

Cyber Detect &  
Respond Portal –  
*Reference Guide  
for MS-ISAC &  
EI-ISAC Members*



The purpose of this reference guide is to provide Multi-State Information Sharing & Analysis Center (MS-ISAC) and Elections Infrastructure (EI)-ISAC members with introductory, high-level information on Deloitte's Cyber Detect and Respond Portal ("Portal"), as well as to highlight important functions and features of the Portal and where Threat Advisories, Vulnerabilities, and other information can be obtained within the platform. This guide is also intended to aid users in navigating the Portal using screenshots along with informative boxes, arrows, text, etc. (in **green** font) to highlight and describe features and options for filtering searches, sorting information, configuring email notifications, etc. to improve the relevancy and usefulness of the Portal's Cyber Threat Intelligence (CTI) and other information. However, this reference guide is not meant to be an official and exhaustive manual on all functions and features of the Portal.

# Table of Contents

Section	Page
Overview of Cyber Detect & Respond Portal	4
MITRE ATT&CK® model	5
Account and authentication setup in Portal	6
Accessing Cyber Detect and Respond Portal	7
Dashboard view	8
Threat Advisories	
Threat Advisories view	16
Threat Advisory in-depth	18
Adding Threat Advisory Notifications	20
Editing Threat Advisory Notifications	21
Vulnerabilities	
Vulnerabilities view	22
Adding Vulnerability Notifications	24
Editing Vulnerability Notifications	25
Account Settings view	26
Bi-weekly Deloitte Cyber Threat Briefings	28
Deloitte Portal Terms of Use & Deloitte Privacy Statement	29

# Overview of Cyber Detect & Respond Portal

- Deloitte’s Cyber Detect & Respond Portal (“Portal”) is a secure, online platform for obtaining industry-leading **Cyber Threat Intelligence (CTI)** for enhancing knowledge, understanding, and the ability to identify potential cyber threats & attacks and reduce enterprise cyber risk.
- The Portal provides **in-depth analysis and recommendations from Deloitte’s worldwide network of Cyber threat analysts**, with **threat reports mapped to known tactics, techniques, and procedures (TTPs)** of cyber threat actors and malware campaigns.
  - Threat reports include **mappings of observed threat actor techniques to MITRE ATT&CK® Framework tactics** to help network defenders focus threat identification and hunting on behaviors and artifacts which may indicate a cyberattack.
  - Reports include real-world samples of observed attack procedures (e.g., phishing email excerpts, sanitized malicious code)
- The Portal also enables a **“pull” vs. “push” approach for obtaining CTI** that is ***tailored to an organization’s specific IT environment and cyber threat landscape.***
  - **Filter by categories and keywords** specific to threat actor group, malware campaign, system / application, industry, etc. to “reduce noise” and **focus on cyber threat and vulnerability information most relevant to your organization.**
  - **Configure email-based threat notifications and reporting, vulnerability notifications, etc. according to desired frequency** (e.g., daily, weekly) and filtered according to relevant categories of information, as noted above.
  - The **Portal Dashboard includes numerous options for tailoring graphical information on cyber threats and vulnerabilities** presented in individual “modules” (i.e., tiles) and even the ability to establish multiple dashboards, each with its own set of modules with differently configured graphical information providing a uniquely valuable view to a particular user.

# MITRE ATT&CK® model

Cyber Threat reports available in the Deloitte Portal include all observed techniques mapped to relevant MITRE ATT&CK® tactics, as demonstrated in the *notional* example below.

TACTICS (The "why?")	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
	Brute Force	PowerShell	External Remote Services	Bypass User Account Control	Bypass User Account Control	Brute Force	Local Network Discovery	Legitimate Credentials	Input Capture	Data Obfuscation or Encrypted	C2 Communication Obfuscated or Encrypted	Data Destruction or Encryption
	Downloaders/ Droppers	Process Hollowing	Legitimate Credentials	DLL Injection	Data Encoding	Credential Dumping	Network Shares	Local Network Discovery	Network Shares	Commonly Used Ports and Protocols	Remote Desktop Protocol	Vulnerability Exploitation
	Phishing/ Spam email	Psexec	Modify Existing Service or Create New Service	Legitimate Credentials	DLL Injection	Input Capture	System Information Discovery	Network Shares	Network Sniffing	Connection Proxy	Remote File Copy	
	Remote Desktop Protocol	Regsvr32	Network Shares	Modify Existing Service or Create New Service	Masquerading	Network Sniffing		Psexec		Uncommonly Used Port		
	Remote File Copy	Rundll32	Registry Run Keys/Start Folder	Vulnerability Exploitation	Modify Registry	Vulnerability Exploitation		Remote Desktop Protocol				
	Vulnerability Exploitation	Scheduled Task	Remote Desktop Protocol	Web Shell	Process Hollowing			Remote File Copy				
		Scripting	Scheduled Task		Regsvr32			Remote Services				
		Third-party Software	Web Shell		Rundll32			Third-party Software				
		Windows Management Instrumentation (WMI)	Windows Management Instrumentation (WMI)		Scripting			Windows Management Instrumentation (WMI)				
		Windows Remote Management			Vulnerability Exploitation			Windows Admin Shares				
								Vulnerability Exploitation				
								Windows Remote Management				
TECHNIQUES (The "how?" & the "what?")												

MITRE ATT&CK® includes a fully comprehensive matrix and knowledge base of adversary tactics and techniques based on real-world observations, which, along with additional information on MITRE ATT&CK®, is available at: <https://attack.mitre.org/>.

# Account and authentication setup in Portal

Once a new user is provisioned an account in Deloitte's Cyber Detect and Respond Portal ("Portal"), the user will receive an invitation email, per below:

- Invitation email will be sent from: [noreply@okta.com](mailto:noreply@okta.com). (Please note this is a "noreply" email address which is only used to send emails but cannot receive them.)
- If you do not receive this email, please check your junk folder. If you still cannot find it, please reach out to: [AthenaContactUs@deloitte.com](mailto:AthenaContactUs@deloitte.com) for assistance.
- Each user must activate his/her new Okta account (per email screenshot at below left) **within 30 days of email receipt or the invitation will expire.**
- Another email with the Portal URL and detailed instructions for setting up account authentication will be received from: [USAdvisoryCSApp001@deloitte.com](mailto:USAdvisoryCSApp001@deloitte.com).



If there are problems with how this message is displayed, click here to view it in a web browser.

**Deloitte.**

This is an automatically generated message. Replies are not monitored or answered.

## Deloitte MultiFactor Account (Okta) Activation Required

Hello [Name],

Please activate your Deloitte MultiFactor Account (Okta).

**Click the following link to activate your Deloitte MultiFactor Account (Okta).** This link expires after you have activated your account. If you do not activate your account within **30 days** of receipt of this email, a new activation link will have to be sent for your account.

[One-Time Activation](#)

### Important Please Read!

You only have to activate your Deloitte MultiFactor Account (Okta) once to setup your access. After you have activated your Deloitte MultiFactor Account (Okta), login using the following credentials:

#### Username:

**Password:** Use the password you setup during the Okta activation

**Login Page:** For security purposes a separate email will be sent with the login URL to your applications.

### Okta Activation - Steps following clicking the "One-Time Activation" link:

1. Type in a new password following the password requirements.
2. Select and answer a security question. This is what you will use for the password self-reset feature.
3. Choose a picture for your security image, and then click on "Create My Account."
4. Click "Got it!" on the Okta Notification.
5. Click on the "Cyber Detect and Respond Portal" application:
6. Choose between setting up the MFA using:
  - a. Okta Verify (native phone app)
  - b. SMS Authentication



### Okta Verify - Setup

1. Click on your device type (e.g., iOS, Android) and then click on "Next."
2. Scan the QR barcode to add your account.
3. Click on "Send Push" to send a push notification to your phone. Tap approve on your phone and the system will log you in.

### Okta SMS Authentication - Setup

1. Input your mobile phone number and click on "Send Code."
2. Input the code you received via text message and click on Verify. The system will then log you in.

# Accessing Cyber Detect & Respond Portal

The screenshot shows a web browser at the URL [athena.deloittefusion.net/users/login](https://athena.deloittefusion.net/users/login). The page features the Deloitte logo and a login form. The form includes a text input for 'Email/Username' with the placeholder 'Enter here' and a blue 'SIGN IN' button. Below the button, there is a link for 'User Support Email Us or Call 1-833-597-5441'. An 'Authentication Update' section provides information about a new authentication system for external accounts. At the bottom of the page, there is a copyright notice: '© 2021 Deloitte - Cyber Detect and Respond Portal. All rights reserved.'

**Cyber Detect and Respond ("Athena") Portal URL**  
*(Recommend bookmarking this URL in browser)*

**Begin log-in process by entering email address and then clicking on "SIGN IN"**

**User Support Email Address:**  
[AthenaContactUs@deloitte.com](mailto:AthenaContactUs@deloitte.com)

**User Support Phone number:**  
1-833-597-5441

# Dashboard view

**D.** ☰ 🔍 Search 🔊 👤 Welcome

Welcome to **Cyber Detect and Respond Portal**

Dashboard + Board Actions

Date Range: 📅

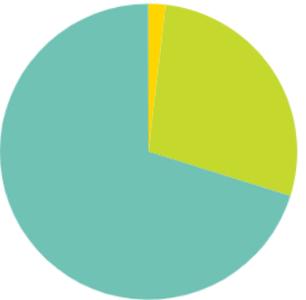
🔍 3 Recent Vulnerabilities 🔍 3 Recent Threat Advisories

**Threat Advisories by Threat Ty ...** 📄 ✕ This Month



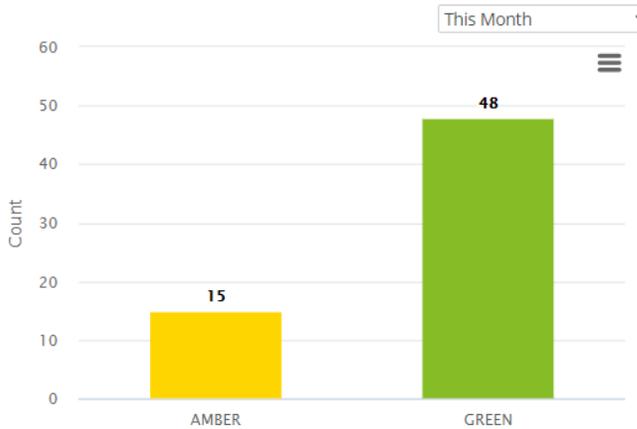
Threat Type	Count
campaign	15
incident	18
malware	10
threat-actor	5
vulnerability	5

**Vulnerabilities by Access Vect ...** 📄 ✕ This Month



Access Vector	Count
ADJACENT NETWORK	2
LOCAL	15
NETWORK	43

**Threat Advisories By TLPs** 📄 ✕ This Month



TLP	Count
AMBER	15
GREEN	48

© 2021 Deloitte - Cyber Detect and Respond Portal. All rights reserved. Privacy | Terms | Cookies | v3.22.9

# Dashboard view (cont'd)

The screenshot displays the Cyber Detect and Respond Portal dashboard. At the top, there is a navigation bar with a search bar and a user profile labeled 'Welcome'. Below this, the main content area is titled 'Welcome to Cyber Detect and Respond Portal'. On the left, a sidebar contains navigation icons, with a green box highlighting a specific icon. A green arrow points from this icon to a 'Portal Support' information box. Another green arrow points from a headset icon in the top right to a floating 'Portal Support' dialog box. The dashboard includes several data visualizations: 'Recent Vulnerabilities' (3), 'Recent Threat Advisories' (3), 'Threat Advisories by Threat Ty ...' (pie chart), 'Vulnerabilities by Access Vect' (pie chart), and a bar chart showing counts for 'AMBER' (15) and 'GREEN' (48).

**Portal Support**  
Available 24x7 to assist users with resolving portal related issues.  
+1-833-597-5441  
AthenaContactUs@deloitte.com

**Portal Support**  
Available 24x7 to assist with portal troubleshooting, issues, etc. You can send an email or call us directly.  
+1-833-597-5441 AthenaContactUs@deloitte.com  
More Info...

**Threat Advisories by Threat Ty ...**  
This Month

Threat Type	Count
campaign	1
incident	1
malware	1
threat-actor	1
vulnerability	1

**Vulnerabilities by Access Vect**  
This Month

Access Vector	Count
ADJACENT NETWORK	1
LOCAL	1
NETWORK	1

**Count**  
This Month

Category	Count
AMBER	15
GREEN	48

As shown above, there are two ways to access telephone and email contact information for "Portal Support" directly from the Portal Dashboard (i.e., landing page).

© 2021 Deloitte - Cyber Detect and Respond Portal. All rights reserved. [Privacy](#) | [Terms](#) | [Cookies](#) | v3.22.9

# Dashboard view (cont'd)

**D.**  ← **Expands side menu options**

**Quick links to 3 most recent reported Vulnerabilities and 3 most recent Threat Advisories**

 Search

Welcome to **Cyber Detect and Respond Portal**

Dashboard +

Date Range:  -

 3 Recent Vulnerabilities

 3 Recent Threat Advisories

**Board Actions** ▾

**Edit**  **Delete** 

**Threat Advisories by Threat Ty ...**  

This Month ▾

Today

Yesterday

This Week

Last Week

**This Month**

Last Month

Last 2 Months

Last 3 Months

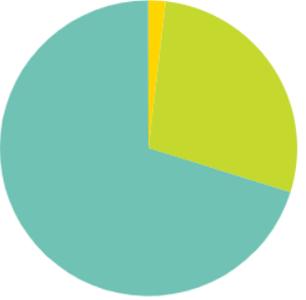
Custom Range



● campaign ● incident ● threat-actor ● vulnerability

**Vulnerabilities by Access Vect ...**  

This Month ▾



● ADJACENT NETWORK ● LOCAL ● NETWORK

**Threat Advisories By TLPs**  

This Month ▾

Count

60

50

40

30

20

10

0

15

48

AMBER GREEN

**Cyber threat and vulnerability information graphically displayed in each module can also be displayed for a variety of time periods.**

**Dashboard “modules” are fully customizable and provide user-specific, graphical views of various, relevant, and continually updated sources of cyber threat and vulnerability information and intelligence.**

© 2021 Deloitte - Cyber Detect and Respond Portal. All rights reserved.

Privacy | Terms | Cookies | v3.22.9

# Dashboard view (cont'd)

**Deloitte.**

Expanded direct link, side menu options

Dashboard +

Date Range: [Calendar Icon]

3 Recent Vulnerabilities

3 Recent Threat Advisories

Threat Advisories by Threat Ty ... This Month

Vulnerabilities by Access Vect ... This Mon

Threat Advisories By TLPs

athena.deloittefusion.net says  
Do you really want to delete Dashboard?

OK Cancel

15 AMBER

GREEN

LOCAL NETWORK

Today Yesterday This month This year Last month

	May 2021							Jun 2021								
	W	Su	Mo	Tu	We	Th	Fr	Sa	W	Su	Mo	Tu	We	Th	Fr	Sa
This month	16	25	26	27	28	29	30	1	21	30	31	1	2	3	4	5
This year	17	2	3	4	5	6	7	8	22	6	7	8	9	10	11	12
Last month	18	9	10	11	12	13	14	15	23	13	14	15	16	17	18	19
	19	16	17	18	19	20	21	22	24	20	21	22	23	24	25	26
	20	23	24	25	26	27	28	29	25	27	28	29	30	1	2	3
	21	30	31	1	2	3	4	5	26	4	5	6	7	8	9	10

Cancel Apply

Edit a Board

Board Name \*  
Dashboard

Cancel Save

Board Actions

Edit Delete

Feature for editing name of current dashboard

Feature for deleting current dashboard

Click on side menu links to:

- View Threat Advisories
- View Vulnerabilities
- Contact Support
- Logout
- Return to main Dashboard view

Date range set here will apply to all data across all Threat Advisories and Vulnerabilities modules in Dashboard.

# Dashboard view (cont'd)

The screenshot shows the Cyber Detect and Respond Portal dashboard. The main interface includes a navigation menu on the left, a search bar at the top right, and a 'Welcome' message. The dashboard displays several widgets: 'Recent Vulnerabilities' (3 items), 'Recent Threat Advisories' (3 items), 'Threat Advisories by Threat Ty ...', 'Vulnerabilities by Access Vect ...', and 'Threat Advisories By TLP's'. Three callouts are present:

- Create new dashboard:** A callout points to a '+' icon in the 'Dashboard' section and a 'Create a Board' modal window. The modal contains a 'Board Name' input field and 'Cancel' and 'Create' buttons.
- Copy current dashboard:** A callout points to a 'Copy Board' modal window. This modal includes a 'Board Name' input field and a 'Copy from' dropdown menu, with 'Cancel' and 'Copy' buttons at the bottom.
- Add module(s) to dashboard:** A callout points to a 'Board Actions' dropdown menu in the top right corner, which contains 'Create Board', 'Copy Board', and 'Add Module' options. Below this, an 'Add Module' modal is shown, listing available modules: 'Cyber Detect and Respond Portal' and 'Threat Advisories data by TLP's'. Each module has a checkbox and a small donut chart icon. The modal also includes a 'Filter Modules' dropdown set to 'All', a 'Create New' button, and 'Cancel' and 'Add to Dashboard' buttons.

© 2021 Deloitte - Cyber Detect and Respond Portal. All rights reserved. Privacy | Terms | Cookies | v3.22.9

# Dashboard view (cont'd)

The screenshot shows the 'Cyber Detect and Respond Portal' dashboard. It features a top navigation bar, a sidebar, and several data visualization widgets. Annotations with green arrows point to specific configuration elements:

- Top Right:** A callout box titled 'Edit Module' contains configuration options: 'Module Name' (with a dropdown menu), 'Threat Advisories by Threat Type', 'Module Type' (with a dropdown menu), and 'Dated By' (with a dropdown menu). A separate callout points to the 'Module Type' dropdown, stating 'Select between Threat Advisories or Vulnerabilities to display for each module'. The dropdown menu is open, showing 'Threat Advisory' (highlighted in blue) and 'Vulnerability'.
- Center:** A callout box titled 'Edit information reported by each module through configuring a wide array of data points' points to the 'Dated By' dropdown menu. The menu is open, showing 'Published' (highlighted in blue), 'Created', and 'Modified'. Another callout points to the 'Published' option, stating 'Select respective report / notification milestone for setting date-based reporting in module'.
- Bottom Right:** A callout box titled 'Select date or date range for reports / notifications to display in module' points to the 'Dated By' dropdown menu. The menu is open, showing 'Published' (highlighted in blue), 'Last Month', 'Last 2 Months', and 'Last 3 Months'.

The dashboard includes widgets for 'Recent Vulnerabilities' (3 items), 'Recent Threat Advisories' (3 items), and two pie charts. The first pie chart is titled 'Threat Advisories by Threat Type' and shows categories: campaign, incident, malware, threat-actor, and vulnerability. The second pie chart is titled 'Vulnerabil...' and shows categories: ADJACENT NETWORK, LOCAL, and M. A bar chart on the right shows values for 'MBER' (15) and 'GREEN'.

# Dashboard view (cont'd)

Welcome to **Cyber Detect and Respond Portal**

Dashboard +

Date Range: [Calendar Icon]

3 Recent Vulnerabilities

3 Recent Threat Advisories

Threat Advisories by Threat Ty ...

This Month

Global  
North America  
Latin America  
Europe  
Asia-Pacific  
South Asia  
Middle East / North Africa  
Russia / Central Asia  
Sub-Saharan Africa  
Australia / New Zealand  
Non-State

ADJACENT NETWORK LOCAL

campaign incident malware threat-actor vulnerability

**Edit Module**

Select Configurations

Module Name \*  
Threat Advisories by Threat Type

Module Type \*  
Threat Advisory

Dated By \*  
Published

Published \*  
Last Month

Tip  Does Not Equal  
Tip

Region Ids  Does Not Equal  
Region Ids

Industry Ids  Does Not Equal  
Industry Ids

Threat Type  Does Not Equal  
Threat Type

Cancel Save

Filter advisories reported by Traffic Light Protocol (TLP) designation

Filter advisories by (world) regions(s)

Filter advisories by industry(ies) / sector(s)

15

White  
Green  
Amber  
Red

Select All Deselect All

All  
Energy, Resources and Industrials  
Financial Services  
Consumer  
Government and Public Services  
Life Sciences & Health Care  
Technology, Media & Telecommunications

Terms | Cookies | v3.22.9

# Dashboard view (cont'd)

Welcome to **Cyber Detect and Respond Portal**

Dashboard +

Date Range: [Calendar Icon]

3 Recent Vulnerabilities

3 Recent Threat Advisories

Threat Advisories by Threat Type

Threat Type  Does Not Equal

Threat Type

Select All Deselect All

Malware

Vulnerability

Campaign

Threat Actor

Board Actions

Edit Delete

Filter by Threat type:

- Malware
- Vulnerability
- Campaign
- Threat Actor

Threat Advisories By TLPs

This Month

60

50

40

30

Count

48

Change chart type and data filtered by in module:

Advisory Type  Does Not Equal

Advisory Type

Select All Deselect All

Client Threat Notification

Threat Notification

Threat Report

Threat Study

● campaign ● incident ● malware

Filter by Advisory type:

- Threat Notification
- Threat Report
- Threat Study

Edit Module

Select Configurations

Industry Ids

Threat Type  Does Not Equal

Threat Type

Description

Latest updates and user notices about upcoming changes and events.

View Options

Show Graph

Bar Chart  Pie Chart  Line Chart

Show Records

Filter Results

- Created
- Modified
- Published
- Tip
- Region Ids
- Industry Ids
- Threat Type
- Advisory Type

Cancel Save

Preview

30

25

20

15

10

5

0

Count

9

26

25

9

19

campaign incident malware threat-actor vulnerability

**Note:** This page and the 2 preceding pages provide several examples of configuration options for Threat Advisory modules. While not specifically exhibited in this reference guide, there are similar configuration options for Vulnerabilities modules. Such options for Vulnerabilities modules include filtering on access vector (local, adjacent network, or network) and access complexity (high, medium, or low).

# Threat Advisories view

**Threat Advisories can be accessed from any page in the Portal from the side menu.**

**Multiple filtering options are available, including by:**

- Traffic Light Protocol (TLP)
- Industry
- Region
- Threat Type
- Advisory Type
- Date Range

Advisory Title	TLP 1:	Industry	Region	Threat Type	Advisory Type	Published
Conti ransomware threat group receives an injunction from High Court of Ireland to return stolen data	Green	Life Sciences & Health Care	Global	Incident	Threat Notification	May 21, 2021
STRRAT campaign masquerading as ransomware delivered through malicious PDF attachments	Green	All	Global	Campaign	Threat Notification	May 21, 2021
Colonial Pipeline and CNA Financial paid millions to hackers after ransomware attacks	Green	All	Global	Incident	Threat Notification	May 21, 2021
Ransomware threat actors attempt additional extortion tactics on their victims	Green	All	Global	Threat Actor	Threat Notification	May 21, 2021
Increased Targeting of Virtual Private Network Platforms	Green	All	Global	Campaign	Threat Report	May 20, 2021

# Threat Advisories view (cont'd)

**Threat Advisory (email) Notifications can be set by clicking this button.**

**Sort Threat Advisories by date published in ascending or descending order**

**Search bar enables focused searches for Threat Advisories containing specific keywords.**

**Click the 'i' icon for a 'Search Tips' popup window, which is shown to the left**

**Button for downloading a Threat Advisory**

**Button for viewing details of a Threat Advisory**

**Search Tips**

The single character wildcard search looks for terms that match that with the single character replaced. For example, to search for "127.0.0.1" or "example.com" you can use the search:

example.com

Multiple character wildcard searches looks for 0 or more characters. For example, to search for test, tests or tester, you can use the search:

example.\*

You can also use the wildcard searches for exact match .

"CVE-2015-4037"

Note: You cannot use a \* or ? symbol as the first character of a search.

Reference: [https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-simple-query-string-query.html#\\_simple\\_query\\_string\\_syntax](https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-simple-query-string-query.html#_simple_query_string_syntax)

TLP 1:	Industry:	Region:	Threat Type:	Advisory Type:	Published:
Green	Life Sciences & Health Care				May 21, 2021
Green	All				May 21, 2021
Green	All				May 21, 2021
Green	All				May 21, 2021
Green	All	Global	Campaign	Threat Report	May 20, 2021

# Threat Advisory in-depth

The screenshot shows a web interface for a Threat Advisory. At the top, there is a navigation bar with a search bar and a user profile. Below the navigation bar, the page title is "Threat Advisories". The main content area displays the details of a "Threat Profile: DarkSide Ransomware".

Key details include:

- TLP: Green<sup>1</sup>
- Serial: G-TR-EN-01-15827
- Threat Type: Threat Actor
- Advisory Type: Threat Report
- Published: May 19, 2021, 01:44 pm
- Industry: All
- Region: Global
- Tags: #DarkSide, #GEN-16-0001, #GEN-16-0003, #GEN-16-0004, #GEN-16-0007, #GEN-16-0008, #ransomware

The report content is organized into sections:

- MITRE ATT&CK: Tactics & Software
- Relevance
- Impacted Industry:
- Executive Summary
- Threat Analysis
  - Motivation
  - Sophistication:
  - Intended effect:
  - Introduction
  - Targeting
  - Tools observed in campaigns
  - Tactics, Techniques, and Procedures (TTPs)
- Recommendations
  - Deloitte CTI recommends the following for Security Engineering and IT Teams:
- Sources
- Related Deloitte publication(s)

Annotations on the screenshot include:

- A green box highlights the "Download Advisory" button in the top right corner, with an arrow pointing to it from a text box that says: "A Threat Advisory can be downloaded as a .pdf report contained within a .zip file by clicking on this button."
- Two green boxes highlight the "MITRE ATT&CK: Tactics & Software" and "Threat Analysis" sections, with arrows pointing to a text box that says: "These sections are included in Threat Reports only."
- A green box highlights the "Threat Analysis" section, with an arrow pointing to a text box that says: "The structure and content of the 'Threat Analysis' section of a Threat Report depends upon the 'Threat Type' of the report:" followed by a list of threat types: Malware, Vulnerability, Campaign, Threat Actor, and Incident.

# Threat Advisory in-depth (cont'd)

**Applicable MITRE ATT&CK Tactics, Techniques, and Descriptions of Techniques are also included in all Threat Reports.**

Threat Advisories

Threat Profile: DarkSide Ransomware

TLP: Green<sup>1</sup> Serial: G-TR-EN-01-15827 Threat Type: Three  
Industry: All Region: Global  
Tags: #DarkSide #GEN-16-0001 #GEN-16-0003 #GEN-16-0004 #GEN-16-0007 #GEN-16-0008 #ransomware

Published: May 19, 2021, 01:44 pm

Back Have a question about this report? Download Advisory

**Click this button to draft a Threat Advisory-specific email to submit relevant questions to the following, CTI analyst-monitored address: [detectandrespondportal@deloitte.com](mailto:detectandrespondportal@deloitte.com).**

Tactic	Technique	Description
Initial Access		
Execution		
Persistence		
Privilege Escalation		
Defense Evasion		
Credential Access		
Discovery		
Lateral Movement		
Collection		
Command and Control		
Exfiltration		
Impact		
Software		

MITRE ATT&CK: Enterprise Techniques & Software

Threat Advisory 'Threat Profile: DarkSide Ransomware' (G-TR-EN-01-15827) - Message (HTML)

File Message Insert Draw Options Format Text Review Help Acrobat Tell me what you want to do

Clipboard Basic Text Names Include Tags Voice Sensitivity My Templates

To: [detectandrespondportal@deloitte.com](mailto:detectandrespondportal@deloitte.com)

Cc:

Bcc:

Subject: Threat Advisory 'Threat Profile: DarkSide Ransomware' (G-TR-EN-01-15827)

I have the following question about the above article on the Deloitte Cyber Detect and Respond Portal

# Adding Threat Advisory Notifications

**Click this button to add a Threat Advisory Notification.**

Back Add Notification

Notification Frequency: Weekly

Advisory Type: All Advisories Notification Details: Friday 9:00 AM EST User: Is Active: Active Modified: May 21, 2021

**“Frequency” options include:**

- As Soon as Possible
- Daily
- Weekly

A “Notify Time” option is required when “Daily” or “Weekly” is selected, and a “Notify Day” is also required when “Weekly” is selected.

Enter specific text (e.g., “ransomware,” “phishing,” “microsoft”) for “Query” to filter Threat Advisory Notifications.

**“Advisory Types” options include:**

- All Advisory Types
- Threat Notification
- Threat Report
- Threat Study

Threat Advisory Notifications

Add Threat Advisory Notifications

Frequency \*  
Select Frequency

Advisory Types  
All Advisory Types

Query  
Enter ...

Filtered Deloitte publication(s)

Is Active

Cancel Create

© 2021 Deloitte - Cyber Detect and Respond Portal. All rights reserved. Privacy | Terms | Cookies | v3.22.9

# Editing Threat Advisory Notifications

**Click this button to edit a Threat Advisory Notification.**

**Click this button to delete a Threat Advisory Notification.**

**Modify "Frequency," "Notify Day," "Notify Time," "Advisory Types," and/or "Query" text when editing Threat Advisory Notifications**

Threat Advisory Notifications

All Threat Advisory Notifications

Notification Frequency: Weekly

Advisory Type: All Advisories

Notification Details: Friday 9:00 AM EST

**Edit Threat Advisory Notifications**

Frequency \*  
Weekly

Notify Day  
Monday

Notify Time  
09:00 am

In  
New York (America)

Advisory Types  
All Advisory Types

Query \*  
Enter ...

Filtered Deloitte publication(s)

Is Active

Cancel Submit

© 2021 Deloitte - Cyber Detect and Respond Portal. All rights reserved.

Privacy | Terms | Cookies | v3.22.9

# Vulnerabilities view

Vulnerabilities can be accessed from any page in the Portal from the side menu.

Multiple Vulnerabilities filtering options are available, including by:

- Access Vector
  - ✓ Network
  - ✓ Adjacent Network
  - ✓ Local
- Access Complexity
  - ✓ High
  - ✓ Medium
  - ✓ Low

All Vulnerabilities

Select Filters

Access Vector Access Complexity

Arrange By Ascending

CVE ID	CVSS	Access Vector	Access Complexity	Published
CVE-2021-1559	NYA	NYA	NYA	May 22, 2021
CVE-2021-1557	NYA	NYA	NYA	May 22, 2021
CVE-2021-1553	NYA	NYA	NYA	May 22, 2021
CVE-2021-1548	NYA	NYA	NYA	May 22, 2021
CVE-2021-1547	NYA	NYA	NYA	May 22, 2021

Multiple Vulnerabilities filtering options are available, including by:

- Access Vector
  - ✓ Network
  - ✓ Adjacent Network
  - ✓ Local
- Access Complexity
  - ✓ High
  - ✓ Medium
  - ✓ Low

Search

Welcome

Vulnerabilities Notifications

Hide Filters

Clear Filters

Search

CVE ID	CVSS	Access Vector	Access Complexity	Published
CVE-2021-1559	NYA	NYA	NYA	May 22, 2021
CVE-2021-1557	NYA	NYA	NYA	May 22, 2021
CVE-2021-1553	NYA	NYA	NYA	May 22, 2021
CVE-2021-1548	NYA	NYA	NYA	May 22, 2021
CVE-2021-1547	NYA	NYA	NYA	May 22, 2021

# Vulnerabilities view (cont'd)

**Sort Vulnerabilities by Common Vulnerabilities and Exposures (CVE) identification number (<https://cve.mitre.org/>), Common Vulnerability Scoring System (CVSS) Base score (<https://www.first.org/cvss/>), or by date published in ascending or descending order**

**Button for viewing details of a Vulnerability**

CVE ID	CVSS	Access Vector	Access Complexity	Published
CVE-2021-1559	NYA	NYA	NYA	May 22, 2021
CVE-2021-1557	NYA	NYA	NYA	May 22, 2021
CVE-2021-1553	NYA	NYA	NYA	May 22, 2021
CVE-2021-1548	NYA	NYA	NYA	May 22, 2021
CVE-2021-1547	NYA	NYA	NYA	May 22, 2021

# Adding Vulnerability Notifications

**Click this button to add a Vulnerability Notification.**

**The "Name" entered will appear at the top of Vulnerability Notification emails for rapid identification of associated vulnerabilities.**

**Enter specific text (e.g., "google," "microsoft," "remote execution") for "Query" to filter Vulnerability Notifications.**

**A number entered here will filter Vulnerability Notifications according to a minimum Common Vulnerability Scoring System (CVSS) Base score (<https://www.first.org/cvss/>).**

**© 2021 Deloitte - Cyber Detect and Respond Portal. All rights reserved.**

**Privacy | Terms | Cookies | v3.22.9**

# Editing Vulnerability Notifications

**Click this button to edit a Vulnerability Notification.**

**Click this button to delete a Vulnerability Notification.**

**Modify "Name," minimum CVSS Base score, and/or "Query" text when editing Vulnerability Notifications**

**Vulnerabilities Notifications**

**Edit Vulnerabilities Notification**

Name \*  
Microsoft CVSS 5.0+ Vulnerabilities from Deloitte Portal  
This title will appear in your email notifications to allow quick identification of vulnerabilities.

User \*  
▼

Enter CVSS Base (a number between 0 and 10) or leave blank to query all records\*  
5

Query\*  
Microsoft

Is Active

Cancel Update

© 2021 Deloitte - Cyber Detect and Respond Portal. All rights reserved. Privacy | Terms | Cookies | v3.22.9

# Account Settings view

Welcome to **Cyber Detect and Respond Portal**

Dashboard +

Date Range: [Calendar icon]

3 Recent Vulnerabilities

3 Recent Threat Advisories

© 2021 Deloitte - Cyber Detect and Respond Portal. All rights reserved. [Privacy](#) | [Terms](#) | [Cookies](#) | v3.22.9

Welcome [User Profile]

- Settings
- User Profiles
- Sign out

The "Profile Information" options depicted here are available by clicking on the user's "Settings" link at the top of any Portal page.

**Deloitte.**

Dashboard

Threat Advisories

Vulnerabilities

Support

Logout

Users

Profile Information

First Name:	Last Name:	Company:	Username:	Last Logged: May 26 2021, 08:31 AM
-------------	------------	----------	-----------	---------------------------------------

© 2021 Deloitte - Cyber Detect and Respond Portal. All rights reserved. [Privacy](#) | [Terms](#) | [Cookies](#) | v3.22.9

Edit [Pencil icon]

A user's "Profile Information", which can be edited as needed

# Account Settings view (cont'd)

**Deloitte.**

- Dashboard
- Threat Advisories
- Vulnerabilities
- Support
- Logout

Search

Welcome

### Edit Profile

Back

#### Profile Information

First Name

Last Name \*

Username \*

Email Address

PGP Public Key \*

-----BEGIN PGP PUBLIC KEY BLOCK-----

Cancel Submit

A user can edit any of his/her "Profile Information" displayed above.

© 2021 Deloitte - Cyber Detect and Respond Portal. All rights reserved. [Privacy](#) | [Terms](#) | [Cookies](#) | v3.22.9

# Bi-weekly Deloitte Cyber Threat Briefings

- All Portal users are also invited to attend Bi-weekly Deloitte Cyber Threat Briefings. These 1-hour webcasts provide timely and relevant information on current and high-risk cyber threats, such as attack campaigns, hacker group tactics & techniques, new ransomware strains, etc.
- Each calendar invite received is specific to a particular bi-weekly webcast *and* Portal user and is generally sent 2 days prior to the event. You will need to click on the “Click Here to Join” link (noted in the graphic at below left). You may click on this URL directly in the email invite prior to accepting it, or any time thereafter within the calendar hold itself upon accepting the meeting invite and prior to the webcast.
- After clicking on the “Click Here to Join” link, you will be directed to the bi-weekly webcast registration webpage. In order to attend each webcast, **you must first register for the event** by completing the information on the left-hand side of the webpage and then clicking on the “Submit” button, as shown in the graphic at below right (see number “1”).
- Only after you first register for the webcast, will you be able to later join the event by entering your email address, **which must be the same email address associated with your Portal account and the same email address used for webcast registration**, in the field on the right-hand side of the same webpage and then clicking the “Log In” button (see number “2”).

## Deloitte Cyber Threat Briefing

Please join us for our next bi-weekly intelligence briefing

Dear Intel Community Member,

Thank YOU for being a part of our Cyber Detect and Respond Portal community!

To facilitate sharing of threat information and increase awareness, our next bi-weekly intelligence briefing (Thursday, ) will include:

- Recap our recent threat research, including trends and insights
- Facilitate a question & answer session with our threat analysts

This briefing is by **invitation only** and will be hosted webinars, so that you can **join and interact with our analyst team anonymously**. Your identifiable information will NOT be visible to attendees – including your name, company name, and email address.

We are looking forward to your attendance and participation in this briefing!

Regards,

Deloitte Cyber - Detect and Respond Portal Team

### Webcast link

Join from a PC, Mac, iPad, iPhone or Android device:

[Click Here to Join](#) - Please register in advance

Note: This link should not be shared with others; it is unique to you

Deloitte.

MARKING AN IMPACT THAT MATTERS

Deloitte's Cyber Detect and Respond Portal Web Briefing

Thu, EDT

Complete this form to enter the webcast. (\* indicates required field)

First Name:

Last Name:

Email\*:

City:

Submit

FAQs and System Test

Already registered for an event in this series? Log In Now

Email:

Log In

# Deloitte Cyber Detect and Respond Portal Terms of Use & Deloitte Privacy Statement

## Terms of Use

These Terms of Use apply to your use of the website that links to this Terms of Use document (the "Website"). To the extent there is an executed agreement with Deloitte & Touche LLP ("we" or "us") governing your licensed use of any technology, or your access to any membership or subscription offering, available on this Website (an "Agreement"), your use and access to any such technology or offering will be further governed by such Agreement. To the extent there is a conflict between these Terms of Use and an Agreement, the terms of the Agreement shall control. By using this Website, you are agreeing to these Terms of Use. If you do not agree to these Terms of Use, then you are not allowed to use this Website and should immediately terminate such usage.

### Use of Content; Restrictions

Unless otherwise indicated in the relevant content, and on the condition that you comply with all of your obligations under these Terms of Use, (i) you are authorized only to view and print the content on this Website for informational, noncommercial purposes and provided that any copy of the content that you make must include the copyright notice or other attribution associated with the content; and (ii) you are not authorized to copy or use any software, proprietary processes or technology embodied or described in this Website.

You will comply with all applicable laws in accessing and using this Website. You acknowledge that we may use your personal information and data according to our Privacy Statement, set forth in the Privacy link on this Website.

This Website and its contents are protected by copyright, trademark, and other laws of the United States and/or other countries. We and our licensors reserve all rights not expressly granted in these Terms of Use. References to other parties' trademarks on this Website are for identification purposes only and do not indicate that such parties have approved this Website or any of its contents, nor should they be construed as an endorsement of them or their content by us.

You will need a username and password (a "User Account") to access the Website. You are responsible for anything that happens through your User Account, unless and until you request deactivation in accordance with this Agreement. Without limiting the foregoing, you agree to the following:

- At any given time, you will create and maintain only one User Account for yourself. You cannot have multiple User Accounts for your use of the Website. Your User Account will be for you alone, and you cannot share or transfer it to anyone else.
- You shall keep your User Account password secure and confidential.
- You shall not remove any copyright, trademark, or other proprietary rights notices found on the Website or any of its content ("Content"), including any Content from us, another Deloitte Network entity, or a third party.
- You shall not engage in any action that directly or indirectly interferes with the proper working of, or places an unreasonable load on, our or service provider's infrastructure, including spamming or the distribution of computer viruses or other malicious code.
- You shall promptly notify us upon becoming aware of any unauthorized use of your User Account or any other breach of this Agreement.

### Disclaimers and Limitations of Liability

THIS WEBSITE CONTAINS GENERAL INFORMATION ONLY, AND WE ARE NOT, BY MEANS OF THIS WEBSITE, RENDERING PROFESSIONAL ADVICE OR SERVICES. BEFORE MAKING ANY DECISION OR TAKING ANY ACTION THAT MIGHT AFFECT YOUR FINANCES OR BUSINESS, YOU SHOULD CONSULT A QUALIFIED PROFESSIONAL ADVISOR.

THIS WEBSITE IS PROVIDED AS IS, AND WE MAKE NO EXPRESS OR IMPLIED REPRESENTATIONS OR WARRANTIES REGARDING IT. WITHOUT LIMITING THE FOREGOING, WE DO NOT WARRANT THAT THIS WEBSITE WILL BE SECURE, ERROR-FREE, FREE FROM VIRUSES OR MALICIOUS CODE, OR WILL MEET ANY PARTICULAR CRITERIA OF PERFORMANCE OR QUALITY. WE EXPRESSLY DISCLAIM ALL IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, COMPATIBILITY, SECURITY, AND ACCURACY.

YOUR USE OF THIS WEBSITE IS AT YOUR OWN RISK AND YOU ASSUME FULL RESPONSIBILITY AND RISK OF LOSS RESULTING FROM YOUR USAGE, INCLUDING, WITHOUT LIMITATION, WITH RESPECT TO LOSS OF SERVICE OR DATA. WE WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES OR ANY OTHER DAMAGES WHATSOEVER, RELATING TO OR ARISING OUT OF THE USE OF THIS WEBSITE, EVEN IF WE KNEW, OR SHOULD HAVE KNOWN, OF THE POSSIBILITY OF SUCH DAMAGES.

THE ABOVE DISCLAIMERS AND LIMITATIONS OF LIABILITY ARE APPLICABLE TO THE FULLEST EXTENT PERMITTED BY LAW, WHETHER IN CONTRACT, STATUTE, TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE) OR OTHERWISE.

## Additional Terms

If any portion of these Terms of Use is invalid or unenforceable in any jurisdiction, then (i) in that jurisdiction it shall be re-construed to the maximum effect permitted by law in order to effect its intent as nearly as possible, and the remainder of these Terms of Use shall remain in full force and effect, and (ii) in every other jurisdiction, all of these Terms of Use shall remain in full force and effect.

We may revise these Terms of Use at any time in our sole discretion by posting such revised Terms of Use at the Terms of Use link or elsewhere in this Website. Such revisions shall be effective as to you upon posting, unless explicitly stated by us. It is your responsibility to be aware of any such revised Terms of Use by checking this webpage. Your continued use of this Website following changes to these Terms of Use constitutes your agreement to the revised Terms of Use.

*Last Updated on: June 05, 2020*

URL to Deloitte's 'Privacy Statement' referenced in the TOU: <https://www2.deloitte.com/global/en/legal/privacy.html>

URL to Deloitte's 'Cookie Notice' referenced in the TOU: <https://www2.deloitte.com/global/en/legal/cookies.html>

**Note: Portal TOU and Deloitte 'Privacy Statement' & 'Cookie Notice' can be accessed via links at the bottom of any Portal webpage**

[Privacy](#) | [Terms](#) | [Cookies](#) | v3.22.10



Official Professional Services Sponsor

Professional Services means audit, tax, consulting, and advisory.

**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of DTTL and its member firms. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.