SAPPHIRE™

Breach Attack Simulation

Service Definition

Classification: Internal use Only

Document Information

Document title:	Breach Attack Simulation Service Definition
Date	
Client Reference	
Sales Contact	
Technical contact	

Proprietary Notice

Service Definition
Breach Attack Simulation

Overview

Breach Attack Simulation (BAS) testing compliments penetration testing and red and purple teaming exercises, by validating your organisations security posture through specific simulated advanced attacks that are known to be carried out by significant threat actors. In simple terms, simulating the attack paths and techniques that are likely to be used by malicious actors.

Services features:

- Understand your security vulnerabilities by automating testing of threat vectors.
- Attempt lateral movement and data exfiltration.
- Scale up your cyber defences by running scenarios and emulations.
- Strengthen defences by emulating real attacks and tuning SIEMs.
- Full Purple team testing, allowing real time testing.
- Customised methods know as Tactics, Techniques and Procedures (TTPs).
- Advance Persistent Threat (APT) approach and analysis.
- The attack simulation will follow the MITRE ATT&CK Framework.
- Ransomware is common attack method request for data exfiltration.
- Attempts to deliver custom payloads and scripts.

Service benefits:

- Allows organisations to assess the effectiveness of their cybersecurity defences.
- These simulations help fine-tune their incident response plans.
- Completing and understanding breaches allows prioritisation of security investments effectively.
- Prioritise remediation efforts based on the risk level.

Functional and non-functional Detail

The service is a scenario based external and internal simulated test over a period of 5 days. The aim is to take out the reconnaissance part of this assessment and we will be provided with a starting point by our GCloud customer. This can be an external IP, endpoint machine or connected to the internal network via Sapphire Connect.

The exercise will test Highland Spring's perimeter security controls and technology that is in place as we would expect to be blocked at some stage. Testing will be based on a grey-box scenario with the test aim to search for defects due to improper structure or use of insecure applications or services. The attack simulation will follow the MITRE ATT&CK Framework.

Sapphire will attempt a basic foothold in the network to see how easily we could use common tools, tactics and processes to leverage and use lateral movement, privilege escalation and ultimately delivering a payload (C2 script). This will allow you to identify what additional controls they need to consider to mitigate the risks from this.

The aim is data exfiltration as this is a common element reported from ransomware incidents. The scenario will be split, attempt based on an attacker on the network with no credentials and see if data can be exfiltrated. Then with credentials (found or provided) to see if it is possible to traverse

the network. We would expect that a standard user should have to go through the proxy server and should face firewall egress filtering but are there any obvious gaps here to consider.

Information Assurance

There are no external regulators within the industry sector that Sapphire 'as a company' has to provide assurance to. Sapphire complies with all legal and statutory requirements as well as client requirements. Individuals are members of professional CHECK schemes. A compliance Matrix which is ISO27001 certified details these areas and can be made available during an onsite audit.

As a 100% Cyber Security company, our credibility is built not only on our long-standing reputation amongst our clients for successful testing and auditing services but is also demonstrated by our certifications. Sapphire was one of the first organisations in the UK to achieve certification to ISO 27001, the international information security standard. The organisation is also a member of the NCSC CHECK scheme; developed to enhance the availability and quality of IT health check services provided to government in line with HMG policy.

All our testers are SC cleared, as part of their CHECK Team Member and CHECK Team Leader status, sponsored by GHCQ.

For standard testing, we deem that we will hold and process information IL2 and below. For IL3 and higher, Sapphire would recommend using our IT Heath Check service outlined separately within Sapphire's Cloud submission.

Level of Backup/Restore and Disaster Recovery

Sapphire has a Business Continuity and Disaster Recovery plan in place to enable the company to quickly regain its previous performance and standing after any threat to business continuity, showing as little interruption Sapphires employees and our Customers.

Daily tape backups are taken and stored securely off-site on a weekly basis.
Information security is critical to Sapphire, and that of its customers. It is the goal of Sapphire to ensure that:

- Information is protected and controlled against unauthorised access or misuse.
- Confidentiality of information is assured.
- Integrity of information is maintained.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Information security training will be provided to all personnel.
- Security statements will be issued and signed by all personnel.
- Assets are classified and protected as required.
- Physical, logical, environmental and communications security is maintained.
- Operational procedures and responsibilities are maintained.
- All identified information security incidents (breaches, threats, weaknesses or malfunctions) are reported to the CEO, and investigated through the appropriate management channel.

- Infringement of this Policy may result in immediate disciplinary action or criminal prosecution.
- Business requirements for the availability of information and information systems will be met.

On-boarding and Off-boarding Processes

For all consultancy services, Sapphire will provide a project cost which will include scoping, phased delivery, reporting and associated deliverables and presentations to senior management. The project cost will be identified following the scoping call/meeting.

Service Pricing

A typical BAS will be completed over a minimum of 5 days at £1,100.00 per day, subject to scope.

Service Management

Sapphire's uses project management techniques as a methodical approach to planning and guiding a project from start to finish. Using best practice methods, we adopt key processes which direct our customers through five stages: presales, scoping, executing, controlling, and after care support. Project management is applied to all Sapphire's service range and is widely used to control the complex processes of IT security project and solutions.

Customer and account management is achieved using Salesforce. This system manages customer information, opportunities and administration (quotes, purchase orders and invoices).

Service Constraints

None, as the service will be defined during the project scope.

Service Levels

Sapphire is the first line support for all our customers and all calls should be raised through our Helpdesk. Support will be provided between 08:30 and 17:00, Monday to Friday. Calls should be directed to the Sapphire Helpdesk by telephone, fax or e-mail.

Tel: 0845 58 27999
Email: support@sapphire.net

The requester must provide at least the following information.

Company and position
Contact telephone number
E-mail address
Brief description of fault

Other support numbers:

Lisa Ingham 07976 057156
lisa.ingham@sapphire.net
(Business Services Manager, Sapphire)

Alan Moffat 07535 666210

alan.moffat@sapphire.net
(Business Services Director, Sapphire)

Response to Helpdesk calls will be within 4 hours. From the initial call the requester will automatically be informed by e-mail of the log number for future reference. The response to the call will be from an Engineer via, telephone, fax or e-mail.

On completion of a call an automatic e-mail completion will be sent to the requester together with an incident report.

The Customer is entitled to escalate faults at any time, for example if there is a need to highlight the critical nature or impact of a service outage. The following escalation path should be used:

Level	Contact	Description
Level 1	Sapphire Helpdesk	The first point of escalation should always be the Sapphire Helpdesk and escalation must be separate from the initial call to log the fault. The client must obtain a case reference number for the fault.
Level 2	Sapphire Professional Service Manager	This is the second point of escalation in the event of the Helpdesk being uncontactable or an increase in call priority being required. The client should quote the case reference number provided.
Level 3	Sapphire Sales Director	This is the third point of escalation in the event of the Manager being uncontactable or a further increase in call priority being required.

Financial Recompense Model

Sapphire does not offer any additional recompense beyond what is covered by our Professional Indemnity Insurance.

Training

Sapphire can provide general information security awareness training, and internal auditor specific training, drawing on experience of a wide-ranging security practice across technical and systems disciplines. Our training program includes:

- Digital Forensic Readiness Training
- Insider Threat Management Course
- Tailored Cyber Security Training courses
- BCP Desktop Exercises
- Technical Solutions Training
- ISO27001 Awareness Training
- Security Related Training / Skills and Knowledge Transfer
- The National Information Security Conference (NISC)

Ordering and Invoicing Process

Following receipt of a purchase order, a credit account application will need to be completed for all new customers to Sapphire. Once approved, a job will be created, and a project team will be assigned to the GCloud customer. On completion of the project and reports have been submitted and signed off by the customer an invoice will be initiated. All invoices are to be paid within a 14-30 day agreed notice period.

Termination and Cancellation Terms

The Professional Services Agreement (PSA) Terms and Conditions may be terminated by either party on giving at least 30 days' notice to the other. If we give notice, you shall be liable to pay all charges up to the expiry of the notice. If you give notice, you shall be liable to pay all charges until 30 days after the date we receive the notice or until expiry of the notice, whichever is the latter. Your service of notice does not avoid any other liability for Service already provided. You shall be entitled to any data or work in progress created in relation to the Service up to the date of termination unless notice is served as a result of a breach of this Agreement by you in which case all rights to such data or work in progress remain with us.

Sapphire reserve the right to invoice in full any job cancelled or deferred within 9 working days of the scheduled delivery/start date*. Jobs cancelled/deferred between 10 and 21 working days of the scheduled delivery/start date will be subject to an invoice of 50% of the total job value**.

Please note: Any time used/spent on will be invoiced (plus associated expenses including travel and accommodation). This time will be deducted from the overall time allocated to the project and may necessitate a further purchase order being raised to cover the projected shortfall in allocated days.

*The invoice for cancelled/deferred jobs within 9 working days of the start date will be equal to the whole value of the purchase order or alternatively 5 days consultancy – whichever is the smaller.

**The invoice for cancelled/deferred jobs within 10 – 21 working days of the start date will be equal to the 50% of the value of the purchase order or alternatively 5 days consultancy – whichever is the smaller.

Data Restoration / Service Migration

Data is backed-up, in order to ensure that, if required, a valid back-up of previous data is available, for purposes of restoration, or in case data becomes corrupt or lost. Sapphire conducts a tape backup restore test and UPS test process on a twice annual basis.

Consumer Responsibilities

Information gathered during the scoping stage will be used in the preparation of a test plan, schedule and scoping agreement. The scoping meeting can be a conference call or formal meeting. Based on the scoping detail, a document will be generated and will require signing prior to the commencement of any testing. Failure to receive this may result in a delay to the start of testing.

In addition, a signed Vulnerability Test Agreement is mandatory. This provides Sapphire the Authorisation from the Cloud Customer that testing can be carried out against the agreed systems.

Typically we will need to know how many IP addresses we are required to test, number of devices, systems or servers.

For any remote internal testing, the customer will need to setup Sapphire Connect. Sapphire have developed a secure VM specifically for internal testing. The Sapphire Off-Site Internal testing (OSIT) system is a dedicated, custom-built remote access system designed solely to facilitate effective and secure security testing of networks without requiring a physical presence on your site. It positions us in the same way as if we were on-site with the GCloud customer.

The system comprises of a virtual machine (OSIT-VM) that is installed within the network environment to be tested. This connects to the Sapphire OSIT gateway system and is then available for use by an authorised Sapphire tester. The OSIT-VM is analogous to the laptop carried by the tester in a traditional engagement and provides the same facilities and capabilities for testing the network.

The system has many advantages over other remote testing methods. The use of a VM based system in preference to connecting a tester's system to a VPN connection allows for faster testing as all scanning traffic is contained within the local network and does not have to traverse relatively slow Internet links. Also tests can be performed to find issues at the lower layers of a network that cannot be visible across a VPN, such as unintentional data broadcasts or name resolution weaknesses. It is usually possible to deploy and configure the system when system administrators are working remotely.

Getting up and running is straight-forward. Sapphire will provide OSIT-VM images for the major virtualisation systems (see below) and then only require a configuration file from Sapphire and a simple firewall rule allowing the OSIT-VM to connect out to the Sapphire OSIT gateway system. There is no need to expose the system or any other part of the customer's network to direct access from the Internet.

Authorised testers securely connect to the Sapphire infrastructure and from there can connect to your OSIT-VM where they are again authenticated using individual public/private authentication key-pairs. Control of who can authenticate to the OSIT-VM is in the hands of the customer. All usage of the OSIT network, infrastructure and access to OSIT-VMs are monitored via the Sapphire SIEM.

To get the OSIT-VM there are four versions to choose from:
https://connect.sapphire.net/vmware-image (VMWare and Virtualbox)
https://connect.sapphire.net/hyperv-image (Hyper-V)
Azure Marketplace. Search for "Sapphire Connect" (Azure)
Community AMI search for "sapphire connect" (AWS)

Customer setup documentation will be provided separately.

Technical requirements

When carrying out any penetration testing or vulnerability assessment assignments, Sapphire testers will adhere to guidelines, codes of ethics and principles published by:

OWASP:	The Open Web Application Security Project.
CREST:	Council of Registered Ethical Security Testers.
CHECK:	NCSC IT Health Check.
The Cyber Scheme:	Leading NCSC accredited assessment body.

For flexibility it is often appropriate to combine elements of all three of the above. Specific testers might be assigned dependent upon test criteria.

Sapphire testers will always work within current legislation; the Computer Misuse Act and its various amendments, Data Protection and other relevant laws and acts will be observed during any testing and/or data handling procedures.

Sapphire's typical approach/methodology to penetration testing/vulnerability assessments involves two discrete steps or phases:

A summary of a typical methodology and approach is detailed below:

Phase 1 - Targeting or Network Mapping – where the objective is to determine what an internet located attacker can see of the [company name] network and systems.

This is generally an information gathering phase and will give Sapphire testers an overview of how the targeted devices are interfacing with the internet or other external networks.

Employing recognised security testing techniques, Sapphire testers will gather information about the network in order to characterise and map the network's boundaries.

Using a combination of public domain and proprietary network mapping tools, network sweepers, and port scanning tools, Sapphire testers will identify any probable points of entry into the targeted network.

An example of the steps that Sapphire testers might execute would be:

- Tracing IP packets between network segments in order to determine the network topology. Typically, tools such as traceroute, ping, nmap and tcptraceroute are used in this step, and these tools are coordinated by [company] proprietary mapping scripts.
- Querying Domain Name Services (DNS) to determine if a zone transfer can be executed and internal DNS information obtained. Tools such as dig, the bind tools and proprietary scripts are used for this step.
- Using port scanning software such as nmap to identify any open ports or services (e.g. mail, telnet, high number ports) on devices or servers reachable via the Internet.
- Connecting to open ports using TCP or UDP network utilities to determine the type(s) of operating system(s), firewall application(s) and network service versions in use. This is typically accomplished using tools such as bannergrab-ng, nmap, amap, netcat and proprietary scripts.

Phase 2 - Vulnerability Mapping and Exploitation - the objective is to identify any weaknesses in the security of the system typically using information compiled during Phase 1- Targeting, the overall objective of this phase being to map the profile of each system to be tested against publicly known,

or in some cases unknown, vulnerabilities relevant to the systems under test. Common scenarios that could provide exploitable features may include:

- E-mail (e.g. spoofing, relaying and virus)
- Unrestricted data flows.
- Operating system and software - bugs and configuration errors.
- Mis-configuration or deployment of firewalls or other network devices
- Evaluate attack vulnerabilities of hosts on the network.

Sapphire testers will map the vulnerabilities listed in public sources of vulnerability information, such as CVE, Bugtraq, OSVDB and CERT, to the profiles identified in the network mapping or targeting phase which will also incorporate current underground exploits and vulnerabilities.
Expected results for the Vulnerability Mapping Phase will list the type of system, application or service by vulnerability. The vulnerabilities mapped to each system under test will include relevant tests to be applied.

At all times, the Sapphire testers will take care to avoid infrastructure that is out of scope, and will not exploit vulnerabilities that may have adverse effects on live services without prior consultation with the designated technical contact.

Tools
Sapphire testers employ a wide and varied toolset, which has been built up over many years and numerous testing scenarios.

A number of the tools used by Sapphire testers may fall within the boundaries of the Computer Misuse Act Sections 1-3 as amended by the Police and Justice Act 2006. Whereby they can be employed to gain access to, hinder or impair computer systems. For this reason authorisation will always be obtained before a test can begin, and a full scoping document must be received and signed by both parties.

A selection of other tools regularly used in our testing process includes:

Nikto	Kismet	Nessus
Metsploit	OWASP-Zap	Nmap
Burpsuite	Perl Webscarab	Ettercap
Tcpdump	Firefox	Cain
Wireshark	Sqlmap	Qualys

Finally, we would highlight at this point that, as every security assignment is unique the most valuable tool is the experience of the tester and their ability to assess the systems that they explore and their knowledge of the best tools to investigate potential exploits in each individual situation.

Trial Service

Not applicable for this service.