well versed in common vulnerability types and testing methods. By using the hacker's point-of-view throughout the training course, not only will we teach IT professionals hot to detect attacks, but also give guidance on how systems and applications could be hardened, making exploitation action more difficult.

Our hands-on security training courses are available across the UK and remotely.

What to Expect

Here's a general outline of what happens during our training sessions:

Mapping and Intelligence Gathering

Before the engagement begins, we'll map the attack surface to discover live hosts, services, and versions, as well as mapping application functionality.

Vulnerability Discovery

We'll demonstrate methods of finding and confirming vulnerabilities and highlight how to minimise false positives.

Proof of Concept and Confirmation

Where vulnerabilities are discovered, a proof of concept exploit will be created to demonstrate the potential business risk. This ensures that false positives are removed by manually confirming and demonstrating all discovered vulnerabilities.

Exploitation

We'll show you how to discover weaknesses within exposed applications and leverage those weaknesses to demonstrate as much business risk as possible. In other words, you get to step into the shoes of a hacker for the day.

Remediation

We'll provide guidance on remediation, teaching candidates how to build systems in a more resilient way.

secarma®
CYBERSECURITY EXPERTS

Hacking & Defending Networks

Our Hacking and Defending Networks sessions allow you to get practical experience breaking security systems, before teaching you how to build them in a more resilient way. Learn how to compromise network infrastructure, from zero access to Domain Admin.

WHO IS IT FOR?

Our infrastructure hacking course is designed to teach systems administrators the tools and techniques we use when targeting network infrastructure during real world penetration tests.

It's also a useful course for those looking to break into Penetration Testing who want a first step on the journey.

HOW CAN WE HELP?

System Administrators often focus on building a network to deliver IT functions. They're often tied to strict deadlines and therefore ensuring everything is secure is sometimes not the first priority.

Additionally, many security flaws can be subtle or difficult to spot if you're not well versed in common vulnerability types and testing methods.

By using the "hackers" point-of-view throughout the training course we allow those interested in developing a security testing capability to get started on that journey.

HANDS ON - Labs

Our training course includes the following hands-on labs to ensure you gain practical understanding as well as getting to grips with our testing methodology:

› Kerberos Attacks

Leveraging common Kerberos attacks including party tricks, kerberoasting, overpassing the hash, and more.

› Interception Attacks

Abusing link-local multicast name resolution, as well as address resolution protocol spoofing for credential theft and code execution.

› Vulnerability Exploitation

Automating exploitation through common testing frameworks, as well as looking at the wider vulnerability lifecycle.

› Privilege Escalation

Escalating from a low privileged foothold account up to a highly privileged account through credential extraction and token impersonation.

FEATURES

- ★ Detail remediation guidance for every vulnerability type covered.
- ★ Multiple challenges for each lab, for beginner to intermediate skill levels.
- ★ Guidance on the Penetration Testing methodology.
- ★ Covers the full path from foothold to full compromise.

secarma®
CYBERSECURITY EXPERTS

Hacking & Defending Web Apps

The Secarma testing team regularly run hands-on security training courses across the UK and remotely. Our Hacking and Defending Web Apps sessions allow you to get practical experience breaking web applications, before teaching you how to build them in a more resilient way.

WHO IS IT FOR?

Our web application hacking course is designed to teach web application developers the tools and techniques we use when targeting web applications during real world penetration tests.

It's also a useful course for those looking to break into Penetration Testing who want a first step on the journey.

HOW CAN WE HELP?

Software developers often focus on building an application and making it functional. They're often tied to strict deadlines and therefore, ensuring everything is secure is sometimes not the first priority.

Additionally, many security flaws can be subtle or difficult to spot if you're not well versed in common vulnerability types and testing methods.

By using the "hackers" point-of-view throughout the training course we allow those interested in developing a security testing capability to get started on that journey.

HANDS ON - Labs

Our training course includes the following hands-on labs to ensure you gain practical understanding as well as getting to grips with our testing methodology:

- **Injection**
  Leveraging injection vulnerabilities to extract confidential data, in order to compromise databases and web servers directly.
- **Cross-site Scripting**
  Leveraging XSS attacks to perform virtual defacement, extract confidential information, and perform privilege escalation.
- **Abusing File**
  Upload Bypassing file restrictions to upload malicious files to gain command execution on vulnerable web servers and to pivot into DMZ and internal networks.
- **Broken Authentication**
  We cover a range of authentication and access control issues, from simple bruteforce attacks, to bypassing multi-factor authentication, and missing functional level access controls.

FEATURES

- ★ Guidance on the Penetration Testing methodology.
- ★ Covers the OWASP Top 10 and other key security issues.
- ★ Detail remediation guidance for every vulnerability type covered.
- ★ Multiple challenges for each lab, for beginner to intermediate skill levels.

secarma®
CYBERSECURITY EXPERTS

Security Awareness Training

The Secarma testing team regularly run hands-on security training courses across the UK and remotely. Our Hacking and Defending Web Apps sessions allow you to get practical experience breaking web applications, before teaching you how to build them in a more resilient way.

WHO IS IT FOR?

Our web application hacking course is designed to teach web application developers the tools and techniques we use when targeting web applications during real world penetration tests.

It's also a useful course for those looking to break into Penetration Testing who want a first step on the journey.

HOW CAN WE HELP?

Software developers often focus on building an application and making it functional. They're often tied to strict deadlines and therefore, ensuring everything is secure is sometimes not the first priority.

Additionally, many security flaws can be subtle or difficult to spot if you're not well versed in common vulnerability types and testing methods.

By using the "hackers" point-of-view throughout the training course we allow those interested in developing a security testing capability to get started on that journey.

HANDS ON - Labs

Our training course includes the following hands-on labs to ensure you gain practical understanding as well as getting to grips with our testing methodology:

- **Injection**
  Leveraging injection vulnerabilities to extract confidential data, in order to compromise databases and web servers directly.
- **Cross-site Scripting**
  Leveraging XSS attacks to perform virtual defacement, extract confidential information, and perform privilege escalation.
- **Abusing File**
  Upload Bypassing file restrictions to upload malicious files to gain command execution on vulnerable web servers and to pivot into DMZ and internal networks.
- **Broken Authentication**
  We cover a range of authentication and access control issues, from simple bruteforce attacks, to bypassing multi-factor authentication, and missing functional level access controls.

FEATURES

- ★ Guidance on the Penetration Testing methodology.
- ★ Covers the OWASP Top 10 and other key security issues.
- ★ Detail remediation guidance for every vulnerability type covered.
- ★ Multiple challenges for each lab, for beginner to intermediate skill levels.

secarma®
CYBERSECURITY EXPERTS

Consultancy

Our experts offer various consultancy services that can help you understand your organisation's security posture, test your defences, prepare for worst-case scenarios, and help you meet security objectives.

Secarma's skilled consultants work with you to build your organisation's resilience to real world attacks, and can even manage your security overall if that's what you need. With us, you can expect strong communication with your company's administrators, security team, and board members as standard. We're here to keep you in control, inform, advise, and take the weight off.

Why Invest in our Consultancy Services?

Forward-thinking organisations know that security is the foundation of business success; but what happens when you're unsure how to improve on your current security status, or just don't know where to begin? That's when you need an expert by your side, and our consultants are here to fill that role. We provide an independent view of your organisation's security, consulting with you on what's working, what isn't, and how to improve.

We give you bespoke support that's tailored to suit your organisation's unique needs.

Services

Every organisation is different, so don't expect a "one size fits all" approach from us. Our list of services are designed to meet your security needs and help you protect your organisation. Our services include:

Virtual Information Security Manager – a dedicated expert, embedded within your organisation to provide an independent view of your security posture, manage large-scale projects, and communicate their findings with senior management.

Cybersecurity Maturity Assessment – a detailed evaluation of your organisation's current security status.

Incident Response Scenario Testing – also known as Wargaming, this service is designed to test the effectiveness of your established incident response and business continuity plan.

Cloud Configuration Security Review – this service tests the configuration of your chosen cloud provider's management interfaces for security misconfigurations.

Firewall Configuration Security Review – this review provides system administrators with a comprehensive overview of your organisation's firewall configuration.

Build Configuration Security Review – the in-depth assessment of server builds, end user device builds, or system deployment tools for vulnerabilities, ensuring servers and end user devices are as secure as possible..

vISM

Virtual Information Security Manager

Developing and maintaining a robust cybersecurity posture can be challenging for organisations who either don't have the necessary skills, time internally or the budget to employ a full time, in house Security Manager.

Secarma can provide a Virtual Information Security Manager (vISM) who will be embedded within an organisation for a selected period of time to assist in meeting security objectives.

WHO IS IT FOR?

A service of this nature can benefit a range of companies, who are looking for extra support managing and performing security tasks within their organisation.

For example, small companies might simply not have the resources for a full-time security manager but require the capabilities that one brings. Additionally, organisations may want security guidance from an independent source, not tied to their current hierarchy.

HOW CAN WE HELP?

Secarma's vISM Consultancy can offer a solution to these issues, providing bespoke security support to suit a business's requirements.

Our experienced consultant will provide an organisation with an independent view of their security posture, as well as the additional benefit of acquiring a security capability on a consumption-based pricing model.

WHAT WE TEST

Whilst some organisations may require support in all areas, others may have certain aspects of security competently covered, only requiring assistance in specific areas. With this in mind, this service is broken down into 'modules' which can be utilised in any combination – or in their entirety.

- **Risk Management**
  Assisting in compliance work working towards Cyber Essentials, policy review, and building a strong security culture.
- **Security Protection**
  Assisting in the development of implementation plans for vulnerability management, penetration testing, and secure workstation builds.
- **Incident Detection**
  Assisting in the deployment of log management capabilities, as well as developing an in-house monitoring capability or threat-hunting team.
- **Minimizing Impact**
  Developing incident response plans, incident

secarma®
CYBERSECURITY EXPERTS

CSMA

Cybersecurity Maturity Assessment

Our Cyber Security Maturity Assessment (CSMA) evaluates your organisation's current security posture; looking beyond technical configuration, in relation to its ability to protect, detect and respond to security threats.

Think of it as a simplified version of the NCSC Cyber Assessment Framework, tailoring the assessment to focus on responsive solutions, organisations can implement to become more robust.

WHO IS IT FOR?

At Secarma we believe that all businesses, regardless of size should be given the opportunity to develop a thorough understanding of the risks they face and be given direction by a trusted advisor to improve their own cyber security maturity.

This assessment is for any organisation that wants to assess and improve their current security program to ensure they are prepared to deal with today's most advanced threats.

HOW CAN WE HELP?

Many organisations have the intention to improve their cyber security, but simply don't know where to start or worry they may miss an area of concern. Secarma's CSMA mission is to simplify implementations that align cyber security practices with your organisational objectives and policies.

We will perform a review on your current security posture through an initial orientation meeting, a documentation review and interview workshops. This will give your organisation a deeper understanding, not only in the areas of security strategy you are successfully, but to what degree of maturity has been achieved and how to improve it.

WHAT WE TEST

Our Cyber Security Maturity Assessment will evaluate an organisation's preparedness and grade their maturity in the following areas:

Risk Management

Security policies ranging from organisational roles, security training, assessing risks and communicating security goals.

Security Protections

Documenting and grading an organisation's technical enforcement of security policy.

Incident Detection

Monitoring the essential services for security concerns which may impact the security of the systems and the effectiveness of security measures.

Minimising Impact

An organisations ability to address incidents that are detected in terms of planning, testing, and backing up vital information.

secarma®
CYBERSECURITY EXPERTS

Wargaming

Incident Response Scenario Testingt

Modern organisations face a range of cybersecurity risks, and whilst every effort may be made to prevent a breach, if the worst does happen, your business must be prepared to respond to that breach quickly and effectively.

WHO IS IT FOR?

Our Incident Response Scenario Testing (also know as 'Wargaming') is for organisations who have established an incident response and business continuity plan, that wish to test the effectiveness of that plan in a controlled manner.

HOW CAN WE HELP?

Secarma have developed a Cybersecurity Incident Wargaming service, which is designed to explore the effectiveness of an incident response plan against realistic scenarios, through a tabletop exercise.

Wargames are usually scheduled for a three-hour session, allowing for the steps of incident response to be deeply explored, yet still allowing for breaks and open discussion in the group.

At the end of the session, the intention is that the response team will more clearly understand the strengths and weaknesses of their incident response planning.

We have found these sessions work best when each aspect of the response team is represented in the room, such as the board, the technical team, and the communications team.

WHAT WE TEST

We typically develop scenarios that are based on real-world incidents that have previously taken place. However, if your organisation wishes to test against a specific scenario, we can build a bespoke exercise.

Example scenarios include:

- **Malicious Software Outbreak**
  This scenario plays through the common stages of a major malware outbreak to test how well an organisation can identify, contain, eradicate, and recover from an attack such as mass ransomware.
- **Denial of Service Attack**
  This scenario walks through a complex denial of service attack that impacts a major, or public, system. It tests how well an organisation identifies and mitigates the attack, whilst managing the potential public relations impact of service outages
- **Website Defacement**
  This scenario walks through how an organisation responds to a very public breach such as a website defacement. It tests how well they can identify the issue that led to the defacement, restore systems to working order, harden them from further attacks, and manage the public response.

secarma®
CYBERSECURITY EXPERTS

Cloud Configuration Security Review

Secarma's Cloud Configuration Security Review tests the configuration of your chosen cloud provider's management interfaces for security misconfigurations. This is a critical requirement for any businesses that has moved, or is looking to move onto cloud infrastructure.

WHO IS IT FOR?

Many organisations these days have at least some workloads hosted within the cloud. Whether it's a simple "lift-and-shift " of moving onsite assets to the cloud, or something more 'cloud native', it's important to make sure that these systems are secure.

We offer security testing appropriate for all levels of complexity, from simple security reviews of cloud hosted virtual machines, to deep-dive assessments of cloud-native applications.

HOW CAN WE HELP?

If you're hosting an application in the cloud and are concerned about application vulnerabilities within the system, then we can perform a traditional application penetration test.

However, if your concern is with how the hosting environment itself is set up then the most efficient way to determine if a cloud setup is secure, is to review the configuration panel itself.

This is an open book approach to security testing that ensures that available security options are configured, that systems are locked down, and that accounts with access are appropriately protected.

WHAT WE TEST

The specifics of the testing depend entirely on the deployment and features in use on the target cloud platform, however some commonly assessed areas include:

- **Identity and Access Management**
  Ensuring account utilise multifactor authentication and adhere to the principle of least privilege.
- **Storage**
  Ensuring that permissions to storage such as AWS S3 Buckets and Azure Storage are locked down and that keys are protected.
- **Network and Instance Security**
  Ensuring that the cloud platform adequately filters traffic and segments services.
- **Transit Security**
  Ensuring that data in transit between systems is encrypted and the configuration is hardened.
- **Logging and Monitoring**
  Ensuring that any actions taken within the cloud platform, and that may impact the systems security, are appropriately logged and that significant issues are highlighted to administrators for review.
- **Remote Access**
  Ensuring that remote access to the cloud platform is hardened against internet-based attacks.
- **Key Management**
  Ensuring that services such as Azure Key Vault and AWS Key Management are appropriately used and hardened, and that logging is enabled.

secarma®
CYBERSECURITY EXPERTS

Firewall Configuration Security Review

Firewalls are an essential component of network security; they monitor incoming and outgoing network data, either permitting or blocking based on security rules. Upon initial installation these configurations are often locked down, but then over time as network and business requirements evolve, changes are made which reduce the protection the firewall once offered.

A Firewall Configuration Security Review will highlight these areas of weakness, enabling an organisation to reconfigure their firewall rules for better security.

WHO IS IT FOR?

Firewalls are designed to be the first line of defence against cyber attacks, making them a fundamental security system that all organisations should be using and reviewing on a regular basis.

Firewall Security Reviews are also required for standards such as Payment Card Industry Data Security Standard (PCI-DSS), the General Data Protection Regulation (GDPR), and ISO 27001. Therefore, any organisations needing to comply to these standards should consider this review.

HOW CAN WE HELP?

It is essential that the configuration and ruleset of your firewall, meets the business and compliance requirements of your organisation. However, its common for firewall settings to be changed and forgotten about over time, or misconfigured leaving your networks open to attackers.

Our Firewall Configuration Security Reviews can provide system administrators with a comprehensive overview of the configuration of your firewall or similar security device, highlighting areas of weakness.
This will allow your organisation to understand and remediate any firewall security issues, to ensure that it's as locked down as possible.

WHAT WE REVIEW

Our consultants will review your firewall configuration and rulesets, identifying, verifying and prioritising weaknesses based around:

- **Known Vulnerabilities**
  Missing security updates is a common weakness that can lead to devices being compromised.

- **Authentication**
  Authentication systems often have weaknesses such as username enumeration, lack of brute force protection, or even just common and weak passwords.

- **Access Control Systems**
  Where access is granted to hosts, services, or ports, our consultants will review the access to determine if it introduced unexpected weaknesses in the protection or if the allowed access is overly permissive.

Please turn over for a more in-depth look at how we review your firewall settings.

secarma®
CYBERSECURITY EXPERTS

Build Configuration Security Review

A Build Configuration Security Review is designed to provide system administrators with a comprehensive overview of the security of their assets, whereby the local policies and settings of a device are examined to assess their security implications.

WHO IS IT FOR?

Build configuration reviews can assess server builds, end user device builds, or standardised images used for deploying systems (commonly known as "gold images") for security issues and to review their level of security hardening.

Therefore, most organisations would benefit from a Build Configuration Security Review to ensure their servers and end user devices are as secure as they should be.

HOW CAN WE HELP?

This form of assessment is not intended to be representative of a real-world threat, but instead a transparent approach to allow you to gain an understanding of the security-related configurations, and how this may hinder defence-in-depth.

We review the security configuration of devices and give guidance on how systems can be reconfigured to make them more resilient to attacks, including remote attacks, local network attacks, and insider threats.

WHAT WE TEST

We assess all aspects of the device configuration; some commonly assessed areas include:

- **Local Configuration** - The local configuration considers hardening options available on the operating system and device. Such as registry keys, file-system permissions, and BIOS settings.
- **Domain Configuration** - The domain configuration includes any policies or configurations applied as a result of being a domain-joined asset, such as group policy and account lockout options.
- **Network Configuration** - The network configuration includes any policies or configurations which impact the security of the asset from the local-area network such as host firewall configuration and protocols such as NetBIOS.
- **Software Configuration** - The software configuration includes any software installed on the host which may impact the security of the asset such as outdated browsers, office packages, and protections such as Anti-virus.

secarma®
CYBERSECURITY EXPERTS

Contact Us

☎ 0161 513 0960

@ enquiries@secarma.com

secarma®
CYBERSECURITY EXPERTS