GÉANT Security Portfolio

Helping protect and secure vital Research and Education resources

July 2023

Production Services and Solutions

Trusted Certificate Service – geant.org/tcs

The Trusted Certificate Service gives NRENs and their constituents easy access to high quality certificates of the most used types: SSL, grid, client, code signing and document signing.

TCS takes advantage of a bulk purchasing arrangement whereby participating national research and education networking organisations (NRENs) may issue close to unlimited numbers of certificates provided by a commercial CA at a significantly reduced price.

eduVPN – eduvpn.org

A privacy-savvy open-source VPN solution for either controlled access to campus networks or safe internet access or both. eduVPN comes with apps for all major platforms with easy access for end-users.

DDoS Protection

Protection against DDoS attacks coming from the borders of the GÉANT network with NSHARP. A combination of detection and mitigation tools protects the connection of an NREN from unwanted excessive traffic coming through the GÉANT network form upstream internet, transit traffic and other peering connections.

Firewall on Demand

Firewall on Demand (FoD) is a BGP-FlowSpec-based (RFC5575, RFC7674) DDoS mitigation solution which was previously developed in earlier phases of the GÉANT project and is currently provided in the GÉANT core network to allow users (NREN NOC administrators) to administer BGP FlowSpec rules via a web interface. This allows them to filter normally routed GÉANT IP traffic based on the administered BGP FlowSpec rules.

Training and Awareness

CLAW – Crisis Management

The annual CLAW event supplies training and exercises for participants from NRENs for communication and technical (ICT, Security) teams as well as management. The training covers both the crisis management process and personal skills for crisis handling. Some of the exercises are “boxed” and available for playing in your own organisation.

Security Training

There is a range of security training services available, both classroom based and online.
Transits I and II: Flagship classroom training for incident response team .

Operational network security: Online training, four modules of four to five 1-hour webinars.

Forensics: Online training two modules of webinars.

Blue team training: A small scale online hands-on training for incident response teams focused on analysis and forensics.

Security Awareness

Security awareness made easy with a library of materials and a full annual campaign every October - Cyber Security Month.

Content is shared freely and participation in cybersecurity month is encouraged. A wide range of blogs, webinars and promotion material is available: in different languages and optionally white labelled.

Pilot and Research Activities

Tools for SOCs

A comprehensive set of tools for supporting Security Operations, small scale or large scale. These tools support the complete SOC lifecycle with information gathering based on MISP, incident response and incident analysis. The toolset is modular and can be tuned to your needs.

Vulnerability Assessment as a Service

With this activity we provide several solution for security teams:

- An open source free-to-use vulnerability scanner as a service.
- A commercial vulnerability scanner, either cloud based or on premise, with very competitive licensing.
- A free intelligence feed.

DDoS Tooling

A set of tools for detection and mitigation of DDOS attacks in your own network, based on NEMO. It can be deployed in NREN networks to protect the connections of constituents. This has the advantage over DDOS protection in the GÉANT network as it can also protect against attacks coming from other upstream providers.

Business Continuity Frameworks

A comprehensive set of frameworks and good practices for implementing and testing Business Continuity Management, accompanied with a number of example policies, plans and strategies for implementing business continuity management in your organisation.

Pilot and Research Activities

Cyber Threat Intelligence

Analysing, categorising and sharing cyber threat intelligence is key in defending against the growing threats in cyberspace. With this activity we combine the power of several NREN SOC teams as part of the R&E Cybersecurity Intelligence Sharing Hub.

Securing High Speed Networks

Research best practices for securing high-speed networks, including investigation of how security is perceived, whether existing tools can be used, as well as how to make high-speed networks secure by design.

Security Baseline and Benchmarking

The security baseline is a common information security framework dedicated to NRENs and institutions. It outlines all essential aspects of security in a comprehensive set of four groups of measures. The baseline can be used as guidance for implementing or improving security and for benchmarking the maturity of security and preparing for compliance with security regulations like NIS2.

GN5-1 WP8 can assist with implementation and benchmarking with local workshops.

security.geant.org

Co-funded by the European Union

GÉANT