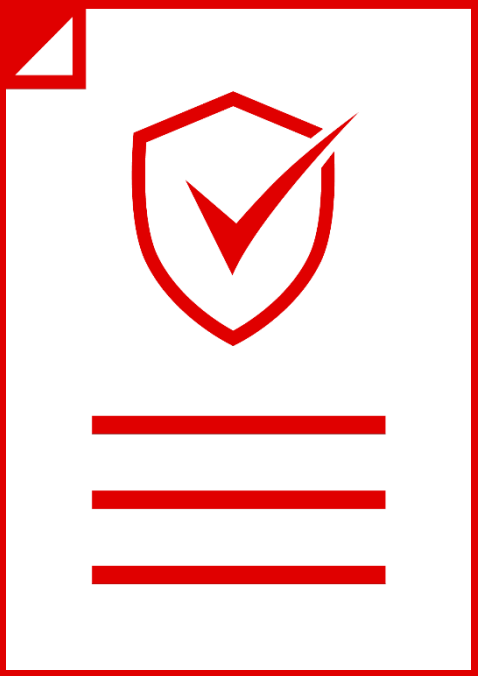

Claranet Cyber Security Service Description

Purple Team Assessment

v.1

claranet cyber security®

Contents

Service Overview 4

Scope 5

Initial discussions 5

Scope Questionnaire & Initial Call 5

Statement of Work (SoW) 6

Recommendation 6

Authorisation to Test 6

Requirements and Assumptions 6

Prepare for testing 8

Scheduling 8

Communication 9

Agreement and confirmation 10

Delivery 11

Commencement of delivery 11

Methodology 12

Handling of sensitive data 12

Review 13

Reporting 13

Quality Assurance 13

Timescales 14

Appendix 15

Service terminology 15

Fees, payment and legal 16

Live systems 17

Reclassification of the scope 17

Legal obligations 18

Service Overview

Purple Team is a type of security testing and takes its title from the combination of red and blue. Red Team refers to ethical hackers delivering attack simulations to establish the risks of likely attack methods. A Blue Team is the organisation's defensive team whose objective is to detect and protect against attacks.

A Purple Team Assessment brings both teams together in a joint exercise which simulates and analyses active attack scenarios based on pre-defined goals. Purple Team Assessments can be applied to the whole organisation, internal assets, the perimeter, and cloud environments.

From a hacker's perspective, each area represents an opportunity to attack - opportunities that can be minimized by reviewing your security in the same way you would your buildings or physical assets.

Like Penetration Testing, Purple Team is a manual service, delivered as standard remotely between Monday and Friday. This document will take you through the the stages of the process including responsibilities and obligations for you, our client and Claranet.

Anything not included in this Service Description will not be provided by Claranet as part of the Penetration Testing unless otherwise agreed by the parties in any Statement of Work (SoW) and/or Order Form together with any additional charges that may be applicable.

This document describes the service Claranet Cyber Security provides and details your responsibilities in relation to this service. The Service Description forms part of an agreement between the parties and is subject to the standard terms of business between Claranet and your organisation or as agreed by the parties and the parties agree to be bound by such terms.

Scope

The initial Scope phase ensures that the Claranet Cyber Security technical team works closely with you to create a service suited to your specific requirements. This initial phase is to assist in defining an appropriate scope for the exercise. The intention to test may be driven by compliance requirements, alignment to best practice, visibility of risk, or a combination of all. Understanding this will help Claranet's scoping team to design the right engagement for you.

Initial discussions

In order to determine the appropriate approach for the Purple Team Assessment, we will need information from you about the objectives of the engagement and the extent of the collaboration and knowledge transfer between Red and Blue Teams required. This information should be provided by completing the Scope Questionnaire for provided to you by Claranet.

Initial discussions will also be supported by a conference call. During this stage, we will discuss the challenges and requirements you have and how the Purple Team Assessment can be designed to best assist in meeting these.

Scope Questionnaire & Initial Call

A Scope Questionnaire will need to be completed by you prior to Claranet providing a quote for the work. It will be followed by a more detailed conversation regarding the objectives and expectations of the engagement. These will allow for a defined Statement of Work (SoW) to be produced along with a prescription of the number of days the engagement will take to complete and a price for those days. Purple Team Assessments are defined by the amount of interaction between Red and Blue Teams and the extent of the knowledge transfer required.

The Scope stage will:

- Identify the drivers and goals for the assessment
- Specify the locations from where the testing will take place if not standard remote testing
- Suggest the ideal timescales for your testing
- Define the times of day where testing is permitted or not permitted
- Establish the depth of testing required
- Clarify the level of collaboration and knowledge transfer required

Statement of Work (SoW)

Once the Scope Questionnaire and initial call have been completed, the Claranet Purple Team Solutions Architect will examine the information provided and apply a rigorous and consistent approach to ensure that sufficient time is allocated to the engagement to meet the objectives; the result of this exercise is the SoW. The notes added to the SoW are based around how Claranet Cyber Security will complete the assessment. e.g. 1 day to test the target with observation from members of the Blue Team, 1 day to review which attacks were detected, 1 day for a guided tabletop discussion regarding variations of this attack and how to better detect and respond.

Recommendation

Claranet Cyber Security will make recommendations regarding the structure of your assessment and return an SoW to you. Engagements will be defined by the type and complexity of the target(s), the extent of Red Team/Blue Team collaboration and knowledge transfer, their location, the time of delivery for the assessment i.e. in-hours or out-of-hours, and the duration of the engagement defined by how many days testers will need to complete the assessment based on the scope information discussed.

A quote will be provided within the SoW document defining the costs of the exercise.

Authorisation to Test

The SoW also includes a section to be signed by you, confirming that you are providing Claranet with your authorisation to conduct Penetration Testing type activities against the specified targets.

Purple Team Assessments cannot commence until a signed SoW is received by Claranet Cyber Security.

By authorising Claranet Cyber Security to undertake the testing activities agreed, you are confirming that you have obtained, or will obtain where necessary, the consent of all appropriate parties for testing to be carried out. Claranet Cyber Security will deliver the Penetration Testing activities in the belief that it has all of the appropriate consents, permits and permissions from you and your companies, as well as employees and sub-contractors where required.

Requirements and Assumptions

This section of the SoW lists the requirements needed by the testing team before the Purple Team Assessment can start.

Responsibility	Claranet	You
Scope Questionnaire: Provide any information required by Claranet relevant to the assessment and in support of a full and exhaustive exercise. This information will form the basis of the final engagement, so it is your responsibility to ensure that the information and access provided is accurate, comprehensive and sufficient.		✓
Statement of Work: Provide an SoW detailing the structure, price and delivery duration for the engagement and in accordance with the details outlined in the Scope Questionnaire and initial scoping call.	✓	
Authorisation to test: Return the SoW to Claranet with the Authorisation to Test section signed.		✓
Drivers: Detail any compliance or industry regulators involved in the assessment. These may have a material effect on the composition of the tests, the consultants that are used, and the style of reporting.		✓
Recommendations: Make recommendations regarding the depth, coverage and type of tests in-line with the desired outcome.	✓	
Managing risk: Identify areas of weakness and or concern that present a risk of system failure and the exposure of sensitive data and then suggest appropriate tests to cover these areas.	✓	
Exclusions: Consider any systems that are to be excluded from the assessment, detailing them in the Scope Questionnaire which forms the basis of the SoW.		✓

Prepare for testing

Scheduling

Purple Team Assessments can be scheduled upon receipt by Claranet Cyber Security of a Purchase Order. Claranet can provide an indication of the potential availability of suitable Penetration Testers at any stage. We will work with you to get the engagement underway as quickly as possible, however, resource availability changes rapidly and the allocation of testers will only be confirmed once a Purchase Order has been received.

Responsibility	Claranet	You
Identify a timescale: Provide potential timeframes for delivery of the work. As the availability of resources changes rapidly, these timeframes are indicative only and cannot be confirmed until a Purchase Order has been received.	✓	
Scheduling dates: Agree the assessment dates and ensure that the targets will be available and accessible at the time of testing.		✓
Access: Provide access details, credentials and supporting information as requested at the point in time needed.		✓
Inform stakeholders: As part of the **Prepare for testing** phase, you will ensure that any stakeholders, including internal and third party, who may be affected by, or want to be aware of, penetration testing activity, are informed.		✓
Permission to proceed: Any third parties who host or are connected to your systems, services, or applications, may require notification of Penetration Test activity. You agree to obtain any necessary permissions or consents in advance of the Purple Team Assessment's commencement. This is particularly relevant for cloud hosting environments.		✓
Reserve and allocate Penetration Testers: Once the Purchase Order has been received, the dates for your Purple Team Assessment can be confirmed.	✓	

Cancellation and delays

Claranet Cyber Security will allocate the appropriate number of Penetration Testers to your engagement. In the event of a delay or cancellation before or during the test, the appropriate fee will be payable. Details of fees for delaying or canceling a Penetration Test will be agreed between you and Claranet prior to the order.

Where a target is not ready for testing or access is not provided prior to the commencement of the engagement, Claranet Cyber Security may decide, for the benefit of all parties, to delay and reschedule the engagement. Where this is the case, an appropriate rescheduling fee will be applied.

Communication

Clear lines of communication are critical to an efficient Purple Team Assessment, covering the transfer of information, how this is achieved, the frequency and the personnel involved. Describing the key personnel on both sides, ensures that the Blue Team can be kept informed according to the plan and that any collaboration and discussion exercises can be arranged quickly and efficiently.

Responsibility	Claranet	You
Contact information: Provide contact details of the Penetration Testers involved in the service.	✓	
Contact information: Provide contact details of those within your company taking part in the Purple Team Assessment. You will also ensure that these contact details are kept up to date.		✓
Encryption of communications: All sensitive communication between Claranet and you, such as reporting results, will be encrypted. Channels available include: PGP, Egress Switch, Encrypted File with out-of-band password sharing.	✓	
Scheduling: Inform Claranet Cyber Security of any changes to the dates, contact details or targets as early as possible. Changes to dates and targets may result in additional costs.		✓
Scheduling: Inform you in a timely manner of any changes to dates or to the Penetration Testers involved in the delivery of the testing activity.	✓	

Agreement and confirmation

At the conclusion of this phase, the design of the Purple Team Assessment, the duration and dates of the engagement, and pricing have all been confirmed and agreed.

Delivery

Commencement of delivery

The Purple Team Assessment will begin on the dates agreed. This will be delivered according to the plan confirmed by us in the SoW.

Responsibility	Claranet	You
Remote Infrastructure Testing: Claranet Cyber Security testers will discuss and agree arrangements for testing the network infrastructure remotely.	✓	
Maintain access: Ensure that access to the agreed target(s) is maintained throughout the testing window. Should access fail, you will act promptly to restore the required level of access to ensure that testing activities can be completed during the dates booked.		✓
Previews and reviews: Depending on the agreed plan for the engagement, Penetration Testers may provide the Blue Team with a preview and discussion of each attack scenario to be deployed, as well as a review following completion of the attack simulation delivery.	✓	
Collaboration and knowledge transfer: Depending on the agreed plan for the engagement, Penetration Testers may organise for Blue Team members to observe or participate in the delivery of testing activities.	✓	

Location for testing

Claranet Cyber Security's Penetration Tester will complete the test from a location agreed during the **Scope** and **Prepare for testing** stages and as outlined in the Statement of Work. Web application and network infrastructure testing are carried out from our offices or from a secure location unless otherwise agreed. If an onsite delivery is required, this should be made clear during the scoping stage as this will affect the personnel involved, the scheduling and the price.

Methodology

An overview of Claranet's Purple Team methodology is available upon request. Purple Team Assessments are tailored to each of our customers and the bespoke plan for your Purple Team engagement can be found in the SoW provided to you by Claranet at the conclusion of the Scope stage.

Responsibility	Claranet	You
The finding of all vulnerabilities: Act in accordance with, and bounded by, the Statement of Work and the number of days purchased. Consequently, it cannot be guaranteed that all vulnerabilities will be found or exploited to the full. Claranet Cyber Security will use our best endeavours to locate and exploit vulnerabilities within the scope but is not responsible for any attacks through vulnerabilities that have not been identified.	✓	

Handling of sensitive data

Part of the objective of a Purple Team Assessment is to assess the risk to sensitive information or to compromise high-value digital assets. Contact with potentially sensitive information is common and therefore will be managed accordingly. Where possible, Penetration Testers avoid coming into the possession of Personally Identifiable Information (PII).

Validating the presence of a vulnerability ensures accuracy in the reported results. Proving that a vulnerability exists within the systems containing sensitive data is achieved in a number of ways, for example; obtaining screenshots of database schemas and file permissions, or displaying files without displaying the contents.

Further to these measures, encryption on Penetration Tester machines protects any data or information we do come into contact with, and regular scrubbing of devices ensures that data is not retained.

Responsibility	Claranet	You
Sensitive data: Act in accordance with the Claranet Cyber Security policy for handling of your sensitive data and general best business practice. Penetration Testers will, where possible, avoid coming into the possession of Personally Identifiable Information.	✓	

Review

Reporting

Once testing activities are complete, a report is produced which includes:

- Executive summary
- Attack narrative depicting how we went about the test and the associated findings along with lessons learned.
- Clear recommendations for the internal security team to learn from the attack approaches and incorporate them in their defenses
- Technical analysis
- Attack execution log report with timestamps
- Gap analysis of techniques that were:
  - Detected
  - Blocked
  - Not detected
- Time taken to detect and investigate each alert

Quality Assurance

At the completion of the report, it is passed through a Quality Assurance process within Claranet Cyber Security where it is reviewed by senior colleagues. Any amendments or changes that are suggested are then fed back to the Penetration Tester(s) involved in the delivery of the assessment so that these can be applied.

It is then sent directly to your nominated contact(s) by the pre-agreed and appropriately secure method.

Full final reports are completed within 10 working days, though larger projects that require multiple reports or those with large volumes of results to report may take longer. Where this is the case, if it can be identified and communicated during the **scope phase** then interim results and draft reports can be provided to ensure that remediation activity is not delayed. Where results are required by a specific date, this needs to be agreed during the **scope phase**.

Timescales

The length of time spent producing the report is determined at the **Scoping** and **Prepare for testing** stage and will usually be booked as close to the completion of the Purple Team Assessment as possible.

Where a final report is needed by a specific date, you must inform Claranet Cyber Security as early as possible so this can be accommodated. We will make all reasonable endeavours to accommodate the request and will discuss these with you at the **Scoping** and **Prepare for testing** stage. This is to ensure that adequate resource can be assigned to the production of your reports at the specified time.

Responsibility	Claranet	You
Accuracy of reporting: Apply a rigorous Quality Assurance process to ensure that the results reported are as precise a reflection of the risk as possible.	✓	
Delivery of reports: Deliver a report as soon as possible following the completion of the engagement.	✓	
Following up reports: Make available testers for remediation discussions. This can be discussed during the Scope and Prepare for testing stage or can be organised through your Claranet contact.	✓	
Receiving reports: Provide contact details (email and mobile phone number) for the individual who is to receive the report. This must be provided at the outset of the engagement and should be included in the information you provide in the Scope Questionnaire.		✓
Following up reports: Decide what type of assistance (if any) will be required to understand and apply the most effective remediation based on the findings of the Purple Team Assessment.		✓

Appendix

Service terminology

Throughout the document or in association with it, a number of terms have been used. These can be found in the general description below.

- **Manual Penetration Testing**; a generic term for assessments using manual techniques to simulate an attack on your systems.
- **Penetration Test or Testing;** typically an assessment of IT infrastructure, networks and business applications to identify attack vectors, vulnerabilities and control weaknesses. When executed properly, a Penetration Test will describe weaknesses in your technical security and provide the information and support that you need to remove or reduce the risk that the vulnerability causes. Claranet Cyber Security provides a range of options for Penetration Testing, covering your applications to your underlying infrastructure. Undertaking a series of Penetration Tests will help you assess your organisation's risk in the face of an attack and help to identify improvements.
- **Report;** a document produced at the end of an engagement that contains details of the vulnerabilities found ranked in order of risk, how they might be exploited and suggested remediation alongside a review of which attack vectors the Blue Team were able to detect and respond to and recommendation for actions to improve detection and response capability.
- **Web Application Penetration Testing**; an authenticated or non-authenticated manual test against Internet-facing applications or application-based business systems.
- **Infrastructure Penetration Testing**; examines servers, firewalls and other network components for security vulnerabilities that could be exploited.
- **Social Engineering**; attempting to gain information or access by deceiving employees in the same way that an attacker would.
- **Red Team Exercises**; usually an attempt to achieve agreed objectives by any legal means possible using a combination of the above attack simulations and where the target organisation actively defends.
- **Purple Team Assessment**; involves the deployment of simulated attack scenarios employing typical methods of likely threat actors. Red and Blue teams collaborate during testing with tabletop reviews of the success of each attack scenario to identify ways to improve the organisation's detect and response capability.

Fees, payment and legal

Fees payable under this Contract will be invoiced on delivery of the Report.

Delays and cancellations

Immediately following the agreement of dates for the Purple Team Assessment to begin and the receipt of the Purchase Order, Claranet Cyber Security will start to allocate resources and facilities and will therefore commit to any third-party expenditure to fulfil its contractual commitments. Claranet Cyber Security may at its absolute discretion allow the engagement to be re-scheduled or cancelled. If this occurs, you agree that you are committed to paying Claranet Cyber Security a proportion of the fees as pre-estimated liquidated damages. In the case of late notice rescheduling, this fee will be in addition to the full price for the engagement which will be invoiced upon delivery of the Report. This will reflect the losses which Claranet Cyber Security will incur because of the cancellation or re-scheduling.

These proportions are as follows:

Cancellation timescale	Cancellation fee (% of engagement price)
Cancellation request received within 7 working days of start date.	90% payable

Reschedule timescale	Reschedule fee (% of engagement price)
Re-schedule request received within 7 working days of the start date with a firm re-booking date.	50% payable

Unavoidable absence

Should a tester allocated to your Purple Team Assessment become unavailable at short notice for reasons that are commercially unavoidable (for example; sickness) then every attempt will be made to provide a replacement at the earliest possible opportunity. In these circumstances, whilst some delay is usually inevitable, Claranet Cyber Security will endeavour to minimise the impact on the delivery of the results.

Live systems

Conducting the assessment may involve the testing of live systems on your current infrastructure. This may therefore have an impact on current workloads and environments and these will be discussed with you prior to commencement and minimised wherever possible. To this end, you will appoint at least one employee who shall act as liaison between yourselves and Claranet Cyber Security. They must have substantial experience of your computer systems, networking and project management of your information systems.

Responsibility	Claranet	You
Operational involvement: No intentional interference will be caused to the operation of your information system, unless it is with your express authority.	✓	
Boundary violations: Inform you of any violations of any test boundaries that occur. In the event of any boundary violation, Claranet Cyber Security will cease testing, document the extent of the violation and inform you as soon as is practicable.	✓	
Liaison: Provide an employee as liaison with Claranet Cyber Security that is technically familiar with your systems as described.		✓

Reclassification of the scope

Changes to the scope for Purple Team Assessments may require the system to be re-scoped. Changes to the scope may incur an additional cost.

Legal obligations

By offering a Purchase Order for the services quoted:

1. You have procured, and acknowledge Claranet Cyber Security is relying upon your obtaining, of any necessary consents as required of your (and your group companies') employees, agents and sub-contractors for the Penetration Testing to take place;
2. You hereby give permission to Claranet Cyber Security to access the various IT systems which may be affected by the Services delivered pursuant to the Statement of Work;
3. You have informed and gained consent where appropriate of any interested parties, individuals, users, third party information stakeholders, third party information service providers or any other parties likely to be affected by the Penetration Testing carried out by Claranet Cyber Security of the planned Penetration Testing, the likely and potential impact and how this may affect them directly, the date and time of the Penetration Testing;
4. You confirm that you have obtained all consents required from data subjects to enable personal data (as defined in applicable data protection legislation) to be disclosed to Claranet Cyber Security to the extent required to carry out the Penetration Testing;
5. You confirm the carrying out of the Penetration Testing does not contravene any law or regulation in so far as it relates to individuals, users, third party information stakeholders, third party information service providers or other parties likely to be affected by the Penetration Testing on your information systems;
6. You agree that you will provide where appropriate, all necessary authorisations for access to target systems to Claranet Cyber Security, including, where necessary, modifications that demonstrate the impact of exploitation of a vulnerability.
7. You agree to take all reasonable measures to protect your information system from any loss or damage that may arise as a consequence of the Penetration Testing. Prior to commencement of the Penetration Testing, you will take copies of information and applications or use any other methods available to them, to ensure the safety and protection of material within the information system. Claranet Cyber Security shall not be liable for any data loss including that which cannot be recovered due to inadequate back up or protection by you.
8. You agree that, where the Penetration Testing is to take place on your premises, you shall ensure that a suitable working environment is provided for the Claranet Cyber Security Penetration Tester which shall include network access and, where necessary, access to data centres, server rooms and/or switch rooms.
9. You agree that should you require a laptop or other device to be security tested by Claranet Cyber Security at our offices you will deliver the laptop and/or other device to Claranet's designated office and collect it from those offices or authorise other means of delivery and return at your own risk. Claranet Cyber Security shall not be liable for the laptop, device, or PDA during transit to or from its offices.

10. You agree to provide Claranet Cyber Security with at least one employee who has substantial computer systems, network and project management experience of your information system to act as liaison between you and Claranet Cyber Security.
11. You agree to co-operate with Claranet Cyber Security and to provide it promptly with such information about your information system, network, premises, equipment, data structures, protocols, software, hardware and firmware as are reasonably required by Claranet Cyber Security to perform the Penetration Testing.
12. You confirm that, where the Penetration Testing is taking place on your premises, the premises are safe in line with current local Covid-19 guidelines, suitable and reasonable to accommodate Claranet Cyber Security's Penetration Tester and the Penetration Testing.
13. You agree that copyright in the report(s) received by you in relation to the Purple Team Assessment shall remain the property of Claranet Cyber Security, and that Claranet Cyber Security, upon receipt of payment in full, hereby grants you a non-exclusive, non-transferable licence to copy and use the contents of those reports for your own internal purposes only.