LYNQ

Security Incident Management

AUGUST 2022

Table of Contents

Overview

LYNQ recognise that security incidents can happen and therefore maintaining effective methods for handling incidents is important. By utilising a comprehensive set of security measures, we ensure to protect customer information and offer the most reliable and secure service we can.

LYNQ continually develop and improve its approach for responding to security incidents that affect services or infrastructure. Our incident response approach includes comprehensive logging and monitoring to ensure potential incidents are detected early. Our ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2020, certified information security management system (ISMS), defines all the processes we need to follow, during all stages of an incident.

Failure or anomalies in our products and infrastructure are continually monitored. These systems alert us immediately if an activity is detected that requires further investigation. Site Reliability Engineers monitor the platform to make sure it is always available.

Certificate No:388482022

Reporting Incidents

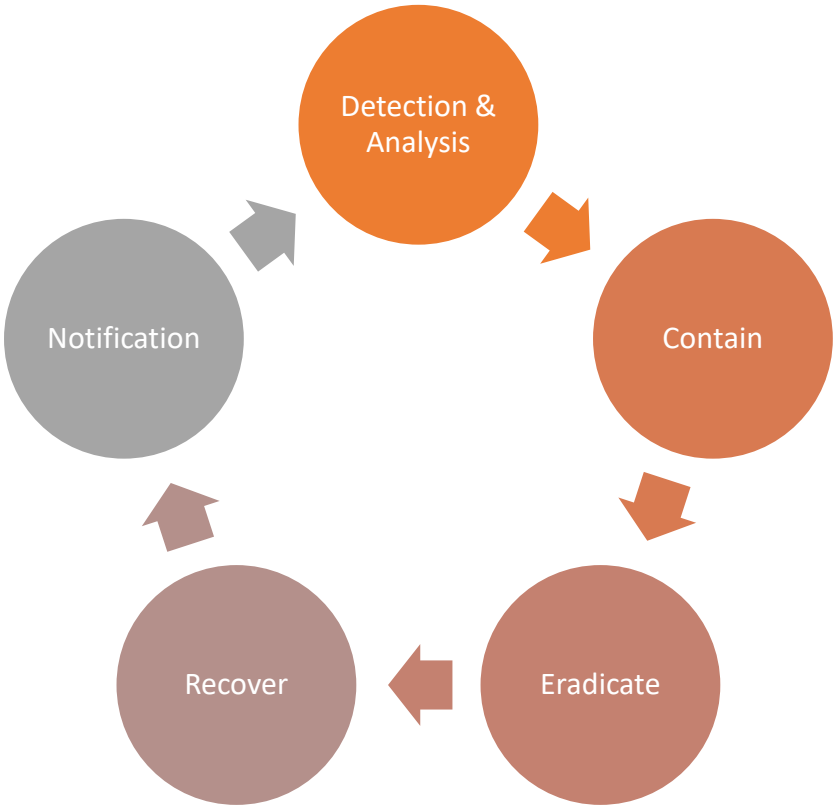
Through our support channel, users are able to make LYNQ aware of vulnerabilities or treats. Security incidents can be reported using our dedicated support email address support@lynqmes.com or by calling the support team on (+44 1329 800 000).

Managing Incidents

Our defined security framework covers the steps we need to take at each phase of the incident response process. The aim of this process is to standardise LYNQ's response to any security incident and ensure that they are appropriately logged and managed in accordance with the law and best practice, so that:

- incidents are reported swiftly and can be properly investigated
- incidents are dealt with in a timely manner and normal operations restored
- incidents are recorded and documented
- the impact of the incident is understood and action is taken to prevent further damage
- the ICO and data subjects are informed as required in more serious cases
- incidents are reviewed and lessons learned

At a high level, our incident management process follows these phases:



Detection and Analysis

The analysis of data from log management systems helps LYNQ to understand the corresponding events leading up to the incident. A consistent approach to dealing with all security incidents is maintained across LYNQ and each incident is evaluated.

The evaluation of the security incident will include some of the following questions:

- Had the incident been identified as a risk prior to its occurrence?
- Did the incident occur despite existing measures being in place?
- Were current policies and procedures followed? If not, why not?
- In what way did the current measures prove inadequate?
- How likely is the incident to recur?
- Did the incident involve deliberate or reckless behaviour?

Categorisation

Once a security incident has been identified, it will be analysed for its severity and impact:

Incident Severity & Impact Levels	
Critical	Critical incident with maximum impact
High	Major incident with very high impact
Medium	Major incident with significant impact
Low	Minor incident with low impact

Contain, Eradicate and Recover

Once an incident has been categorised, there may be a need for immediate action in order to limit the damage from the breach and recover any losses. Action may also be needed to prevent another breach with similar circumstances whilst the investigation is taking place. This may include action taken to prevent any further unauthorised access:

- secure any affected buildings (i.e. changing locks, access codes etc.)
- recover any equipment or physical information
- restore lost or damaged data by using backups
- prevent a further breach relating to the same information (e.g. an attempt to use stolen data to access accounts or services)

Once the potential threat has been contained, the root cause of the incident will be investigated so it can be properly eradicated. Products and infrastructure are constantly checked to confirm they are running as expected.

Notification

Depending on the incident there may be legal, contractual or sector specific requirements to notify various parties. Notification may assist in security improvements and implementation, as well as risk mitigation.

Whenever LYNQ becomes aware of a breach of security involving unauthorised loss, disclosure, or modification of customer data, LYNQ notifies the affected customers within 72 hours as outlined in the Data Protection Addendum (DPA). The notification timeline commitment begins when the official security incident declaration occurs. Upon declaring a security incident, the notification process occurs as expeditiously as possible, without undue delay.

Notifications include a description of the nature of the breach, approximate user impact and mitigation steps (if applicable). If LYNQ's investigation isn't complete at the time of initial notification, the notification will also indicate next steps and timelines for subsequent communication.

If a customer becomes aware of an incident that could have an impact on LYNQ including but not limited to a data breach, the customer is responsible for promptly notifying LYNQ of the incident as defined in the DPA.

Security Bug Fix Policy

LYNQ make it a priority to ensure that security vulnerabilities in its applications are promptly resolved. We have defined the following timeframes for fixing security issues in our products.

Cloud based LYNQ products

Security Incident Resolution Times	
Critical	Within 2 weeks of being verified
High	Within 6 weeks of being verified
Medium	Within 12 weeks of being verified
Low	Within 26 weeks of being verified

Self-managed LYNQ products

Security Incident Resolution Times	
Critical	Within 90 days of being verified
High	Within 90 days of being verified
Medium	Within 90 days of being verified
Low	Within 180 days of being verified

Critical Vulnerabilities

When a Critical security vulnerability is discovered by LYNQ or reported by a third party, LYNQ will:

- Issue a new release for the current version as soon as possible
- Notify the affected customers paying annual license fees and ask them to upgrade to the latest version containing the fix
- Apply the fix to the cloud platform at the earliest maintenance window

Non-critical Vulnerabilities

When a security issue of a high, medium or low severity is discovered, LYNQ will include a fix in the next scheduled release. You should upgrade your installations when a bug fix release becomes available to ensure that the latest security fixes have been applied.

Severity Levels for Security Bugs

The table below indicates how LYNQ determine the severity of the security bugs.

Severity	Characteristics
Critical	• Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices. • Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims, and does not need to persuade a target user, for example via social engineering, into performing any special functions.
High	• The vulnerability is difficult to exploit. • Exploitation could result in elevated privileges. • Exploitation could result in a significant data loss or downtime.
Medium	• Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. • Denial of service vulnerabilities that are difficult to set up. • Exploits that require an attacker to reside on the same local network as the victim. Vulnerabilities where exploitation provides only very limited access. • Vulnerabilities that require user privileges for successful exploitation.
Low	• Vulnerabilities in the low range typically have very little impact on an organisation's business. Exploitation of such vulnerabilities usually requires local or physical system access.