Deloitte.

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

October 2021

Version 2.1

Deloitte.

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

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?")*

TECHNIQUES *(The "how?" & the "what?")*

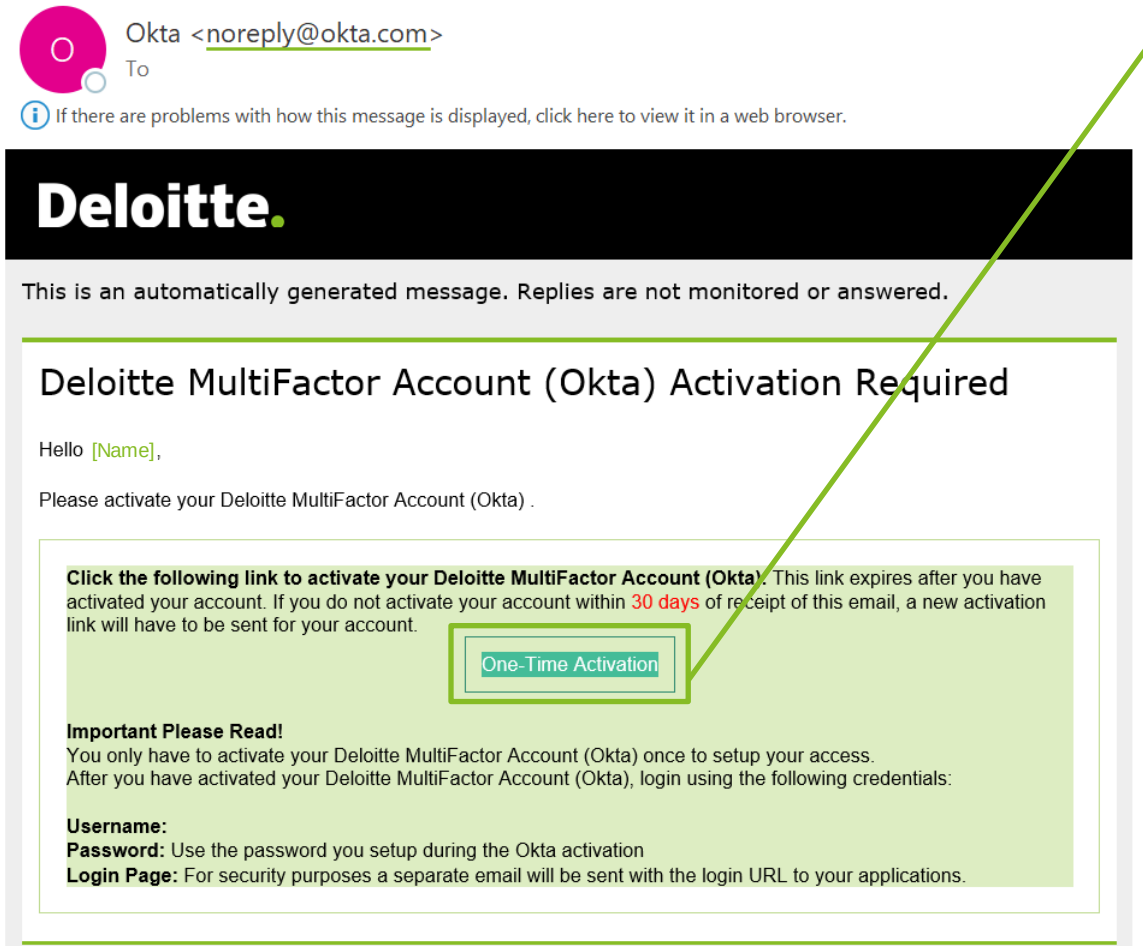
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Brute Force	PowerShell	External Remote Services	Bypass User Account Control	Bypass User Account Control	Brute Force	Local Network Discovery	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				

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. *(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 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.



Okta <noreply@okta.com>
To

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: D. Cyber Detect and Respond Portal.
6. Choose between setting up the MFA using:
   a. Okta Verify (native phone app)
   b. SMS Authentication

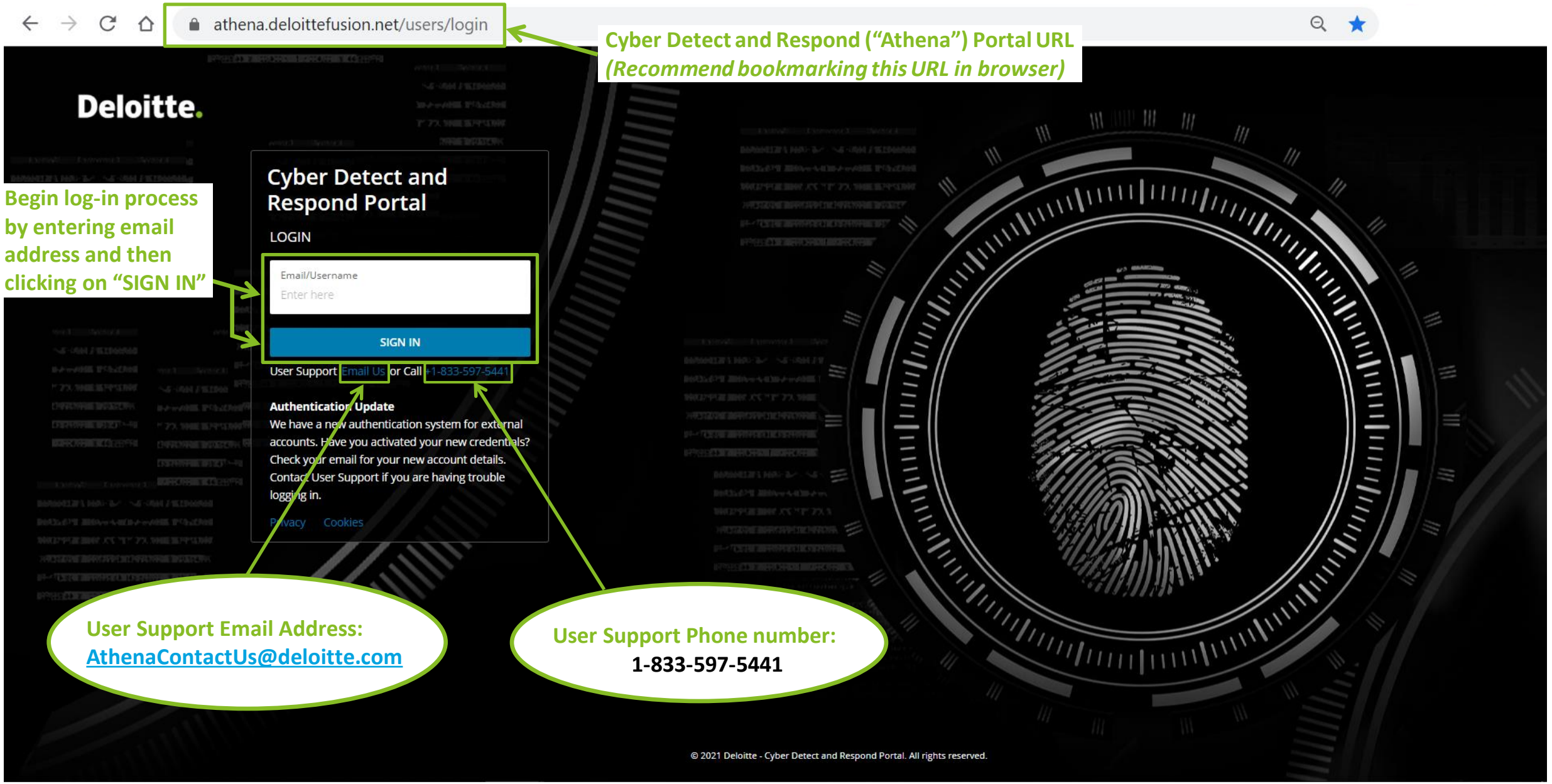
Okta Verify - Setup

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.

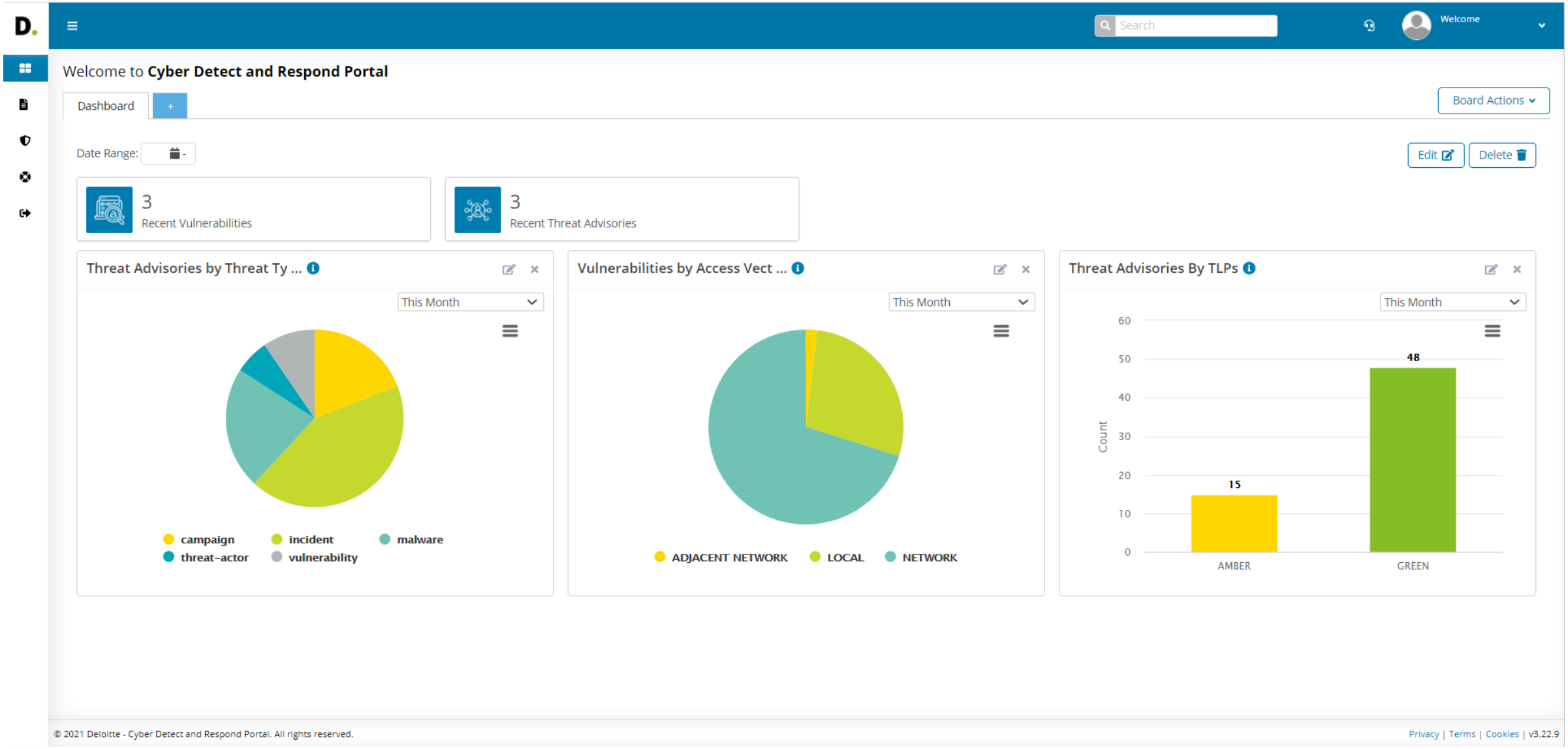
Okta SMS Authentication - Setup

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.

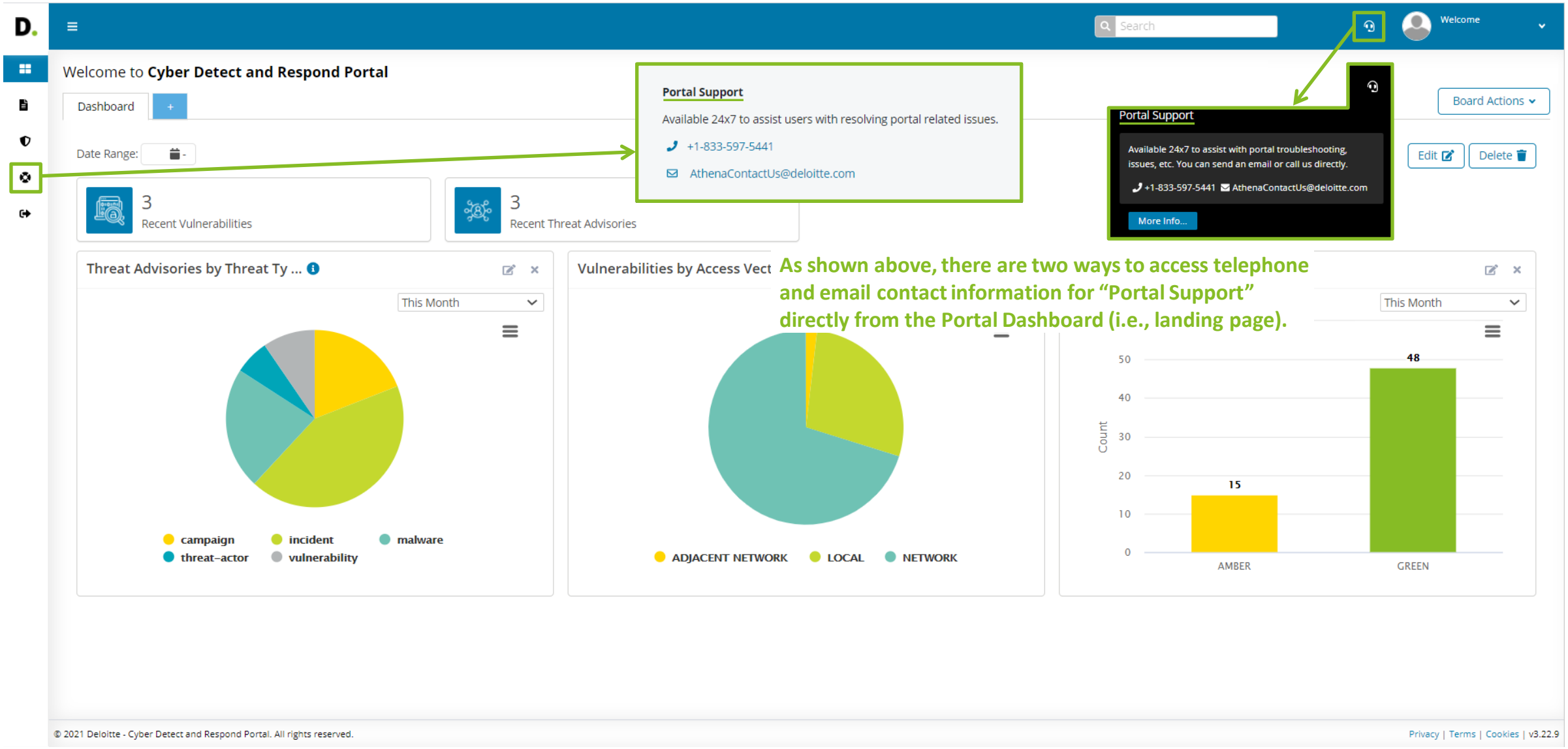
Accessing Cyber Detect & Respond Portal



Dashboard view

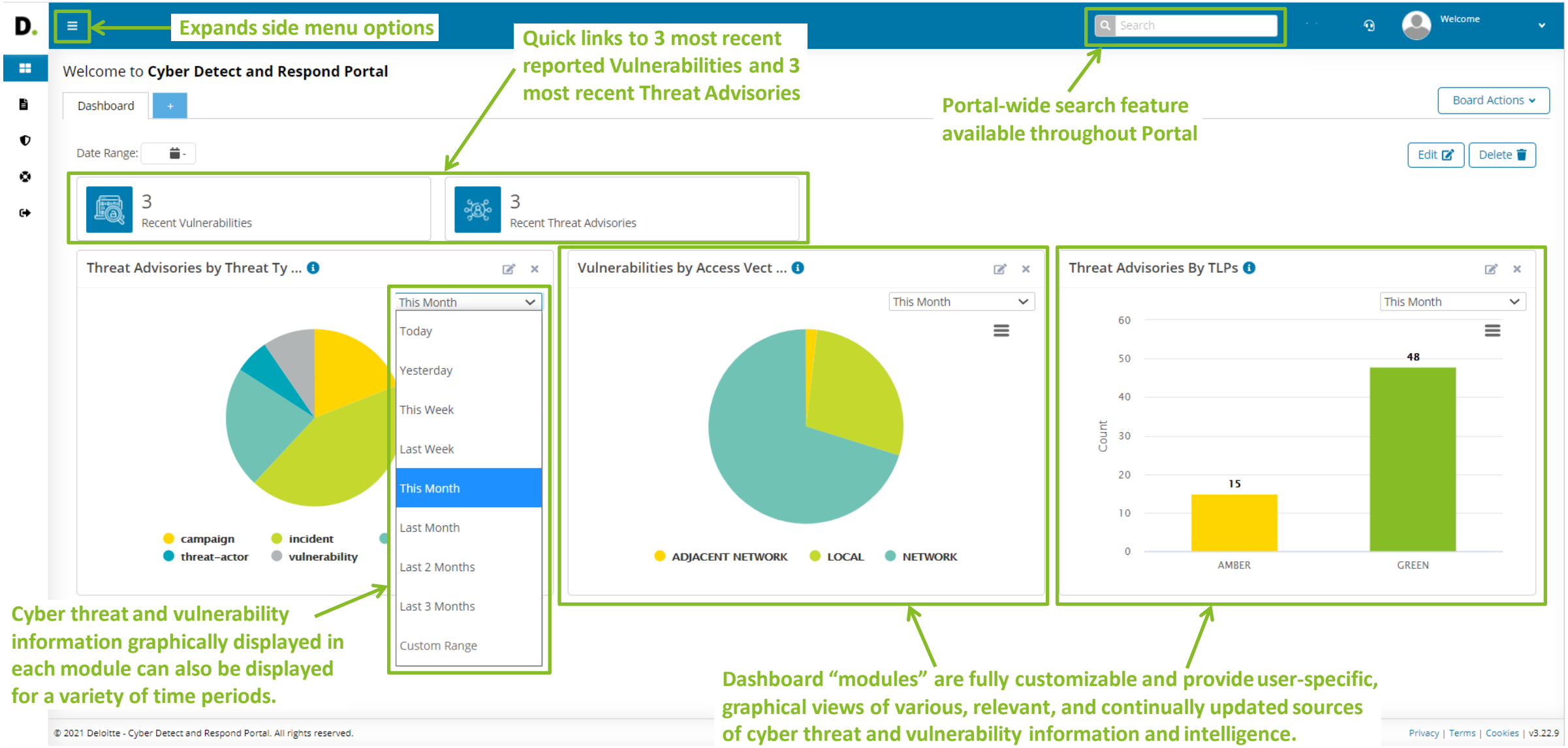


Dashboard view (cont'd)

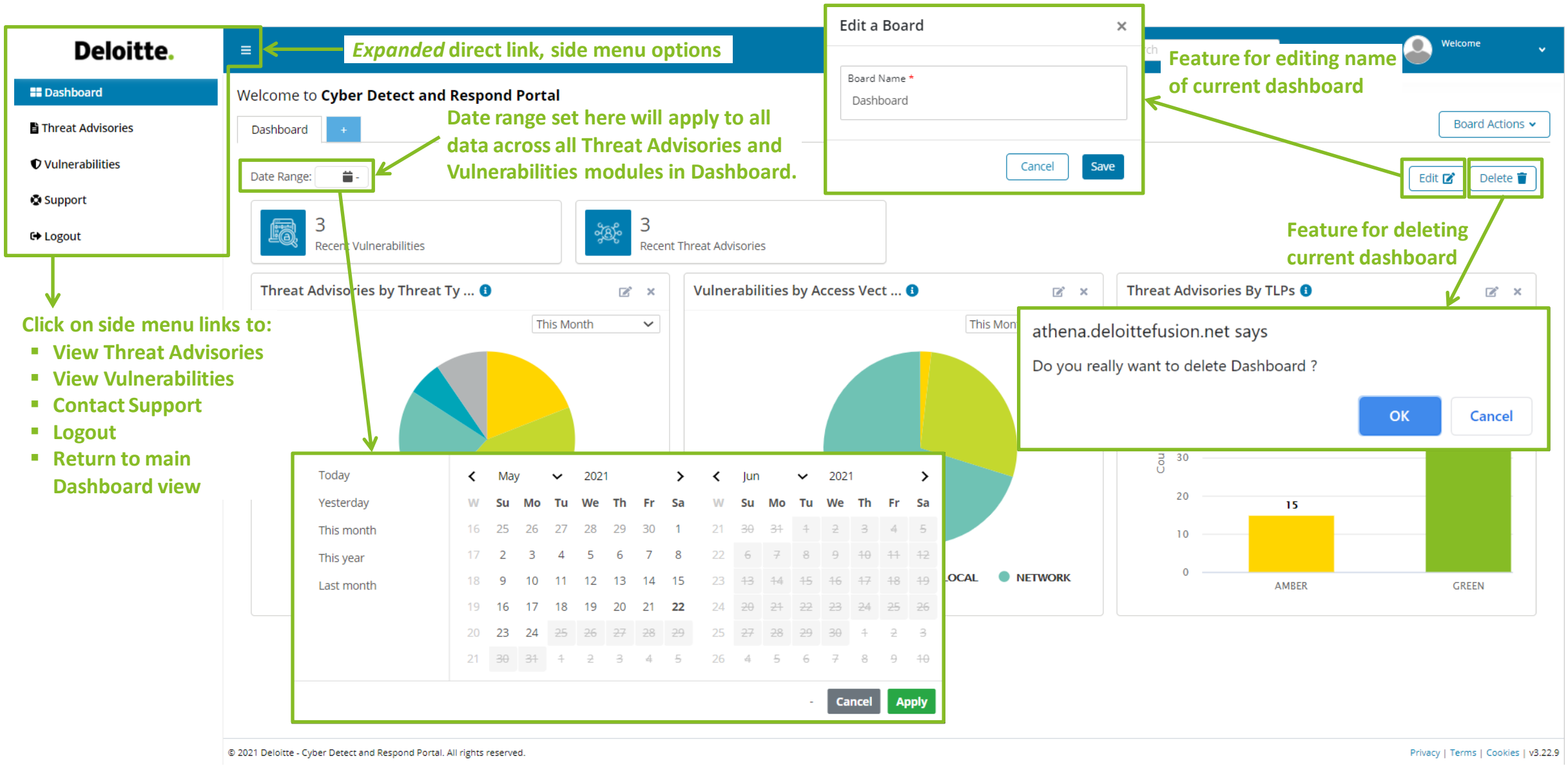


As shown above, there are two ways to access telephone and email contact information for "Portal Support" directly from the Portal Dashboard (i.e., landing page).

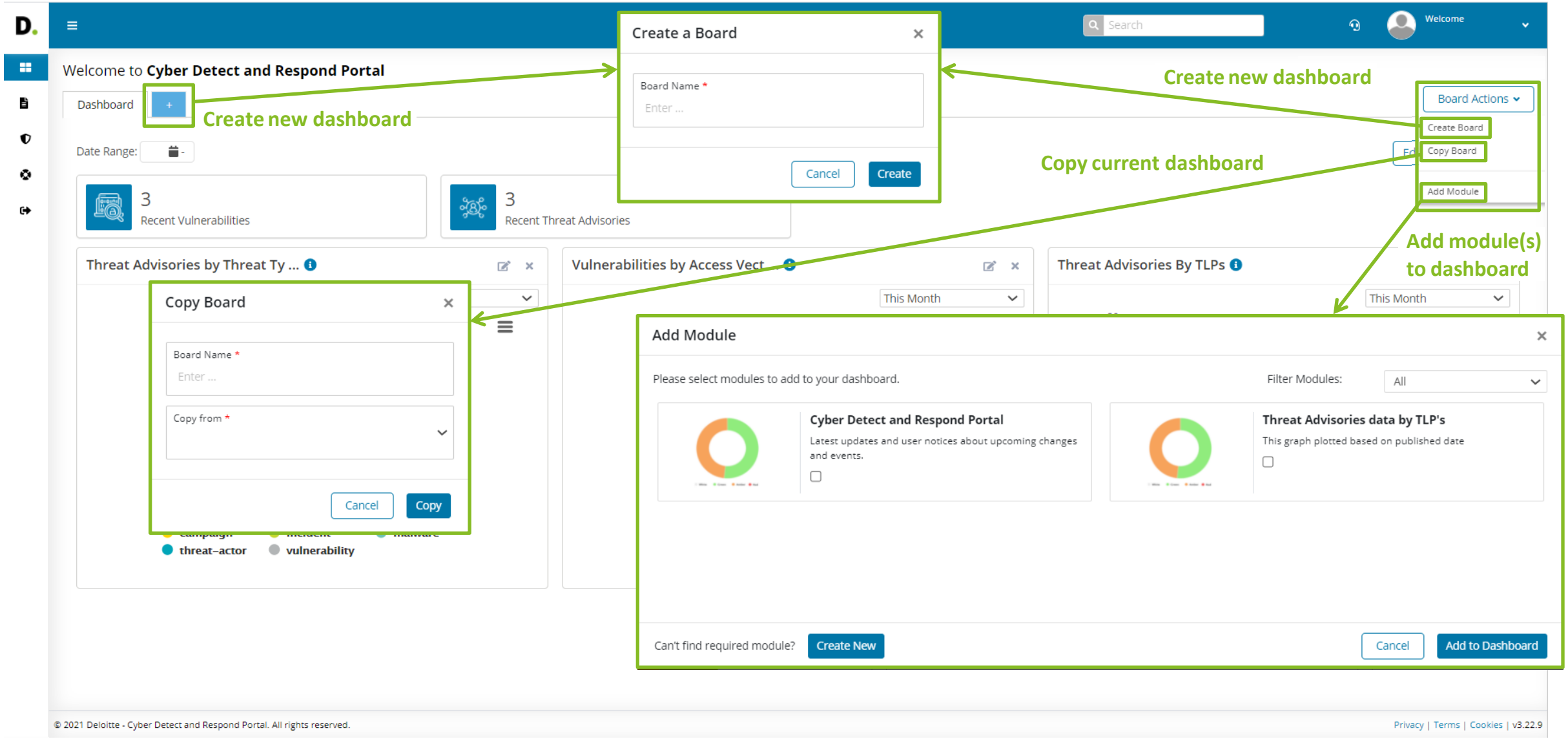
Dashboard view (cont'd)



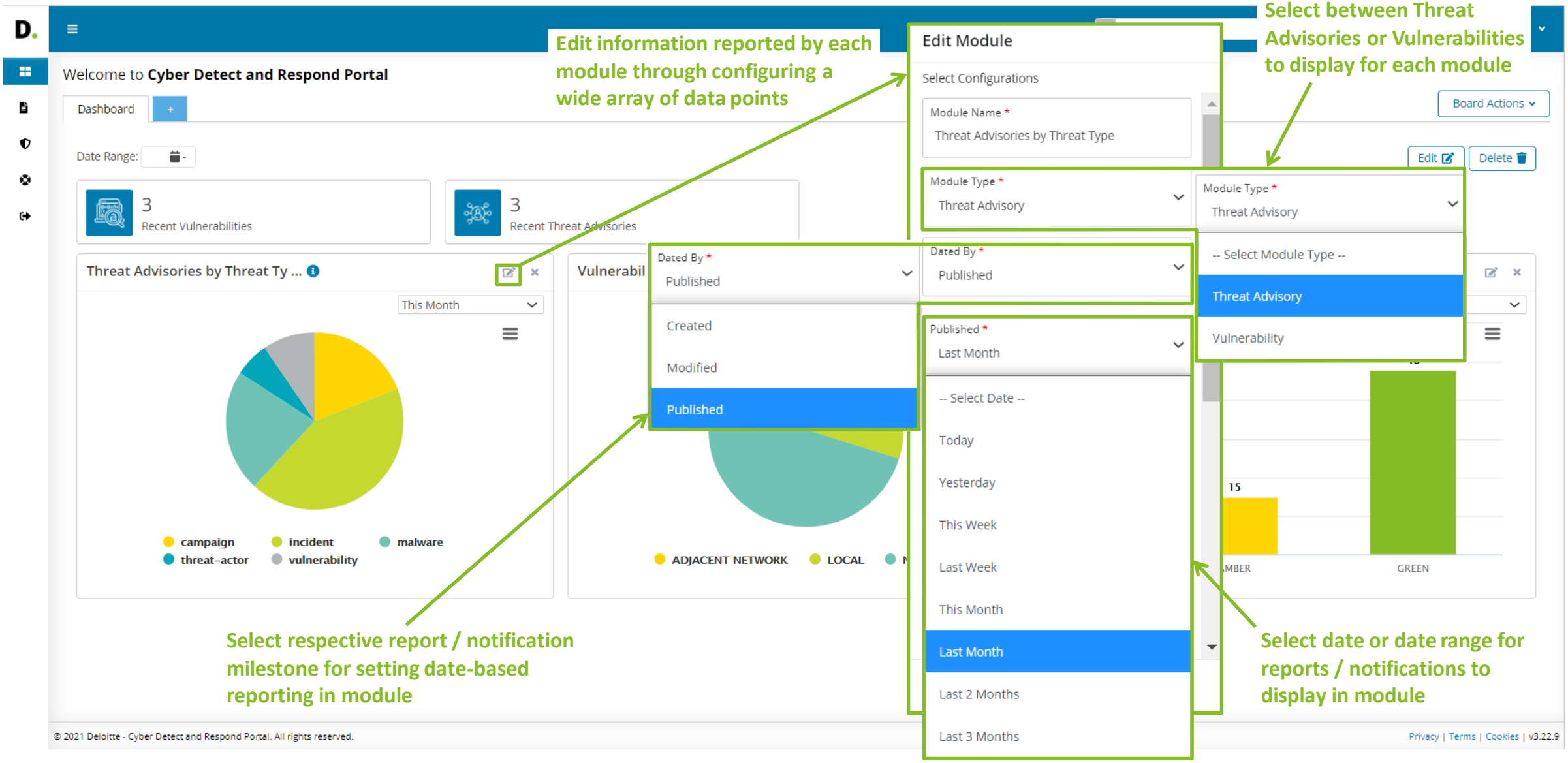
Dashboard view (cont'd)



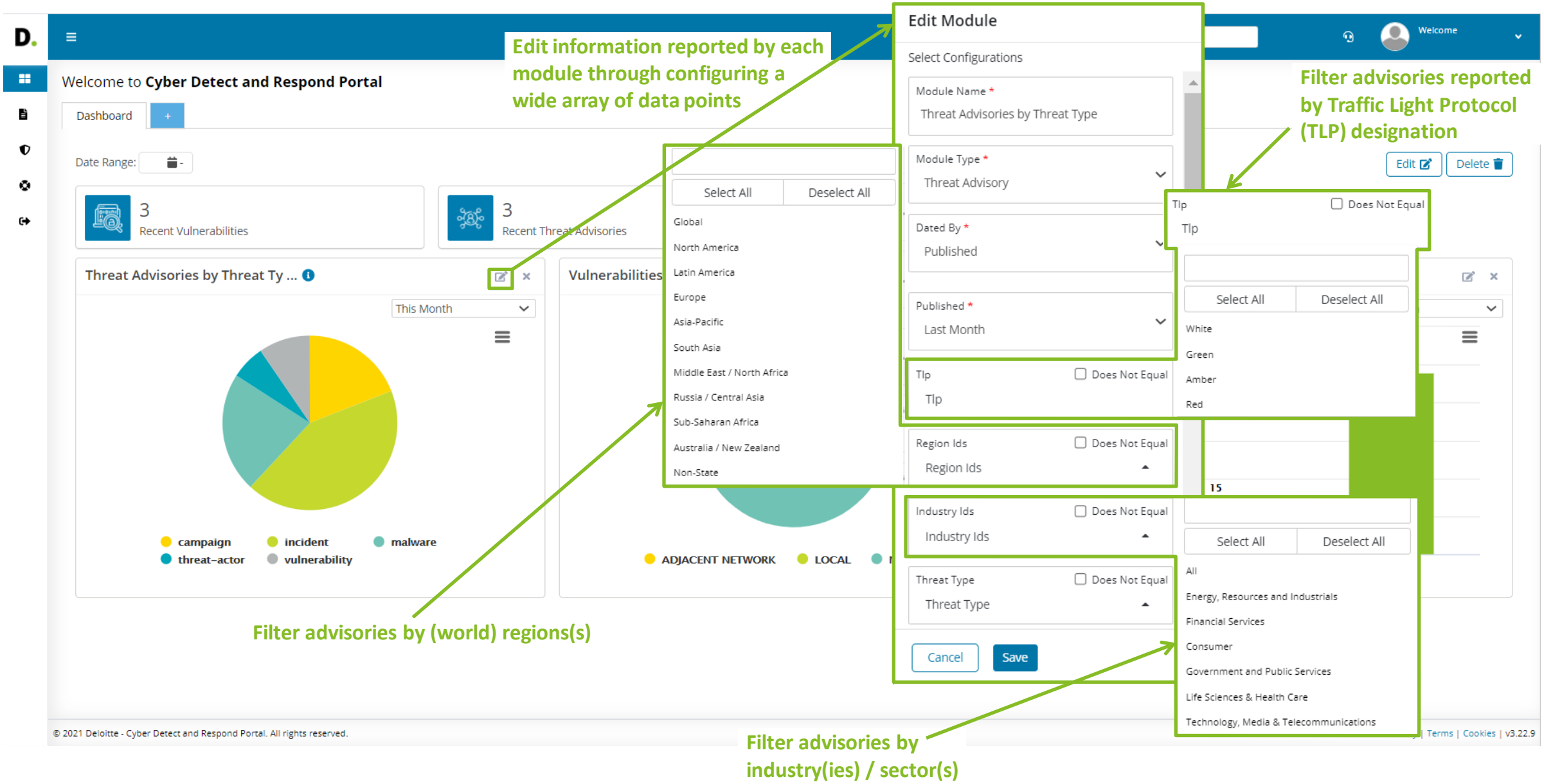
Dashboard view (cont'd)



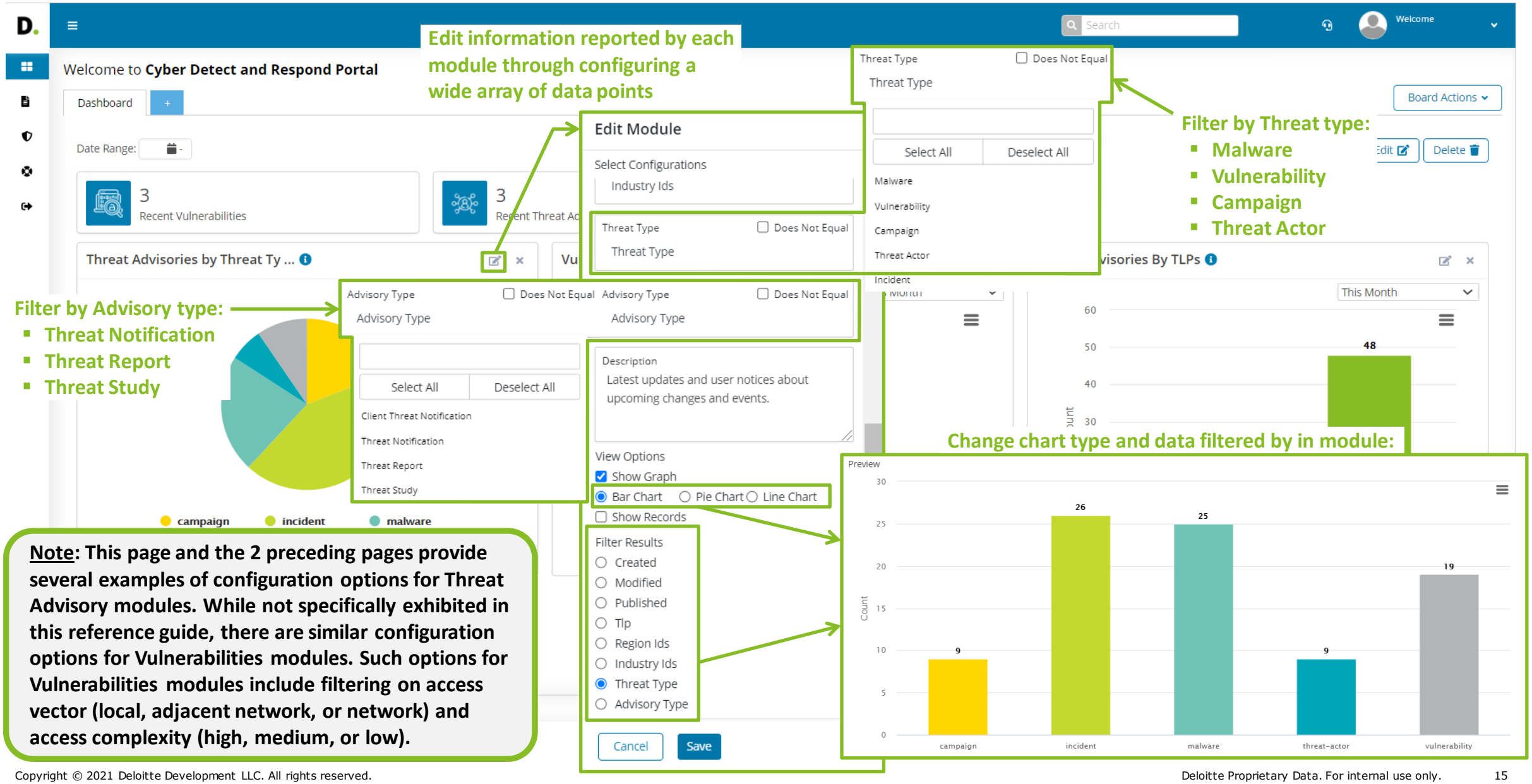
Dashboard view (cont'd)



Dashboard view (cont'd)

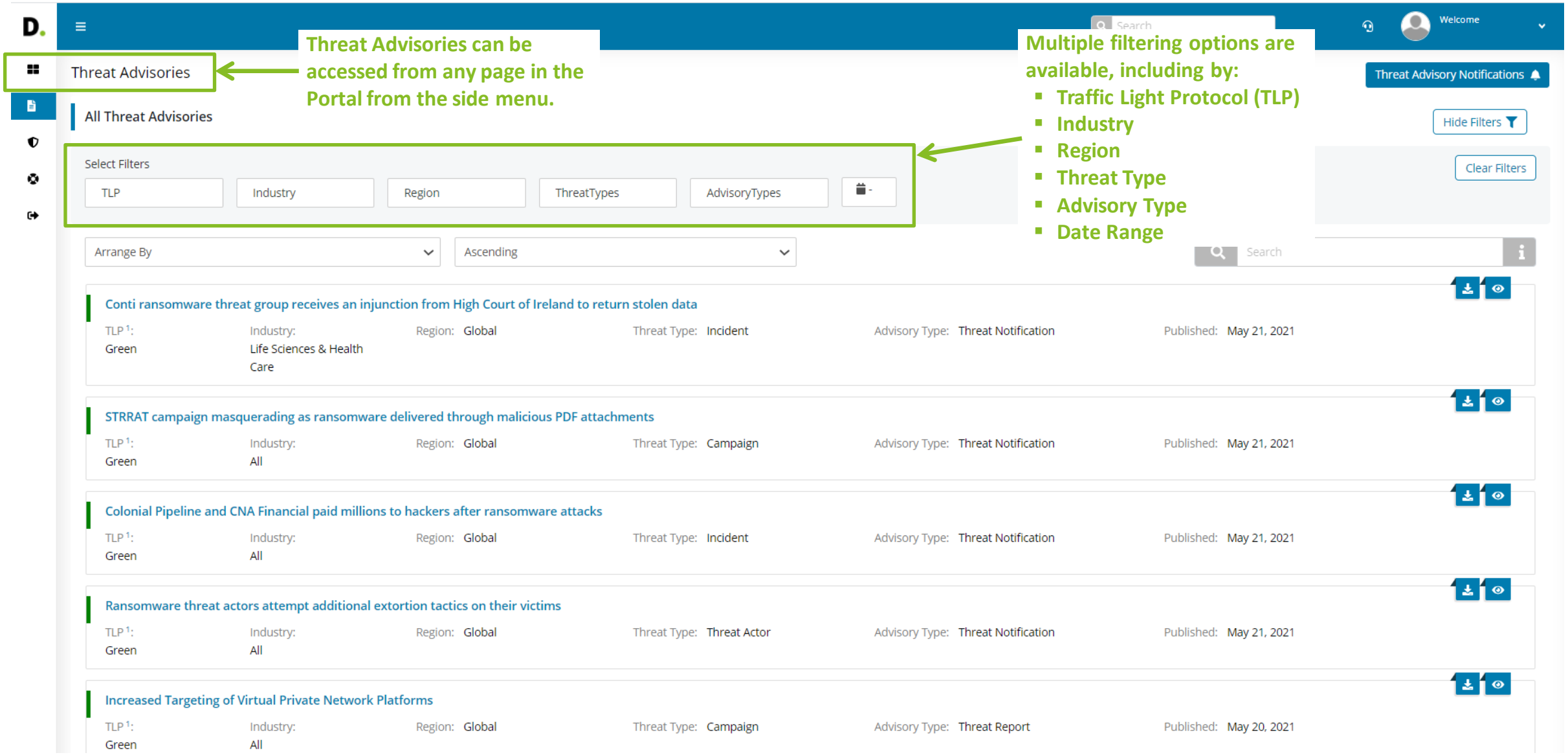


Dashboard view (cont'd)

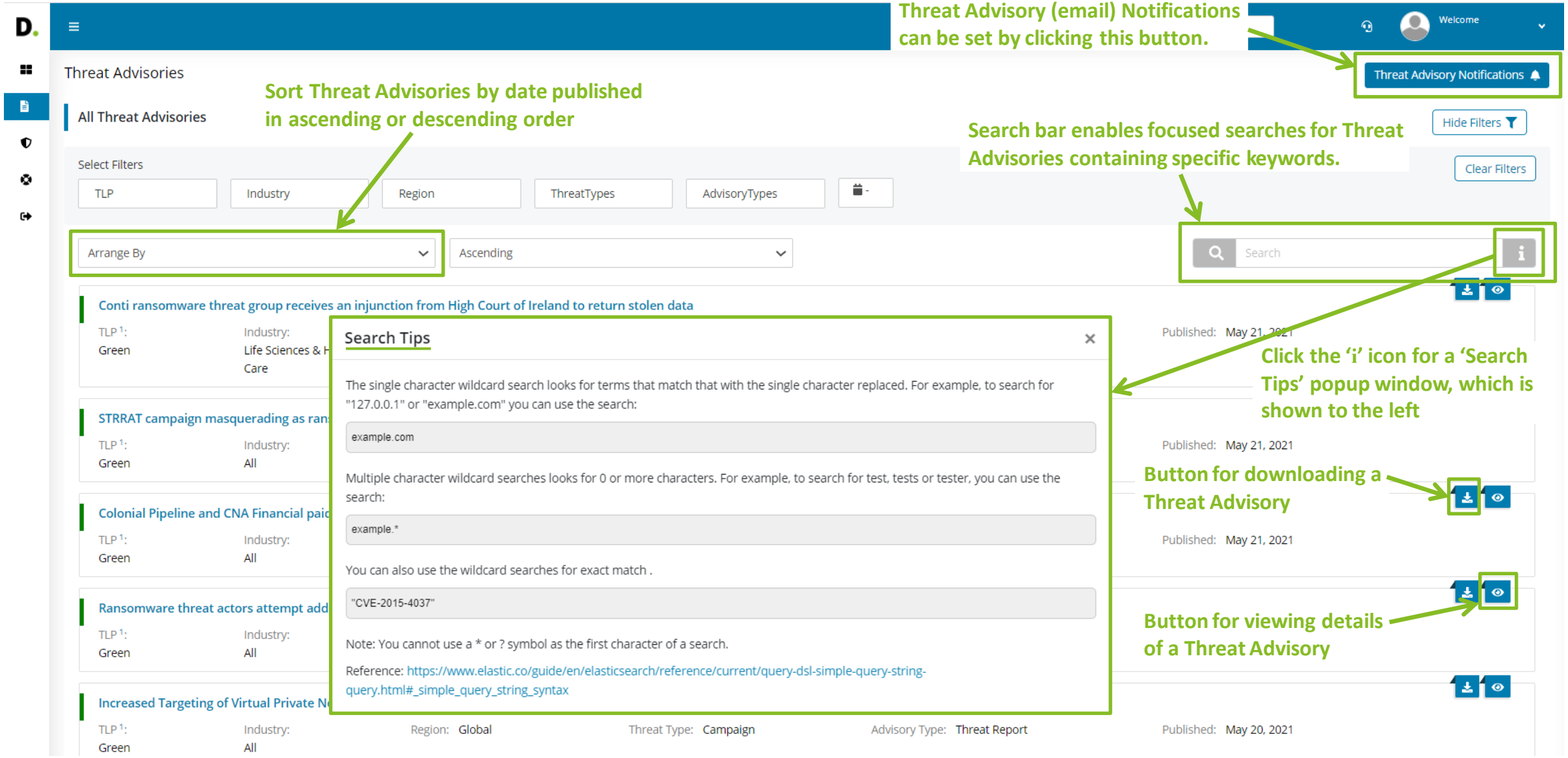


Note: This page and the 2 preceding pages provide several examples of configuration options for Threat Advisory modules. While not specifically exhibited in this reference guide, there are similar configuration options for Vulnerabilities modules. Such options for Vulnerabilities modules include filtering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

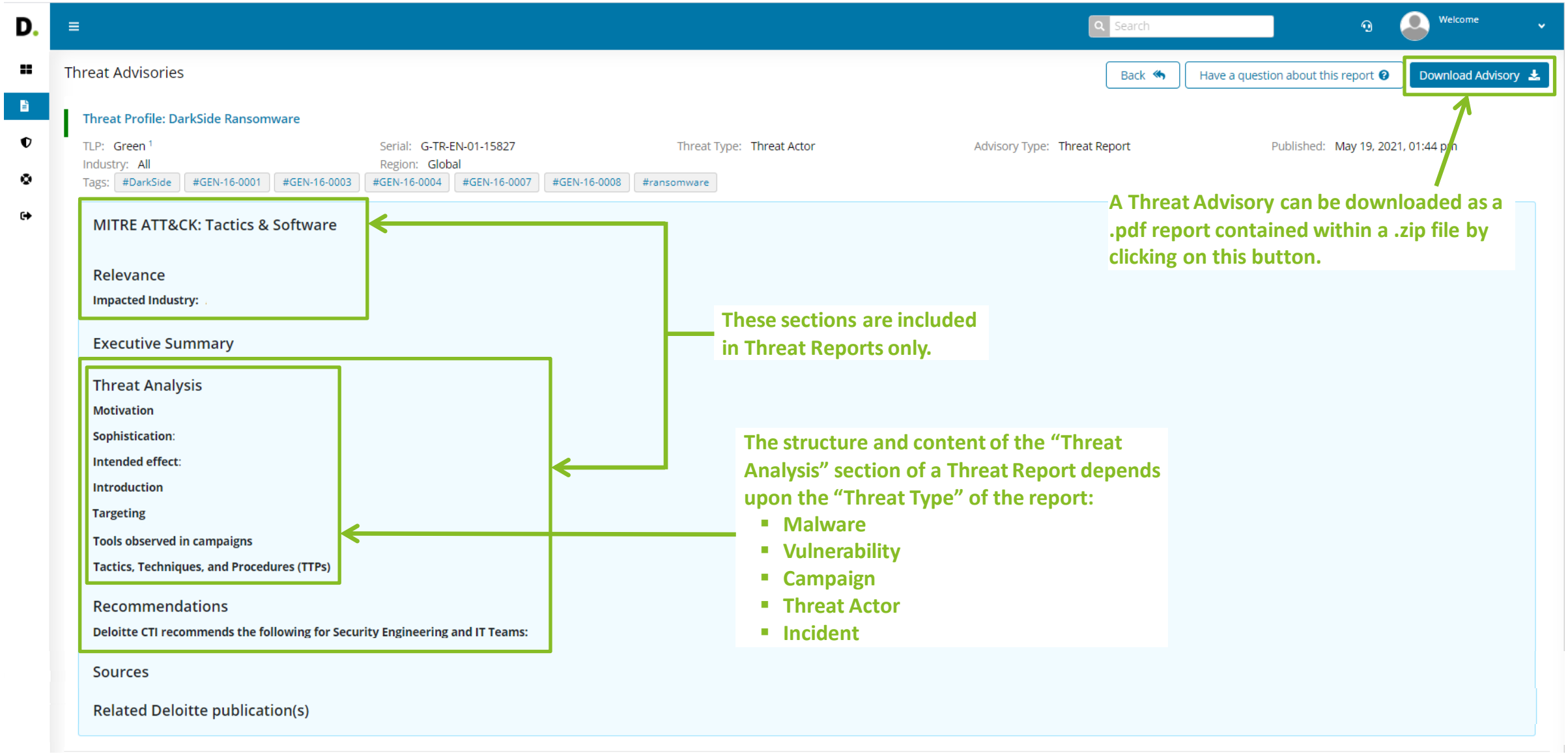
Threat Advisories view



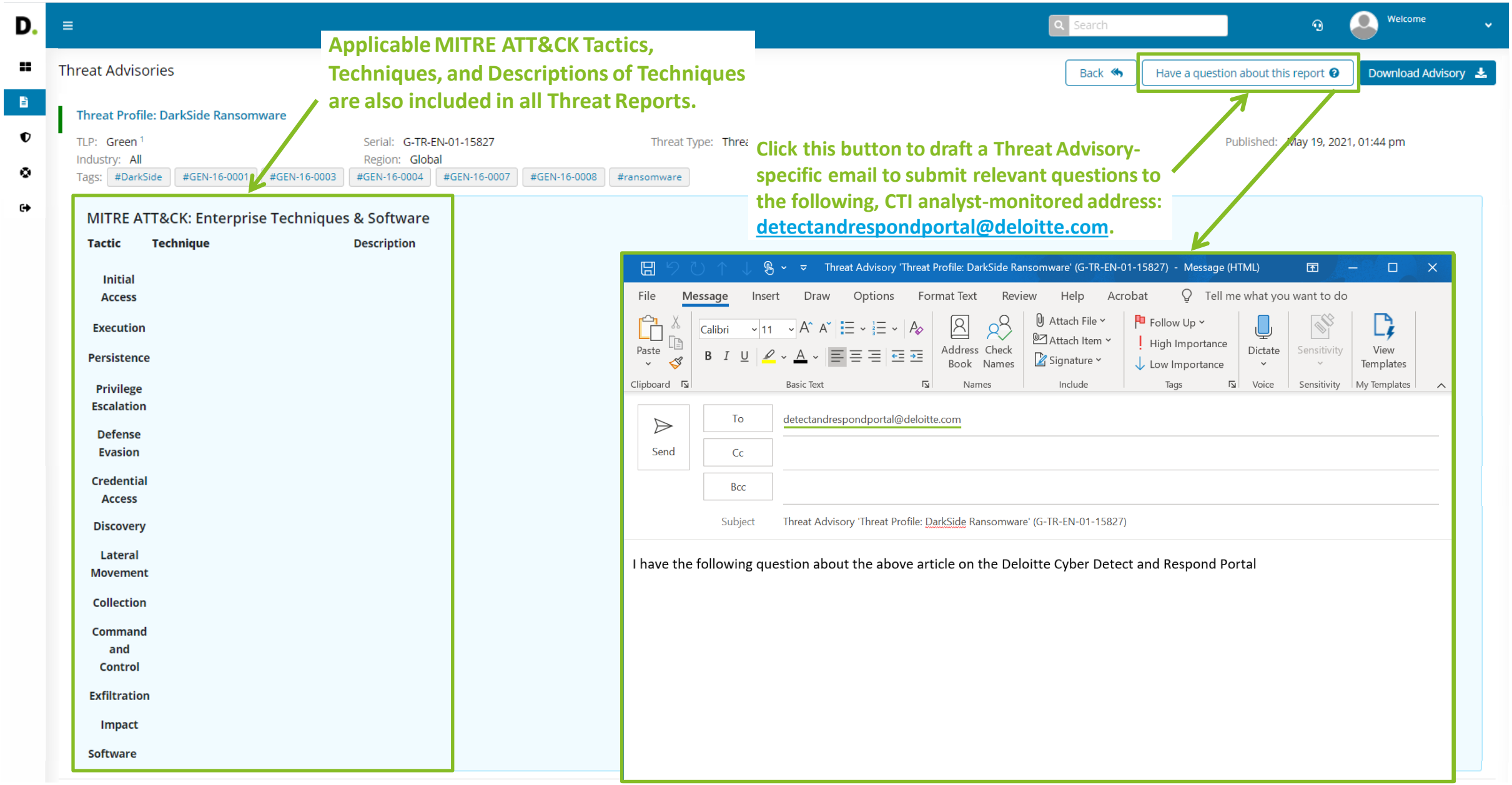
Threat Advisories view (cont'd)



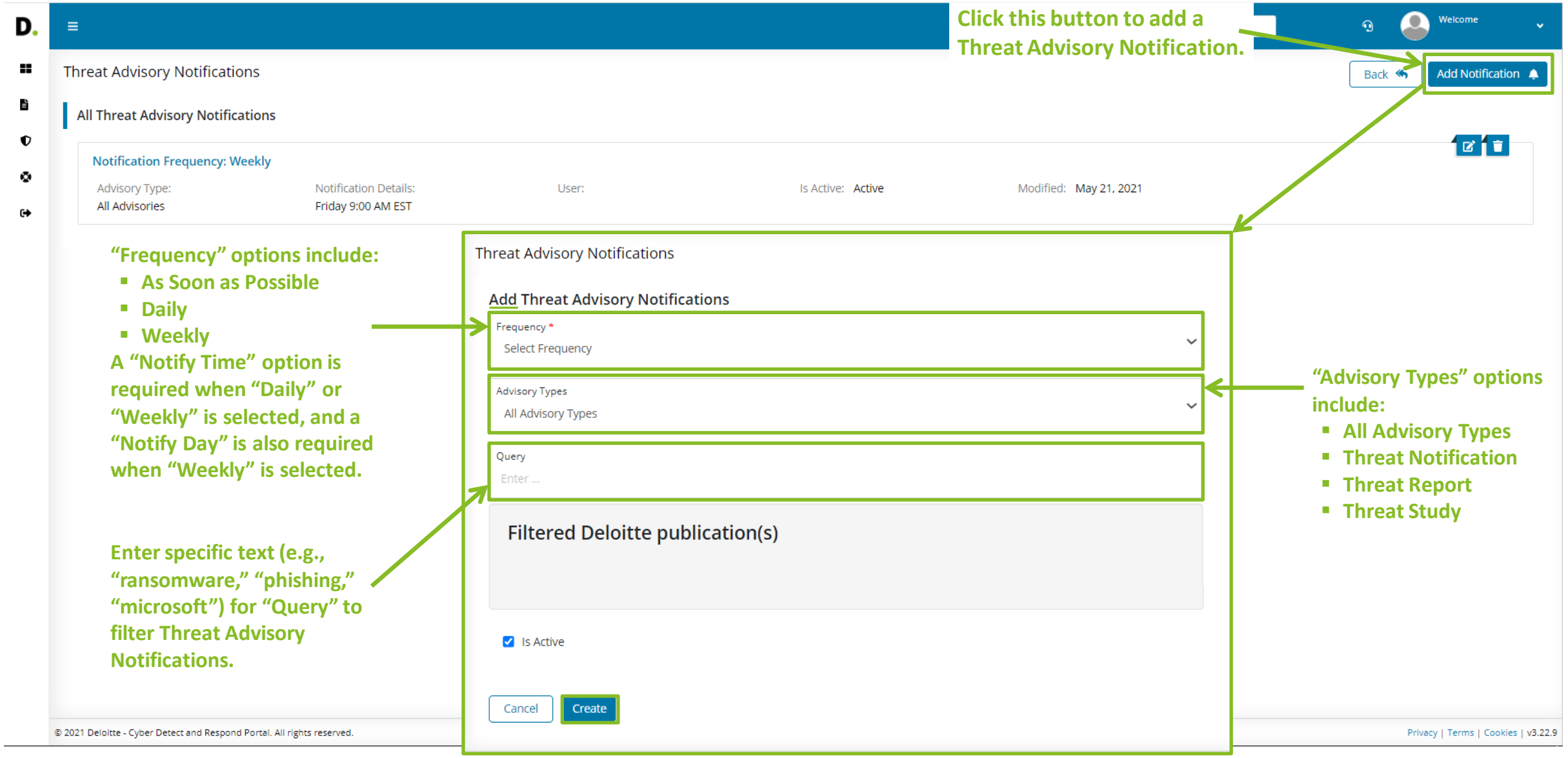
Threat Advisory in-depth



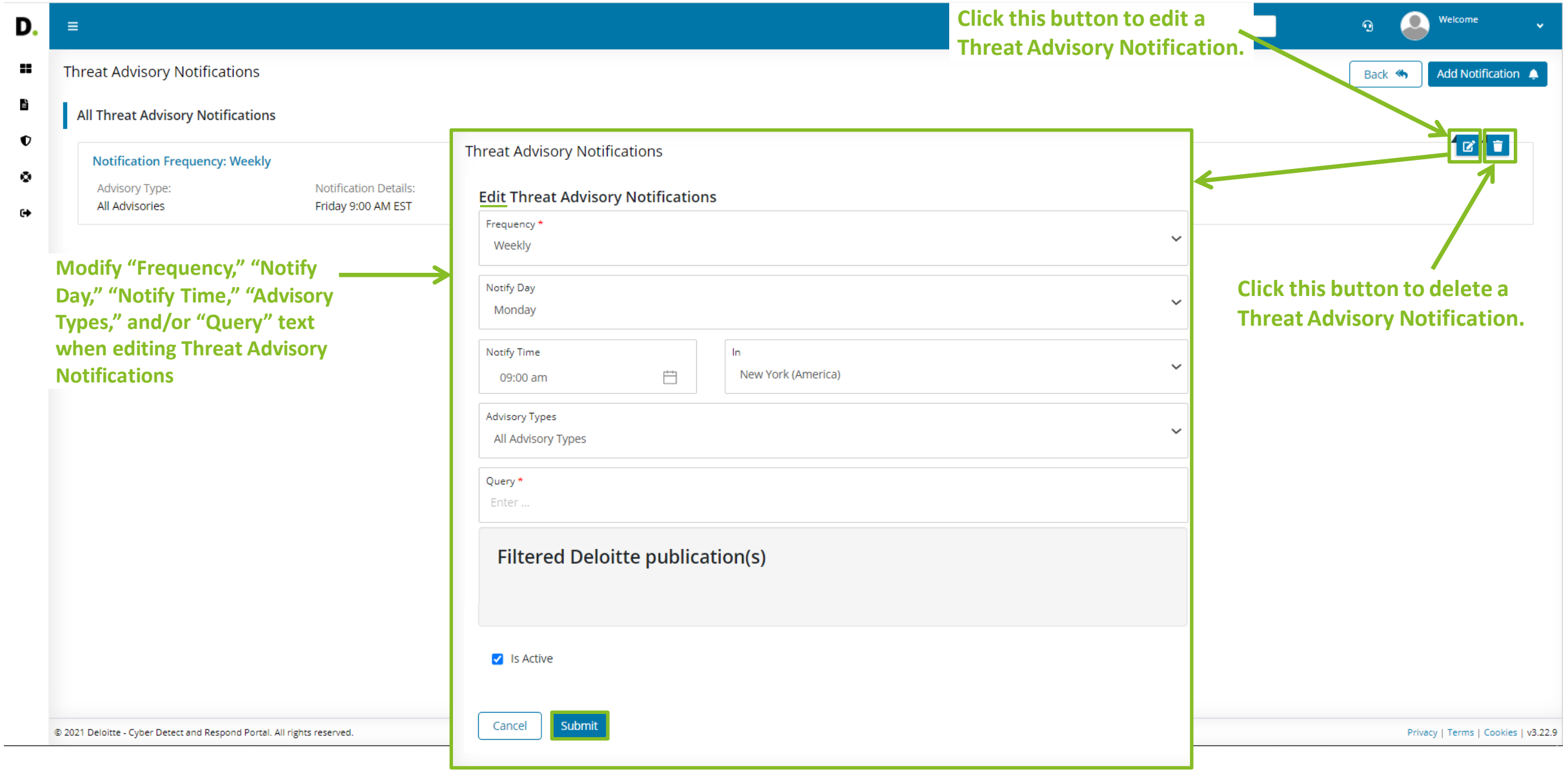
Threat Advisory in-depth (cont'd)



Adding Threat Advisory Notifications



Editing Threat Advisory Notifications

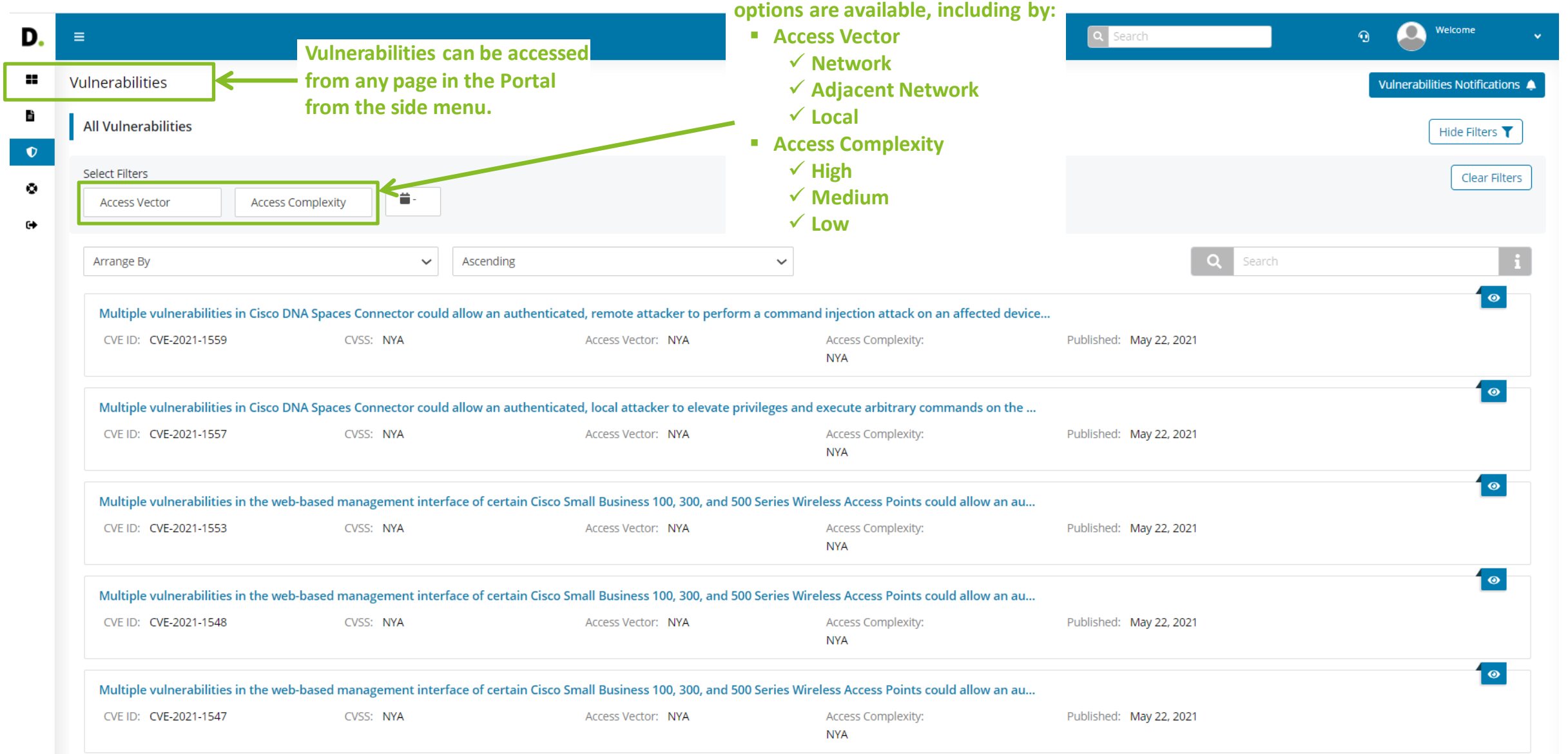


Vulnerabilities view

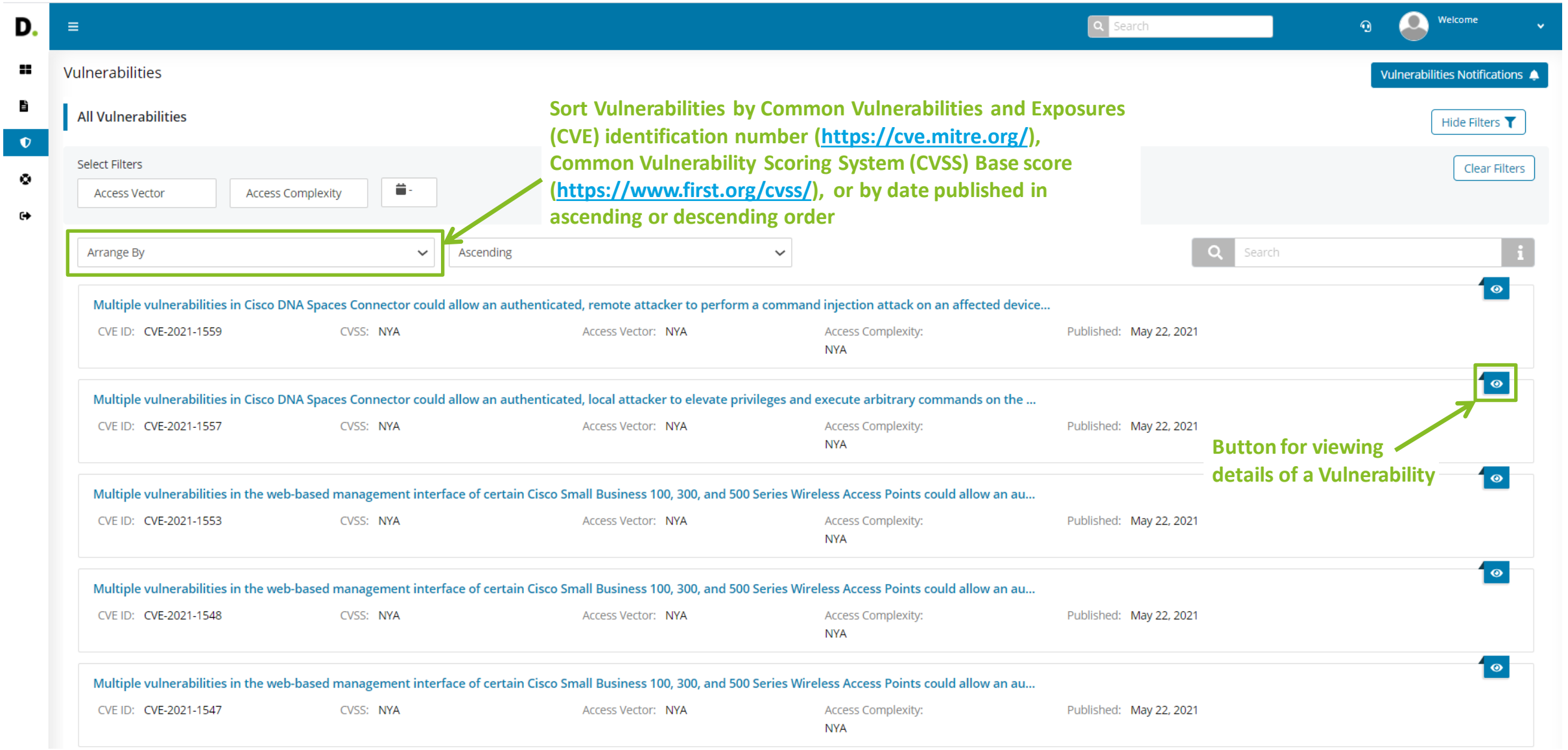
Vulnerabilities can be accessed from any page in the Portal from the side menu.

Multiple Vulnerabilities filtering options are available, including by:

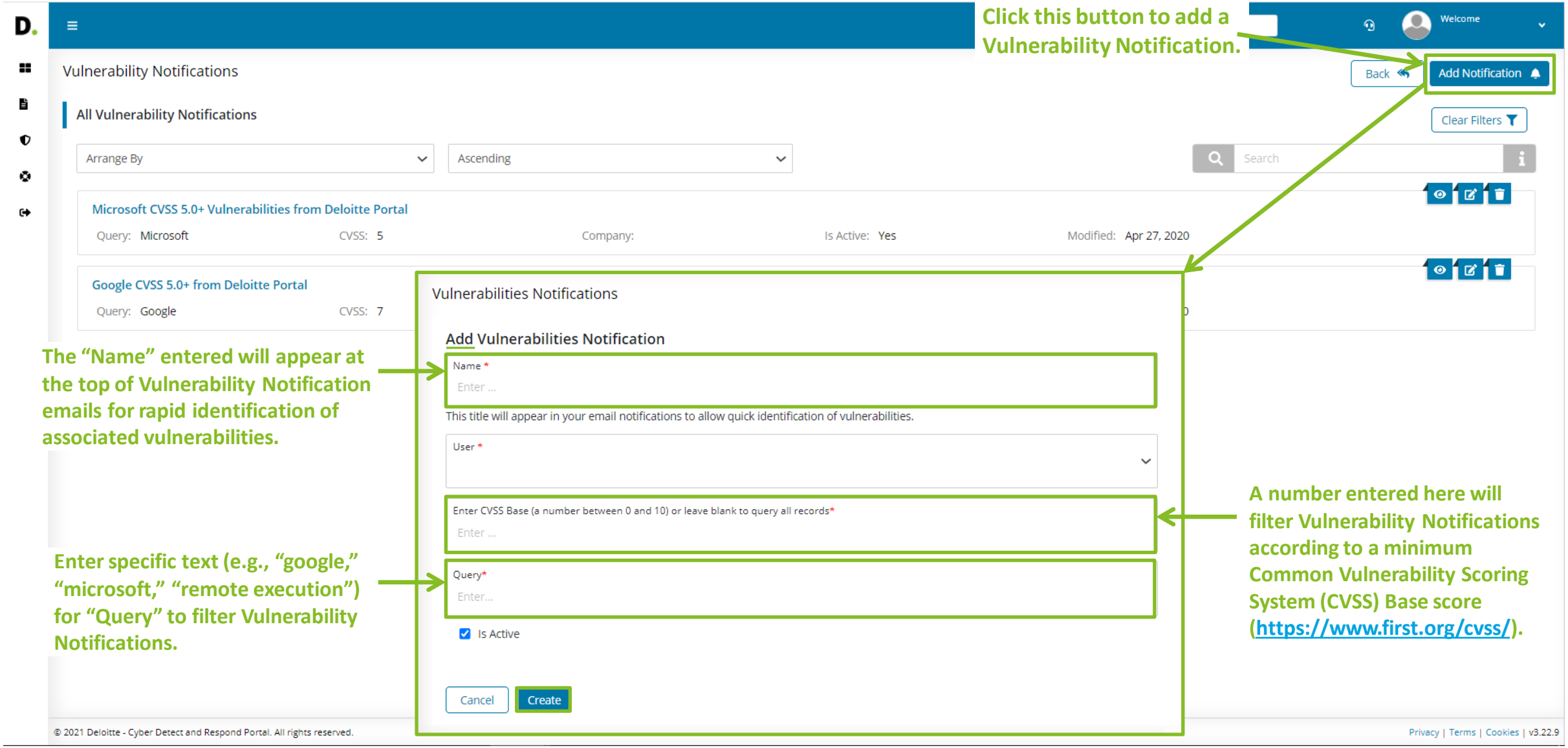
- Access Vector
  - ✓ Network
  - ✓ Adjacent Network
  - ✓ Local
- Access Complexity
  - ✓ High
  - ✓ Medium
  - ✓ Low



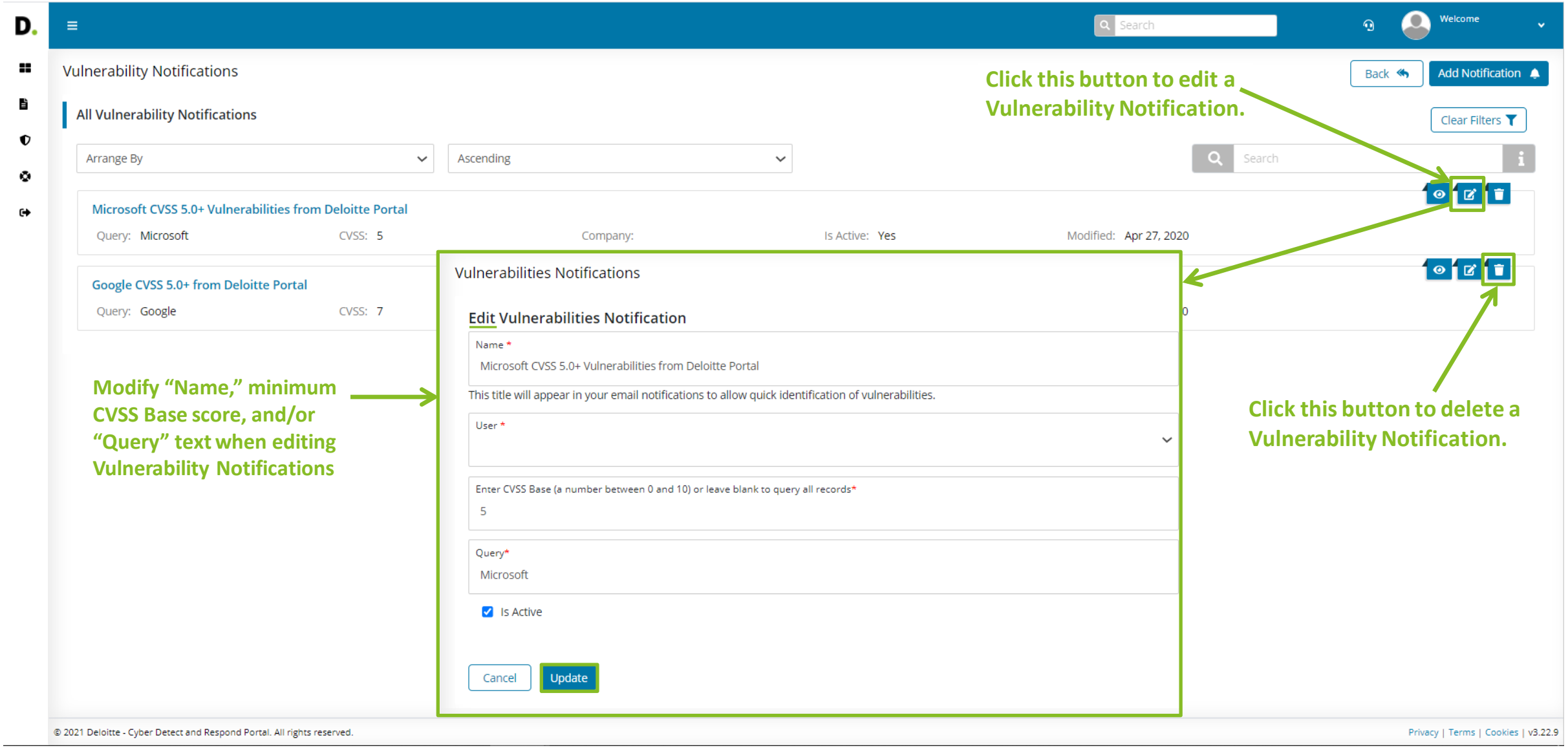
Vulnerabilities view (cont'd)



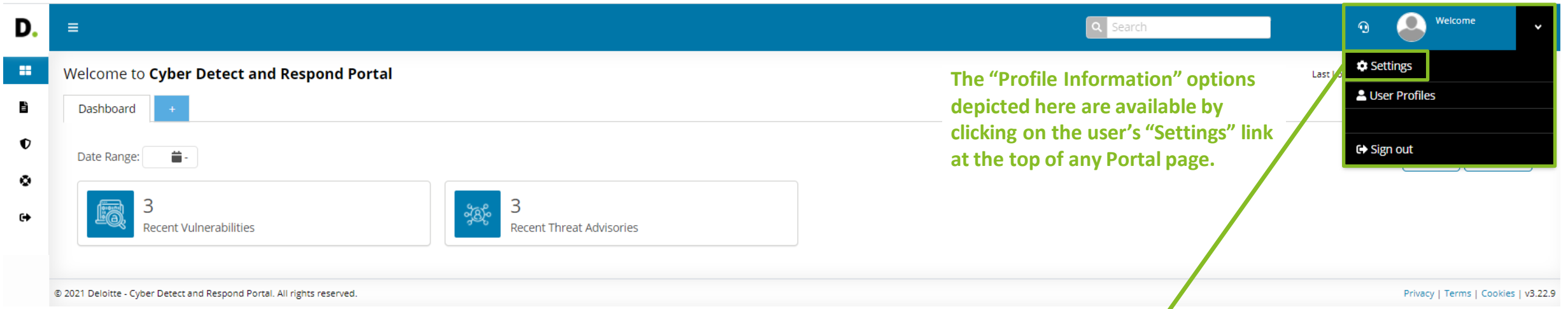
Adding Vulnerability Notifications



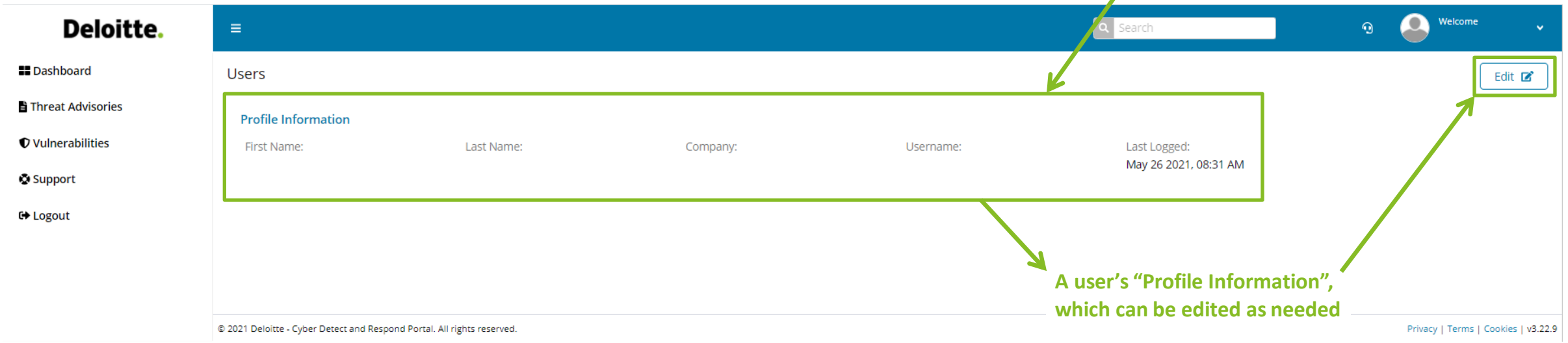
Editing Vulnerability Notifications



Account Settings view

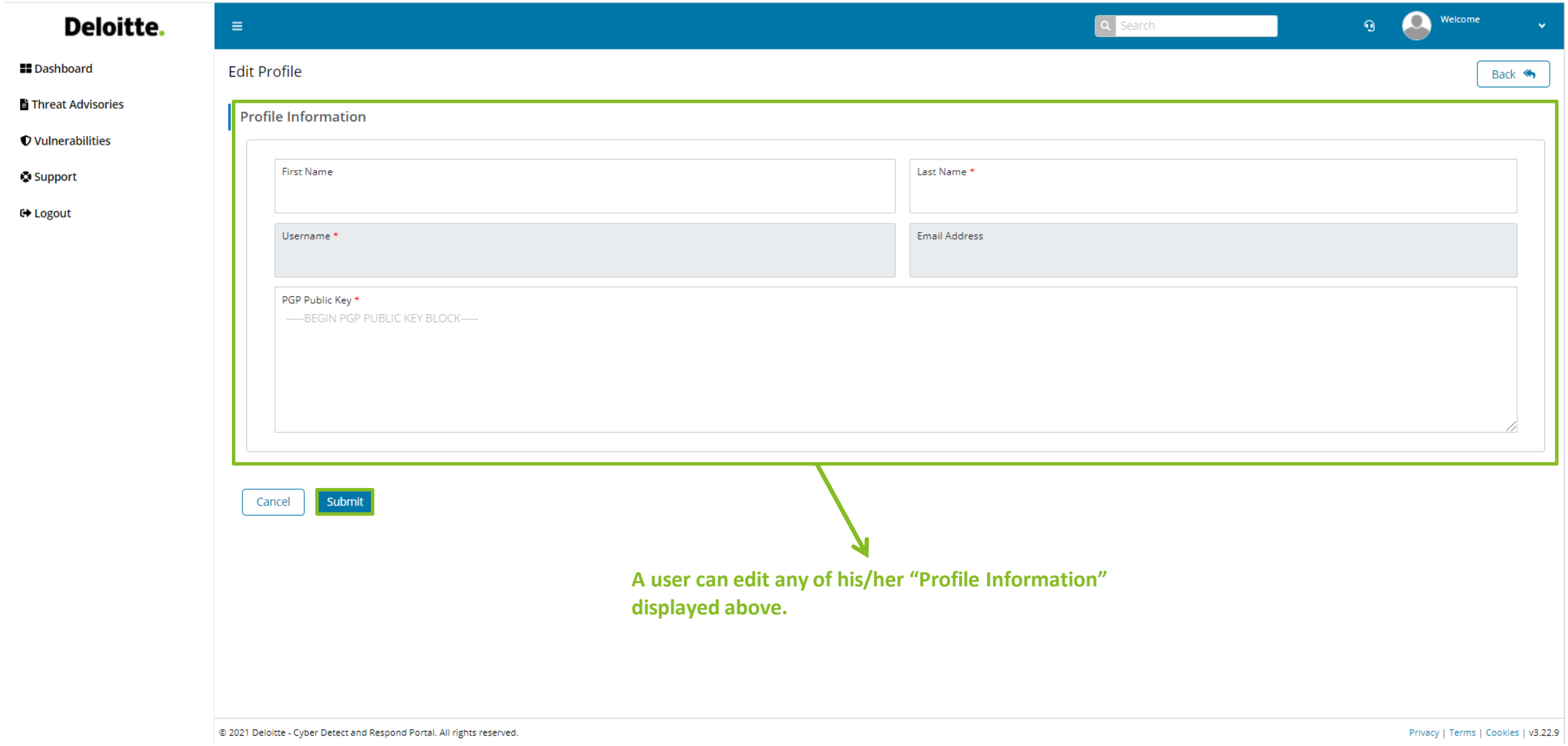


The "Profile Information" options depicted here are available by clicking on the user's "Settings" link at the top of any Portal page.



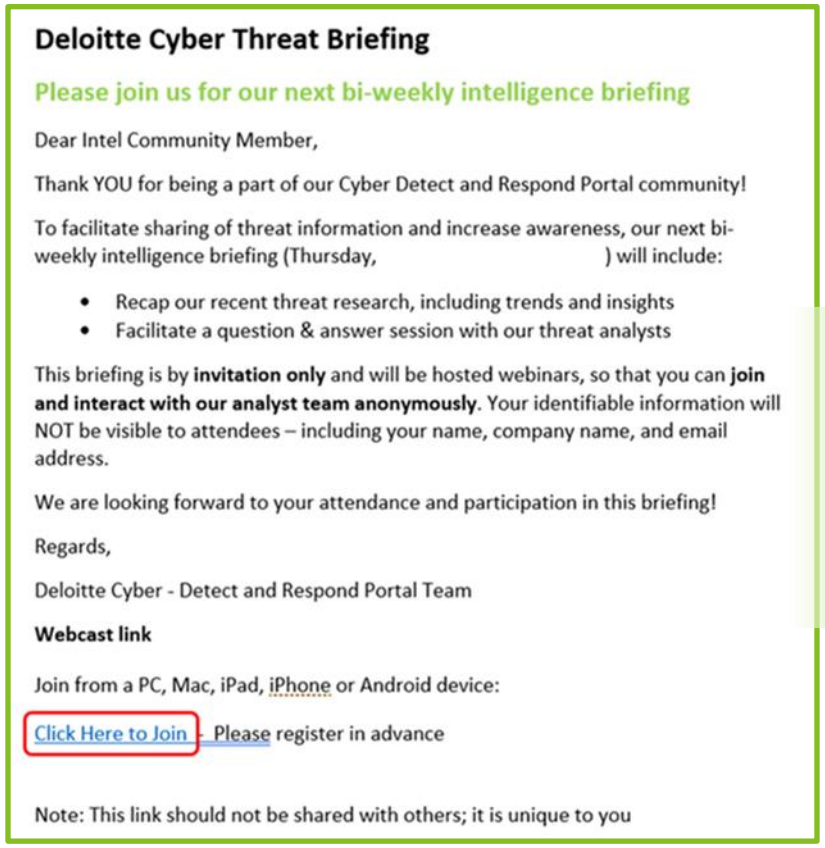
A user's "Profile Information", which can be edited as needed

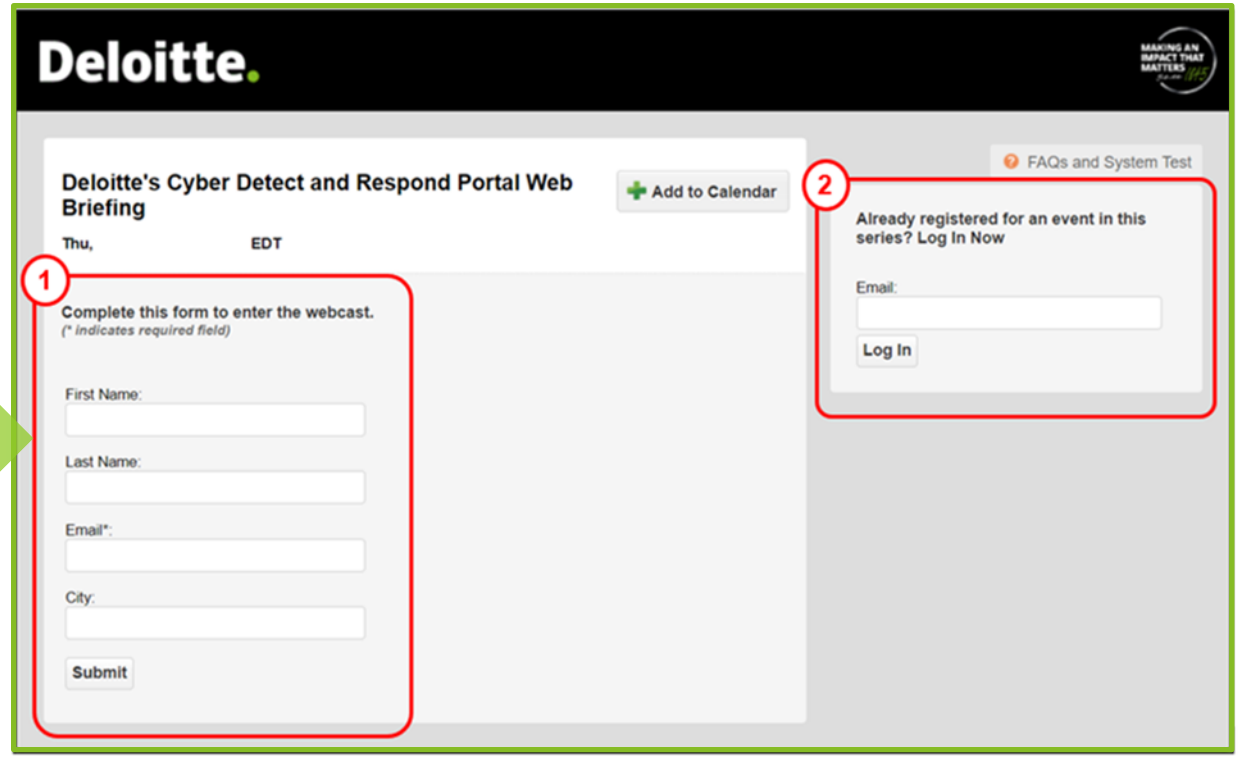
Account Settings view (cont'd)



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 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

Deloitte.

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 for a detailed description of DTTL and its member firms. Please see 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.