Vulnerability Management Service (VMS)

security.geant.org/vulnerability-management/

Service Description

The vulnerability management service is a cybersecurity service designed to identify, prioritise, and address vulnerabilities within an organisation's systems, networks, and applications. It involves monitoring (scanning), assessment, and the remediation of potential security weaknesses to prevent exploitation by cyber threats. A vulnerability management service is needed to protect digital assets and sensitive data from cyberattacks, data breaches, and other security incidents. By proactively identifying vulnerabilities and applying patches (updates to a device) or security measures, it helps mitigate the risk of exploitation.

GÉANT's Vulnerability Management Service provides the capability to scan network-attached IT assets on potential security vulnerabilities such as missing updates or insecure system configurations for example weak authentication or excessive privileges.

Using the results of the service, NREN's or their connected institutions can:

- Investigate and resolve the reported issues.
- Keep track of common vulnerabilities within IT assets of the NREN or the connected institutions.
- Use the service to audit IT-assets to measure compliance.

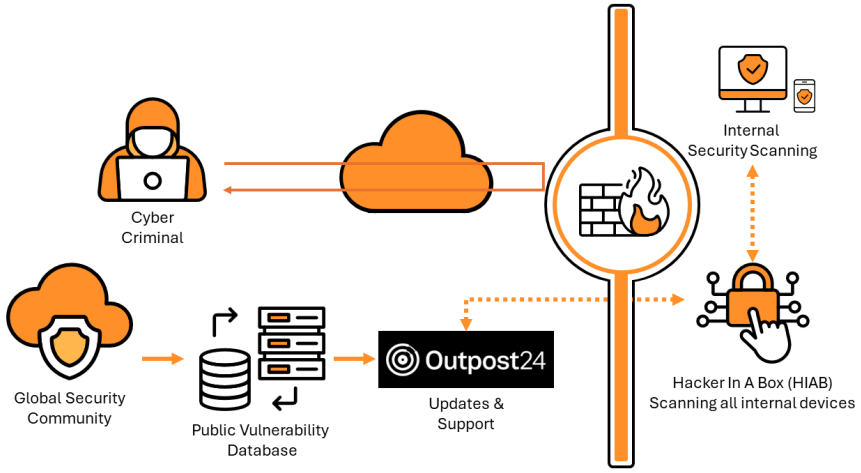
This service is suited for all NRENs that want to improve their security maturity by performing vulnerability scanning for themselves, their connected institutions or want to resell the service to their connected institutions and want to benefit from a competitive price for a commercial product.

Deployment

The service can be deployed to scan both internal and external IT assets using two methods

- Hacker In A Box
- OUTSCAN

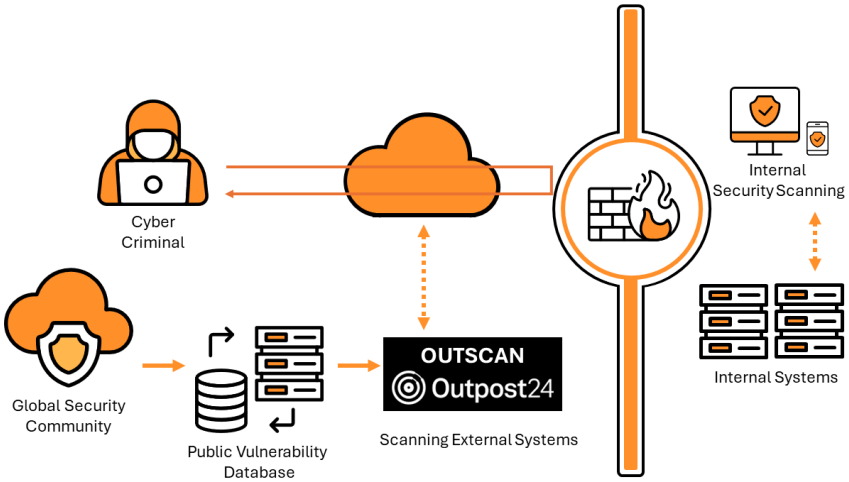
Hacker In A Box



Internally facing assets - are evaluated from a HIAB (Hacker-in-a-Box), a virtual machine that is hosted by the institution and scans the internal network of the users. Assessment information can only be stored in the HIAB but from an efficiency perspective is usually sent to the Outpost24 platform. HIAB operation is controlled through a web browser once deployed to an environment meeting minimum system requirements.

This model scans all internal devices – this is of particular relevance to universities where IT systems may be less well controlled. For example BYOD issues with insecure/compromised student devices or systems built by individuals outside of central IT control.

OUTSCAN



Externally facing assets - are evaluated from Outscan, a cloud-based service operating in Outpost24's private cloud in Sweden. Assessment information is stored in Outscan. Outscan operation is controlled through a web browser that meets minimum system requirements.

This implementation is designed to assist IT departments in monitoring any external or externally facing systems for example firewalls, public servers or cloud based systems

Results can be reviewed in the Outpost24 portal and contain vulnerability descriptions and recommendations to mitigate or fix the vulnerabilities. Results can be exported in XML, PDF, or CSV format.

Pricing Information

GÉANT has negotiated preferential terms with Outpost24 and the business model implemented reduces the need for tendering processes.

NRENs can opt for two different usage models; Fully Managed or Self-Service.

In the Fully Managed model the NREN controls the scans of its own resources and also instigates the scans of the connected institutions that wish to use the service. In this way the institution needs only to provide the NREN with the relevant address ranges to be scanned.

In the Self-Service model, the NREN provides the Institution with management access to the service and they control the scope and frequency of their scanning.

The costs are calculated on a pay-per-use basis and are invoiced every quarter. In all usage models, the NREN is responsible for paying for the hosts scanned.

With the fully managed model, the NREN has more control over which assets are scanned, so the connected institutions cannot make costly mistakes while scanning. In the self-service model, the connected institutions have control over which assets are scanned, so very clear communication between NREN and the connected institutions is required to avoid unwanted large bills.

It must be noted that the full responsibility for paying for the scans lies with the NREN, not with GÉANT.

Required Resources

The NREN needs at least one person to be responsible for the resale process to its member institutions. They need to work closely together to understand their specific needs, including the number of assets to be scanned and their existing infrastructure. They need to make it clear that their affiliates are aware of the monetary outcome of scanning assets.

With this service, scans are not triggered and run on demand. Instead, users schedule scans to assess vulnerabilities in their assets (which can also be scheduled only once). The frequency of these scans depends on factors such as the importance of the system and how frequently it changes. For example, a website that is updated daily may require daily or weekly scans, while servers are typically scanned monthly. The scanning frequency is customised to meet the specific needs of each system and its importance within the organisation.