Vulnerability Management

Service Description

V1.0 January 2025

Contents

+44 (0) 203 855 6215 | info@normcyber.com | normcyber.com

1. Service Description

The Vulnerability Management Service from NormCyber provides regular vulnerability scanning across the Customer's estate. Using vulnerability scanning tools and intelligence feeds, vulnerabilities and the steps required to remediate them are made available in near real time.

The optional Patch Management module helps reduce the burden of remediation by regularly applying patches across some of the most commonly used applications.

+44 (0) 203 855 6215 | info@normcyber.com | normcyber.com

2. Service Operation

Vulnerabilities identified on devices and endpoints will be evaluated, enriched and made available in the Smartbloc portal, in order to assist with the prioritisation of actions.

Patch Management Customers have a regular software update cycle where required patches for in-scope managed products are deployed to compatible devices that have the Norm endpoint scanner installed. Workstation endpoints such as laptops and desktops have a weekly update cycle. Server endpoints have an agreed update cycle. Patches for critical, emergency or "zero-day" software vulnerabilities may be deployed outside of the regular schedule (once Customer approval has been obtained).

2.1. Platform management

The Norm Technical Operations team are responsible for day-to-day platform management as well as investigating and responding to support incidents. Support incidents will be created when there is an issue with the availability or functionality of the Service and further investigation or remedial action is required. These may be raised by the Customer but can also be proactively raised as a result of a monitoring alert or other issue identified by the Norm Technical Operations team.

Platform management consists of the ongoing operational activities required to support the underlying technologies that support the Vulnerability Management Service with the objective of ensuring that the Service is delivered effectively and efficiently by maintaining system performance, quality, and stability.

2.1.1. Ongoing monitoring

Continuous monitoring of the health of the underlying technologies supporting the Vulnerability Management service, such as:

- The health of the Vulnerability Management platforms
- The health of Customer appliances from which Norm is gathering data

2.1.2. Operational management

Regular administrative procedures, such as:

- Hardware and software license management
- Monthly reporting on service utilisation
- Backups of Vulnerability Management platform configuration and data

+44 (0) 203 855 6215 | info@normcyber.com | normcyber.com

3. Service Onboarding

Once an Order is received, a member of the Norm Customer Experience team will get in touch and take responsibility for managing the delivery process. The technology required to monitor the Software installers and agents will be made available for download in the software section of the Smartbloc portal, along with the required user guides in the documents section.

Where specified, Customers will also be assigned a designated delivery team comprised of a:

- Service Delivery Manager, who will manage the delivery and provide updates on a weekly basis.
- Service Delivery Engineer, who will be the main technical point of contact for deployment.
- Focal Analyst, who will begin the process of educating the SOC about the Customer environment and co-ordinating the initial tuning phase.

The Service Delivery Manager will liaise with the Customer and provide support through the delivery and transition to in-life service management, including:

- A kick-off meeting in which a communication plan will be agreed. To include modes of communication, and agreement of target delivery dates.
- Weekly update meetings to review progress, issues, and dependencies and agree next steps.
- Co-ordination with Norm internal teams to facilitate delivery of the service.

3.1. Data collection

Data required to deliver the Vulnerability Management service can be collected from three possible sources, where specified in the Order:

- Internal network
- External network
- Endpoints

This data will be retained for a maximum of 13 months. All Customer-specific data gathered from the service will be used only for the purposes of delivering the Vulnerability Management service; and will be stored, managed, and disposed of in full accordance with UK and EU GDPRs.

3.2. Internal network vulnerability scanner(s)

Norm internal network scanner(s) will be deployed to the Customer environment in agreed locations. The network scanner will be a virtual appliance that is delivered via the Smartbloc portal and commissioned with remote assistance from a member of the Norm Service Delivery team.

The scanner(s) will be configured to scan the network environment on an agreed schedule.

3.3. External network vulnerability scanner

A Norm cloud-hosted network scanner will be deployed within the Norm environment. It will scan and scrutinise all externally facing devices on the IP ranges provided by the customer such as servers, routers, firewalls, VPN gateways etc on a regular schedule.

3.4. Endpoint vulnerability scanner

Norm endpoint scanner agents will be deployed to all compatible in-scope endpoints. They will scan the endpoints for known vulnerabilities on a regular schedule.

4. Service Management

The primary source for day-to-day interaction with the service will be the Smartbloc portal (https://smartbloc-live.com/). Customers will be provided with an administrator account during the delivery phase to enable access the Vulnerability Management dashboard which contains real-time information about vulnerabilities, hosts, and patch status. The vulnerability data gathered from the Vulnerability Management service contributes towards the Cyber Resilience Score.

+44 (0) 203 855 6215 | info@normcyber.com | normcyber.com

5. Customer Obligations

Once the Order is accepted, the Customer shall,

- provide any documentation or information necessary for the configuration of the service within ten (10) working days after it has been requested by Norm.
- be responsible for ensuring the information provided is accurate and up to date.
- be responsible for ensuring that information held by Norm for the configuration of the service remains accurate and up to date.
- provide an Authorised Representative who shall be the Customers Administrator for the Services and responsible for creating and managing access for other Customer End Users who need access to the Service or Smartbloc portal.
- be responsible for Authorised Representatives and End Users' compliance with the use of the Services under this Agreement and will take reasonable and appropriate steps to ensure such compliance.
- ensure that all necessary notices have been provided, and all required consents and/or approvals have been obtained, in order to allow Norm to process the Customer's Data in connection with the Services.
- use reasonable endeavours to prevent unauthorised access to or Use of the Services and notify NormCyber promptly in writing of any such unauthorised access or use.
- use the Services only in accordance with this Agreement, and all applicable laws and regulations.

The Customer shall not,

- make the Services available to anyone other than the Authorised Representatives
- sell, resell, rent, lease, lend, loan, distribute, sublicense or otherwise assign or transfer the Services or any rights thereto in whole or in part
- use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party rights (including privacy rights)
- use the Services to store or transmit Malicious Code
- interfere with or disrupt the integrity or performance of the Services or third-party data contained therein
- attempt to gain unauthorised access to the Services or related systems and/or networks, or
- use the Services in any manner that would cause NormCyber to be in violation of any laws, rulings or regulations

6. Decommissioning

At the end of the service period, access to the Smartbloc portal will be removed and Customer data held by Norm will be deleted after 30 days. The Customer will be responsible for uninstalling agents, and removing configuration applied during on-boarding.

+44 (0) 203 855 6215 | info@normcyber.com | normcyber.com