Diebold Nixdorf

DieboldNixdorf.com

Global Security Portal

User Manual

Release Information

Document version: 1.5

Release date: 15th April 2024

Contents

1 Introduction

The name Diebold Nixdorf is synonymous with security - our heritage is based on innovative solutions that protect people, data, and assets. Keeping financial institutions, retailers, and their consumers safe is in our DNA. For more than 160 years, our clients have placed their trust with us to secure their most vital assets.

From the first bank safes and vaults, we continue to innovate to develop technologies and help guide the industry in response to real world requirements – that will protect, secure, and drive the future of self- service security.

Today, self-service solutions are the primary connection point for financial institutions, retailers, and their consumers—and that touchpoint represents the institution it serves. It must be engaging, but also highly secure. Every single transaction, every single time. There's an inherent level of trust that consumers place in their banks and retailers when they conduct a transaction. If that trust is damaged, consumers will simply take their business—and their assets—elsewhere.

1.1 About this Document

This user manual is meant to provide information to all users of the Global Security Portal (GSP) concerning the functionalities and corresponding processes.

Please note: Access to some functionalities of the Global Security Portal is dependent on the granted user permissions. For example, ACTive Security Notifications require dedicated terms and conditions to be acknowledged to ensure Diebold Nixdorf is not held liable for any damages associated with the use of or the reliance upon information provided through the notifications.

1.2 The ACT Approach

At Diebold Nixdorf, we've always taken an **ACT**ion-based approach to security. Our newly enhanced security portal solidifies our "ACT" global security strategy, offering more tools to help you ACT quickly when fraud occurs.

The ACT approach entails constantly **A**nalyzing, **C**ommunicating and **T**racking threat vectors around the world. It's the foundation of our Global Security Portal and communications process.

Figure 1 – ACT: Analyzing, Communicating and Tracking Threats

2 Getting Started

The Global Security Portal supports two options for user authentication, either by federation between your business/company and Diebold Nixdorf or via a Diebold Nixdorf guest account.

This guide focusses on the registration of a Diebold Nixdorf guest account to access Diebold Nixdorf applications like the “Global Security Portal”. If your business/company prefers to establish federated authentication, please directly get in contact with info.gsp@dieboldnixdorf.com.

2.1 Registration Process

To register for the Global Security Portal, go to https://www.dieboldnixdorf.com/en-us/support/globalsecurityportal/ and select „Subscribe now” from the top or bottom of the page:

Figure 2 – Register on the Login Page

Step 1: Registration
As a first step of the registration you must enter your contact details.
Please make sure to use your company email address, as private email addresses are not allowed.

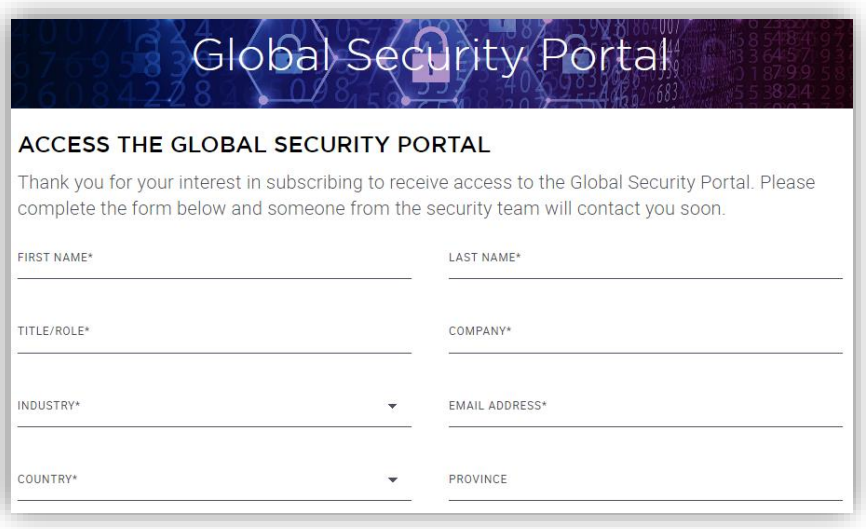

Figure 3: Registration Process

As part of this submission, you must choose your subscription type:

- **ACTive Security Alerts**
  Contain information on modus operandi and attack vectors concerning the Diebold Nixdorf portfolio. Financial institutions should consider taking “action” based on the information provided, if applicable to their operations**.** Access to ACTive Security Alerts includes access fACT Sheets.

- **ACTive Security Notifications**
  Contain initial information on reported incidents in anonymized form. As such, information provided may be unconfirmed, evolving, or otherwise inaccurate, as there is still an “active” investigation in progress. Due to this, access to notifications is permission based and ***requires agreeing to specific T&C’s***. Access must be requested through contacting info.gso@dieboldnixdorf.com specifically. Access to ACTive Security Notifications includes access ACTive Security Alerts and fACT Sheets.

Step 2: Create Guest Account

After submission, it will be verified whether a Diebold Nixdorf Guest Account already exists for your e-mail address. If it exists, please proceed to Step 3). If not, an invitation to create a Diebold Nixdorf Guest account is sent to your e-mail address (by no-reply@dieboldnixdorf.com). Please follow the “Click here to accept the invite” link to start the account creation.

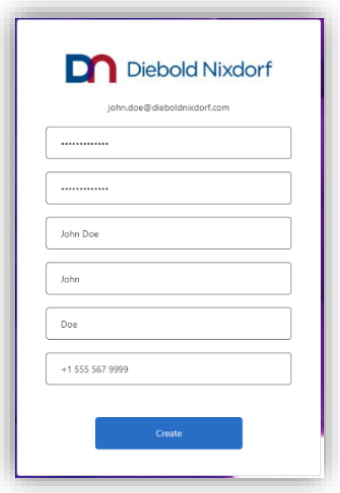

Figure 4: Create Diebold Nixdorf Guest Account

Step 3: Invitation to the Global Security Portal

Once the Diebold Nixdorf Guest Account is created successfully, an invitation to use the Global Security Portal is send by info.gsp@dieboldnixdorf.com to the registered e-mail address.

Please follow the “Click here to accept the invite” link and navigate to finalize the process. Please choose “Sign in using Unily B2C”

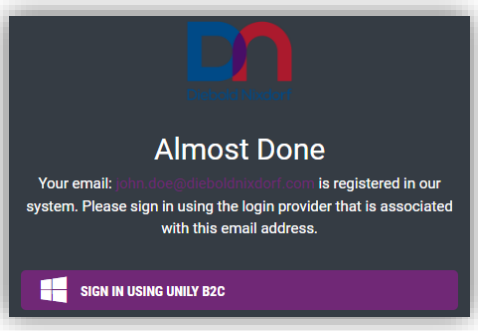

Figure 5: Diebold Nixdorf B2C Login

Step 4: Login to the Global Security Portal

Your browser will open a page like this. Sign in using the credentials of your Diebold Nixdorf Guest Account.

You will be prompted to select an “MFA Method”, please select your preferred option, and click “Send Email/SMS Code”. Once the verification code is received, please enter and click “Verify Email/SMS Code”

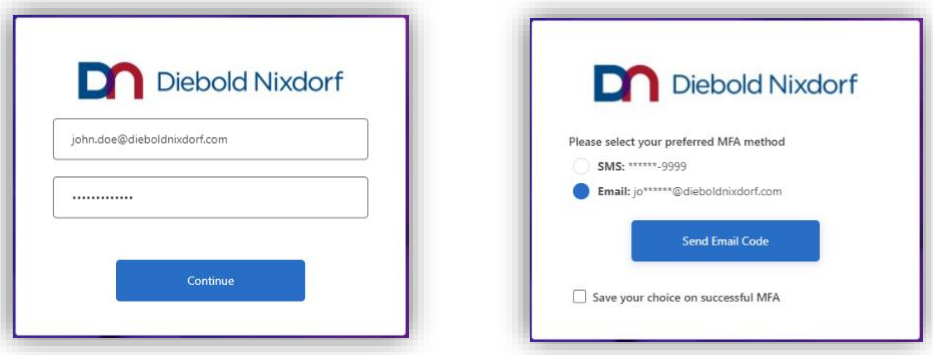

Figure 6: Login with MFA

You will now be redirected to the Diebold Nixdorf Global Security Portal

Note: It is possible that a “Permission denied”- error is displayed on first login. If that is the case, please manually navigate to: https://exchange.dieboldnixdorf.com/sites/global-security-portal/startpage/SitePageModern/103917/gsp-agreement

2.2 Sign In

The log in procedure into the portal can be distinguished by the log in type provided to the user in different situations.

To log into the Global Security Portal, please navigate to https://www.dieboldnixdorf.com/en-us/support/globalsecurityportal/ and select „Login” from the bottom of the Login Page:

Figure 7 – Login to the Global Security Portal

You will now be redirected to https://exchange.dieboldnixdorf.com/loginprompt. Please enter the email address associated with your Diebold Nixdorf login.

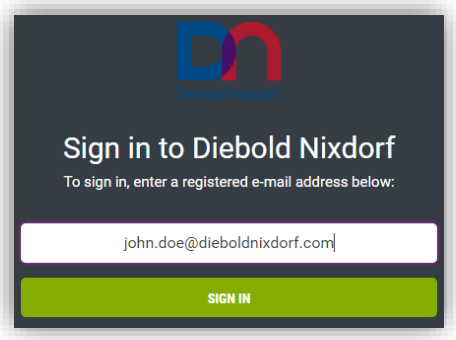

Figure 8: Diebold Nixdorf B2C Login

Depending on the account type (Guest Account/Federated Account), you are being redirected to the respective Credential Provider to authenticate using your credentials. In case of a Diebold Nixdorf Guest account, the following login screen is displayed.

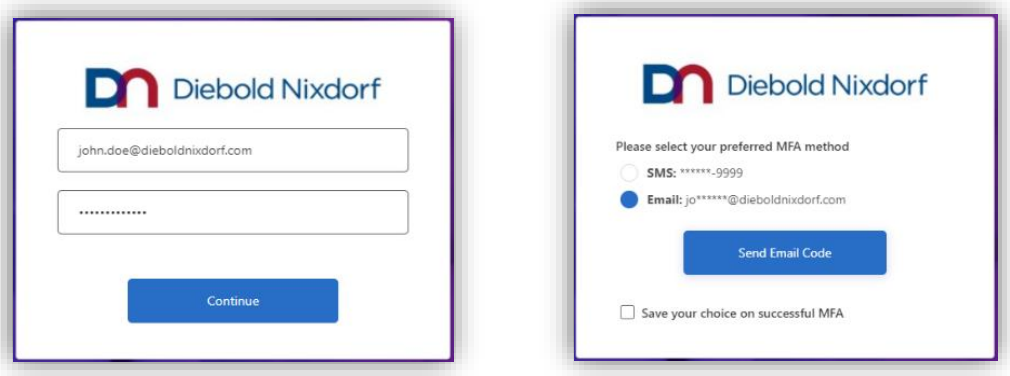

Figure 9: Login with MFA

As part of the login process you will be prompted to select an “MFA Method”, please select your preferred option, and click “Send Email/SMS Code”.

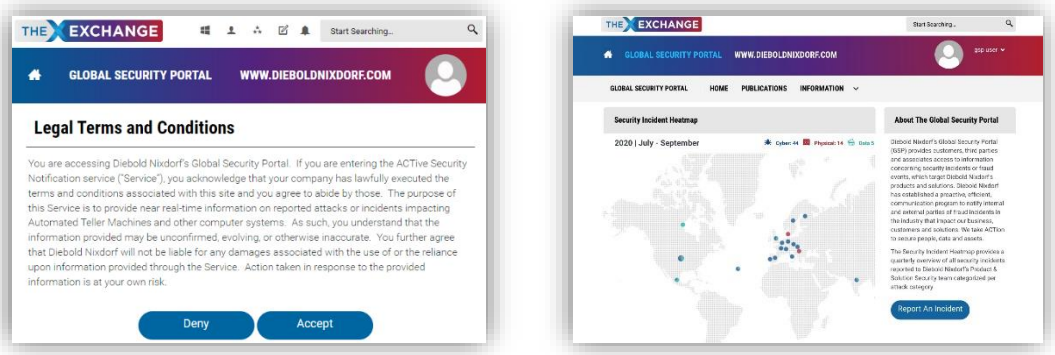

Figure 10: T&C's and Global Security Portal Home Page

You will be automatically redirected to the Global Security Portal. After accepting the legal terms and conditions you will be able to use the Global Security Portal.

2.3 User Management

To adjust the information of the logged in user account, it is currently required to send an e-mail to the info.gsp@dieboldnixdorf.com. You may request to change your personnel information or request any of the following services:

Account specific settings:

- Change Password
- Delete Account
- DN Contact Email
- Reset Password

Company Information

- Occupation / Title
- Street Address
- City
- State or Province
- ZIP / Postal Code
- Country

Contact Information

- Phone Number
- Mobile Number

2.4 Logout

For security reasons it is recommended to log out after using the portal. The related section can be accessed through the navigation pane under the menu item “My Account” à “Log Out”.

The user session automatically times out after an idle period of 15 minutes for security reasons. Whenever this happens, you can always sign in again to a new session.

3 Home Page

The “Home” page is the main hub, or your dashboard, to access the different publications on the Global Security Portal. Access to documents is provided through different document libraries that contain all documents of a certain type, additionally a visualization of all currently tracked incidents is provided through the Security Incidents Map.

3.1 Security Incidents Map

The Security Incidents Map displays all incidents that have been reported to Diebold Nixdorf and are tracked accordingly. It is designed to allow an easy overview of these incidents related to type of incident, number of incidents and country of origin. In general, it must be pointed out that not all reported incidents result in a publication of a document.

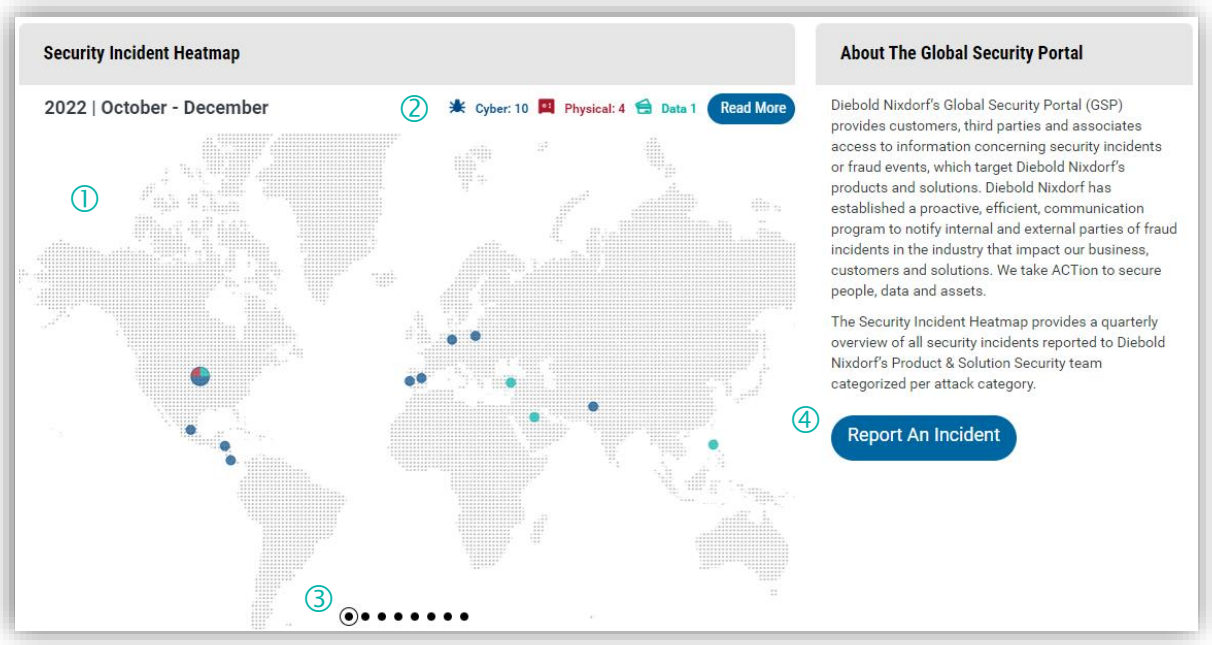

Figure 11 - Security Incident Map

① **Security Incidents Map**
Displays incidents reported and tracked by DN on a quarterly basis by location

② **Security Incidents Overview**
Displays incidents reported and tracked by DN on a quarterly basis by incident type

③ **Incident Map Navigation**
Change the quarter which is displayed in the Security Incident Map

④ **Report an incident**
Report new attacks directly to Diebold Nixdorf

3.2 Access to latest documents per type

The document section of the home page displays dedicated libraries for each document type provided on the Global Security Portal. Each library displays the last five released documents of the respective ACTive Security Alerts, fACT Sheets or ACTive Security Notifications.

Access to these libraries might be restricted depending on the permission level of the user as outlined in section 0 and 4.1.

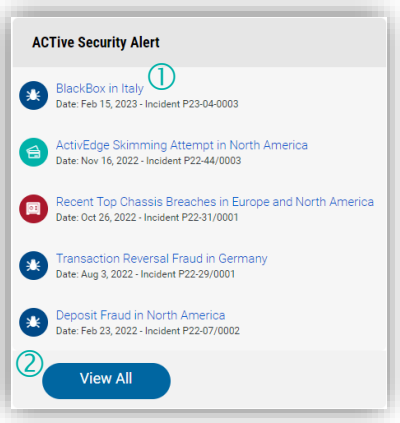

Figure 12 – Document libraries

① **Access to document**
By clicking a row will open the respective document

② **Show all documents of type**
Access to the library archive containing all documents of the type

3.3 Contact Us

The Global Security Portal is striving to constantly increase usability and to deliver relevant information to the user. Users can provide any kind of feedback directly to the Global Security Portal Team by using the “Contact Us” section.

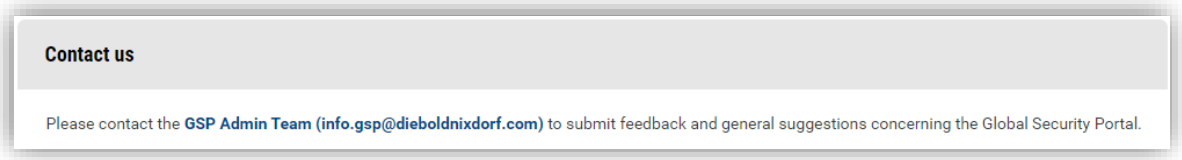

Figure 13 - Contact Us

In case of technical or permission issues, please contact info.gsp@dieboldnixdorf.com.

4 Publications

To access all documents that are published by DN, there is the “Publications” section that contains all publications of all available content types in a library that can be filtered. You can access Publications directly from the Main Navigation menu.

Figure 14 - Main Navigation: Publications

This library summarizes and displays all document types that a user is eligible to access. To allow for quick and easy access, the library allows different filter and display options which are described in the picture below.

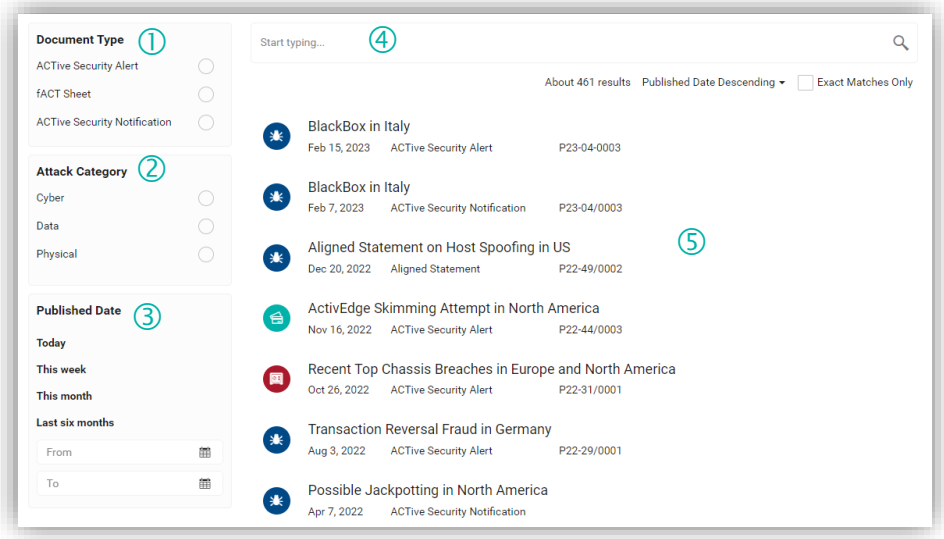

Figure 15 - Publications

① **Filter for Document Type**
Select a document type to restrict the search results to a certain type only

② **Filter for Attack Category**
Select an attack category to restrict search results to a certain category only

③ **Filter for Published Date**
Select a range of dates to restrict the search to only display publications of that time frame

④ **Search bar**
Restrict the search results to a specific document title

⑤ **Result Window**
Allows to access all publications matching the search criteria.

4.1 ACTive Security Notifications

ACTive Security Notifications contain initial information on reported incidents in anonymized form. As such, information provided may be unconfirmed, evolving, or otherwise inaccurate. ACTive Security Notifications are intended for members to decide whether to take individual countermeasures to decrease the overall exposure to their fleet. Actions taken in response to the provided information are at your own risk.

Due to this, access to notifications is permission based and requires a signed agreement to ensure Diebold Nixdorf is not held liable for any damages associated with the use of or the reliance upon information provided through the notifications.

4.2 ACTive Security Alerts

ACTive Security Alerts contain information and high-level description on modus operandi (MO) and attack vectors concerning the Diebold Nixdorf portfolio, which might be applicable to multiple customers.

4.3 fACT Sheets

fACT Sheets are used to summarize Diebold Nixdorf's state of knowledge on a specific situation or attack type at the time of creation. As such, fACT Sheets may not be related to a single incident, could comment on a dedicated third-party publication or on news articles. In addition, fACT Sheets might be used to provide additional details to support ACTive Security Alerts.

5 Attack Definitions

Information on the Global Security Portal is classified according to attack categories and attack types, there is the "Attack Definitions" section that contains information on incident classification and all related definitions. You can access Attack Definitions directly from the Main Navigation menu.

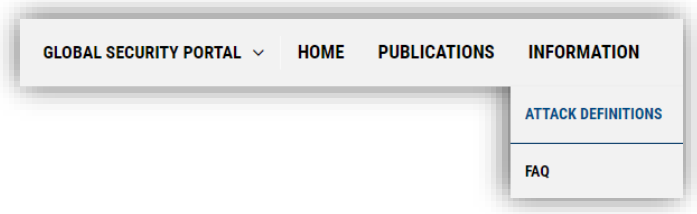

Figure 16 - Main Navigation: Publications

This library contains all Attack Definitions used by the Global Security Portal. The three main attack categories are data, physical and cyber each containing further subcategories (called Attack Types).

Figure 17: Attack Definitions

Each Attack Type uses a dedicated web page that provides detailed information on the respective attack allowing to understand what defines a certain attack, how to detect it and what the potential impact might be.

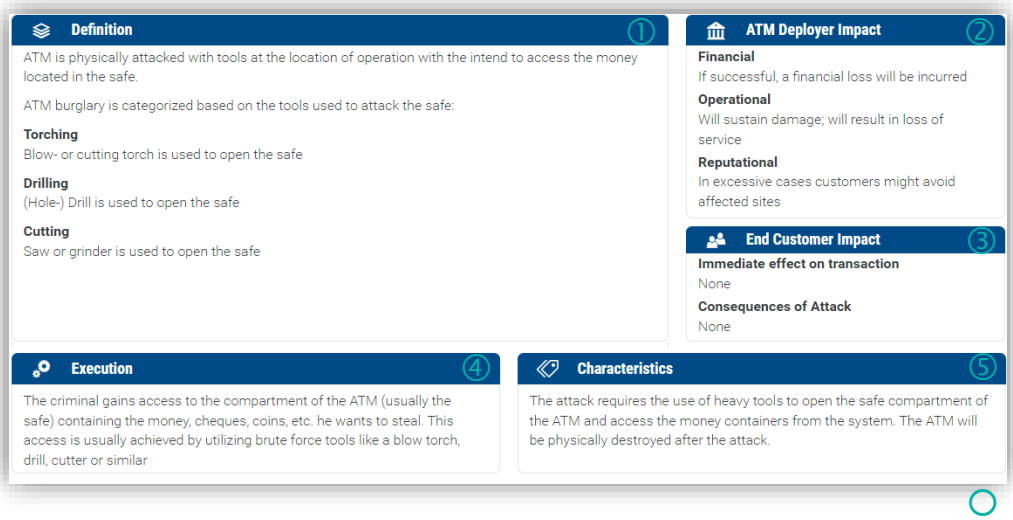

Figure 18: Definition of Modus Operandi

① **Attack Definition**
Description of the Modus Operandi of the Attack as well as potential variants

② **Impact on ATM Deployer**
What is the ATM Deployer impacted regarding financial, operational, and reputational losses

③ **Impact on Card Holder**
Impact on the Card Holder regarding financial losses and attack consequences

④ **Attack Execution Details**
Steps a malicious actor performs while executing the attack

⑤ **Identification Characteristics**
Potential identificatory characteristics to help detection of the attack type

6 Report Incidents

The Global Security Portal allows users to report potential security attacks to Diebold Nixdorf's Product & Solution Security team directly from the portal home page.

Figure 19 – Report an Incident

When “Report an Incident” is selected, an e-mail template will be opened which you may use to describe the incident and provide information on how the Diebold Nixdorf Product and Solution Security team shall get in contact for further investigations.

Please note: The initial contact will be routed through e-mail and is therefore not encrypted. Please do not send confidential data when reporting an Incident. The Diebold Nixdorf Product and Solution Security team will get in contact with an option to share confidential information once the incident is reported initially.

7 Appendix

7.1 Contact

In case of questions or suggestions for this user manual, please contact:

Diebold Nixdorf Product & Solution Security
info.gsp@dieboldnixdorf.com