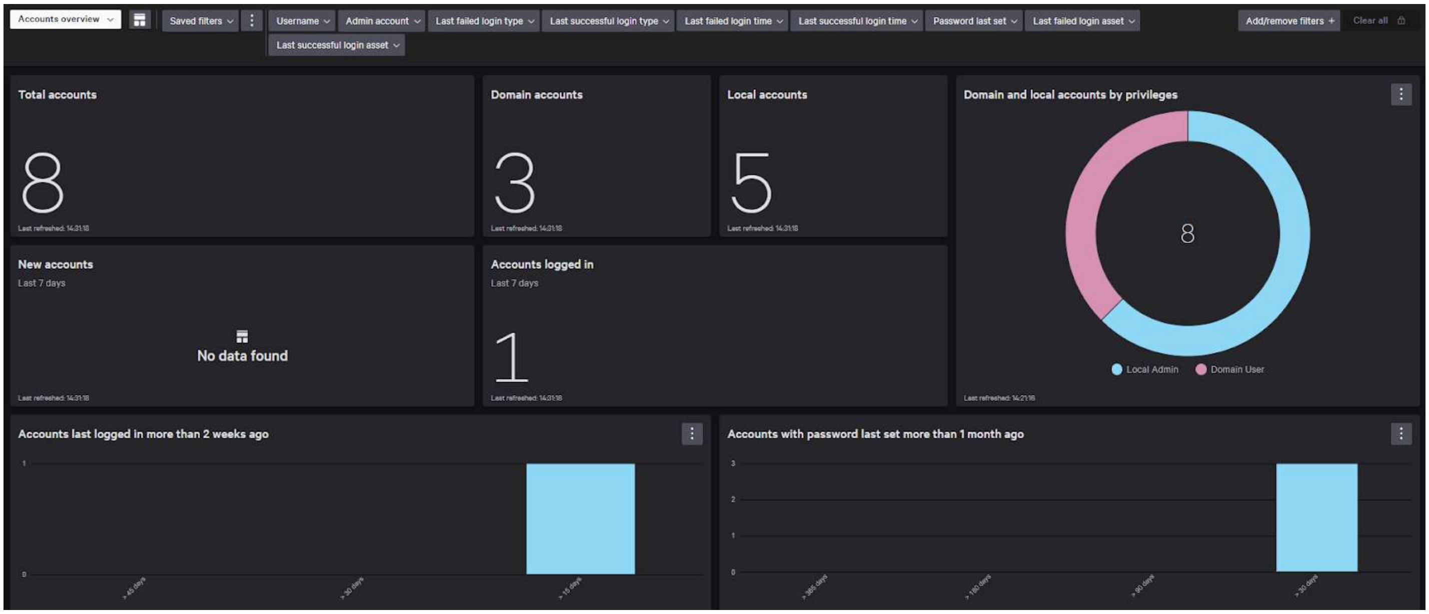
Exposure Management – Accounts and Logins

Crowdstrike's Exposure Management tools provide a lot of visibility into activity on your devices. This includes data about accounts that log into managed assets, as well as tracking the login attempts themselves. I'll show you where this data lives and how you can get value out of the information provided by these tools

Dashboards

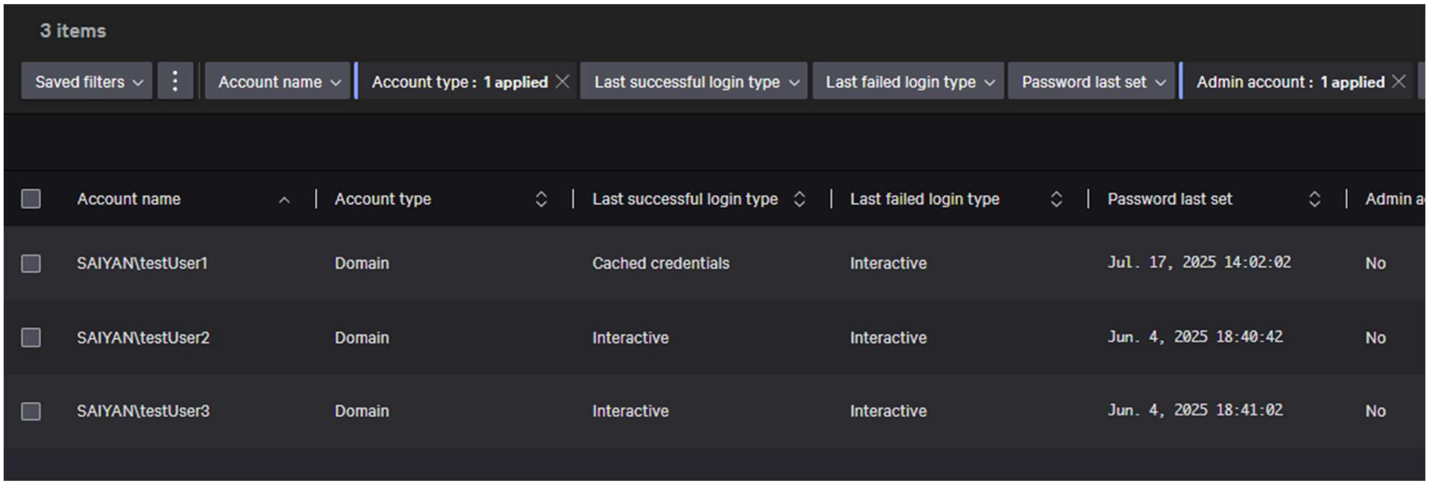
As usual, the dashboards are a great place to get a feel for the available data and how it can be displayed. Start by going to Exposure Management > Accounts > Dashboards. You'll see something like this:



In the top left corner there's a white dropdown menu, allowing you to choose from a few prebuilt dashboards plus any custom dashboards you or a coworker have created and shared. By default these dashboards show all data from your environment, but you can use the filters along the top to drill down into whatever interests you, whether it's a specific account type, accounts that have failed logins recently, or accounts with old credentials.

Note: *Credential age is a particularly important data point to track, especially for domain accounts or accounts with elevated privileges. Many of the attacks we see begin with a compromised account. Crowdstrike is a leader in Endpoint protection, but ensuring passwords are rotated and unneeded accounts are disabled will go a long way in preventing this type of attack attempt* ***before*** *it occurs.*

Many of these widgets are interactive - clicking the pink sector in the ‘Domains and local accounts by privileges’ will show a view of the underlying data with the appropriate filters applied:

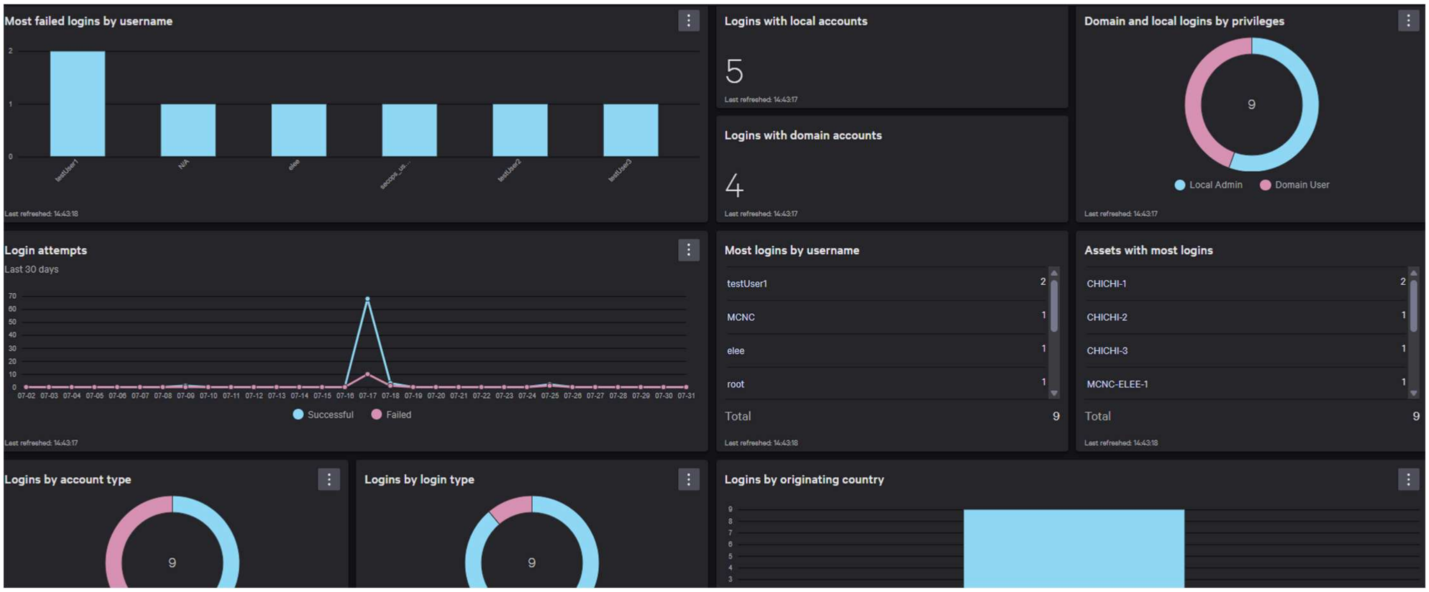


3 items

Saved filters | Account name | Account type : 1 applied | Last successful login type | Last failed login type | Password last set | Admin account : 1 applied

☐	Account name	Account type	Last successful login type	Last failed login type	Password last set	Admin a
☐	SAIYAN\testUser1	Domain	Cached credentials	Interactive	Jul. 17, 2025 14:02:02	No
☐	SAIYAN\testUser2	Domain	Interactive	Interactive	Jun. 4, 2025 18:40:42	No
☐	SAIYAN\testUser3	Domain	Interactive	Interactive	Jun. 4, 2025 18:41:02	No

Moving over to the Login Activity dashboard (use the white dropdown menu on the Dashboards page) gives us a view into the login activity on your managed assets:



Most logins by username

testUser1	2
MCNC	1
elee	1
root	1
Total	9

Last refreshed: 14:43:18

Assets with most logins

CHICHI-1	2
CHICHI-2	1
CHICHI-3	1
MCNC-ELEE-1	1
Total	9

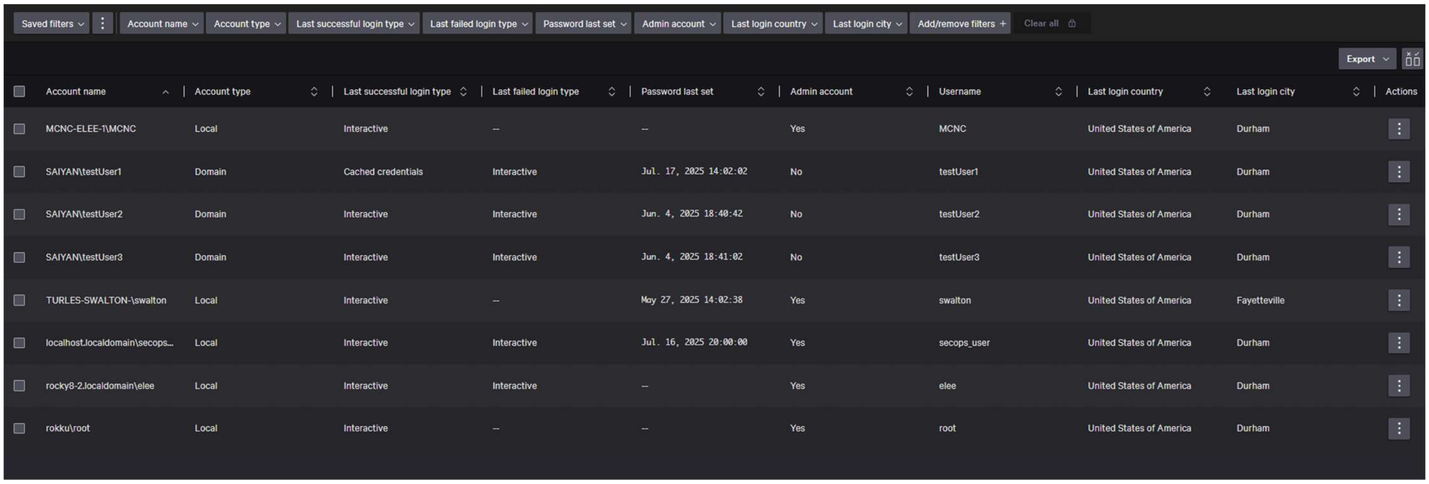
Last refreshed: 14:43:18

This includes helpful information like:

- Who’s logging into which asset?
- Has there been a spike in successful or failed logins over the past 30 days?
- What type of logins are occurring?
- Where in the world are login attempts originating?

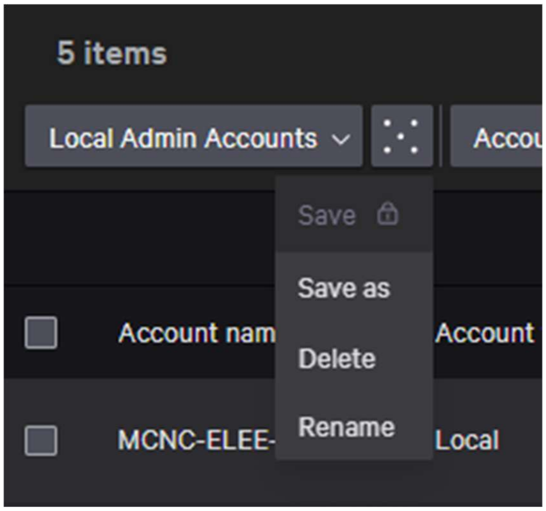
Accounts

We can take a closer look at the data powering the dashboards. Go to the Accounts page – either by selecting 'Accounts' in the tabs along the top or using the menu to go to Exposure Management>Accounts>Accounts. You should see something like this:

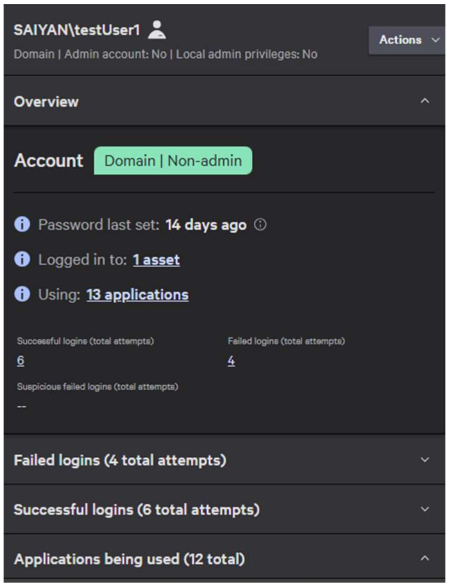


Account name	Account type	Last successful login type	Last failed login type	Password last set	Admin account	Username	Last login country	Last login city	Actions
MCNC-ELEE-1\MCNC	Local	Interactive	--	--	Yes	MCNC	United States of America	Durham	⋮
SAIYAN\testUser1	Domain	Cached credentials	Interactive	Jul. 17, 2025 14:02:02	No	testUser1	United States of America	Durham	⋮
SAIYAN\testUser2	Domain	Interactive	Interactive	Jun. 4, 2025 18:40:42	No	testUser2	United States of America	Durham	⋮
SAIYAN\testUser3	Domain	Interactive	Interactive	Jun. 4, 2025 18:41:02	No	testUser3	United States of America	Durham	⋮
TURLES-SWALTON-\swalton	Local	Interactive	--	May 27, 2025 14:02:38	Yes	swalton	United States of America	Fayetteville	⋮
localhost.localdomain\secops...	Local	Interactive	Interactive	Jul. 16, 2025 20:00:00	Yes	secops_user	United States of America	Durham	⋮
rocky8-2.localdomain\elee	Local	Interactive	Interactive	--	Yes	elee	United States of America	Durham	⋮
rokku\root	Local	Interactive	--	--	Yes	root	United States of America	Durham	⋮

These views can also be filtered and sorted, and columns can be added as needed. Filter sets are saveable for later use, so if you find yourself frequently going back to the same view then saving those filters can save you some time and clicks.



Clicking a row will open a details page where you can see more information about the account like password age, login activity, and applications being used.



SAIYAN\testUser1

Domain | Admin account: No | Local admin privileges: No

Overview

Account Domain | Non-admin

Password last set: **14 days ago**

Logged in to: 1 asset

Using: 13 applications

Successful logins (total attempts)

6

Failed logins (total attempts)

4

Suspicious failed logins (total attempts)

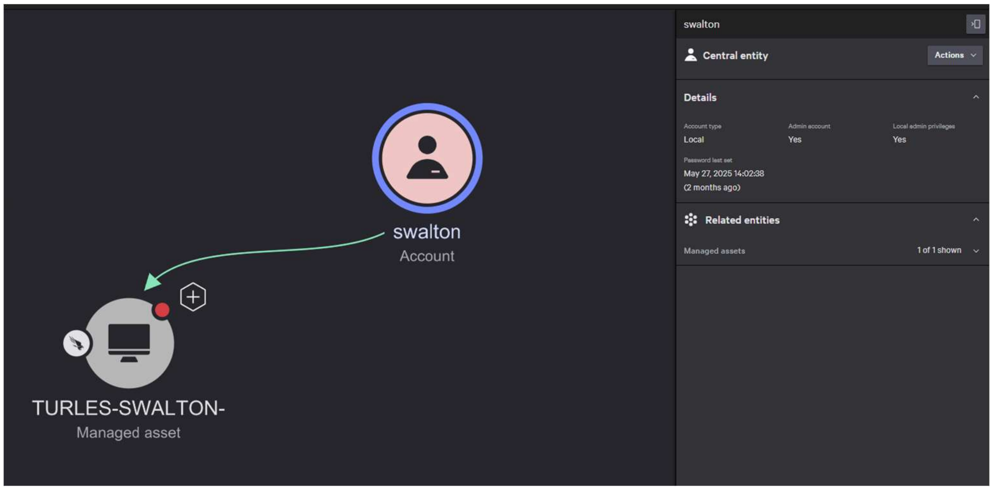
--

Failed logins (4 total attempts)

Successful logins (6 total attempts)

Applications being used (12 total)

Try clicking the 3-dot 'Actions' menu next to a user and selecting 'Asset Graph'. This will generate a visual representation of login activity for that user over a defined time range (the default and maximum is 7 days, but you can lower that if needed).



swalton

Central entity

Details

Account type: Local

Admin account: Yes

Local admin privileges: Yes

Password last set: May 27, 2025 14:02:38 (2 months ago)

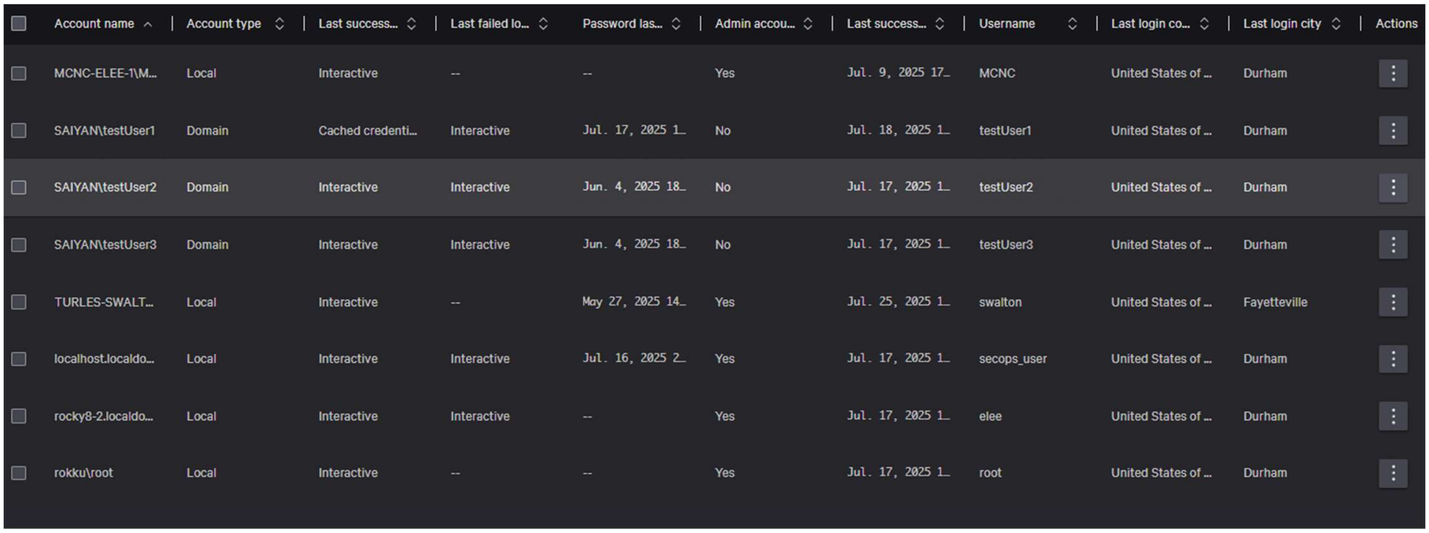
Related entities

Managed assets: 1 of 1 shown

Clicking on the different elements will show more information about the account, asset, or login attempts. These graphs can be expanded by clicking the + icon next to an asset or account. For instance, clicking the '+' by this managed asset will show other accounts with successful or failed logins over the same period as well as any network activity to or from other managed hosts. This makes it easy to follow trails and investigate potentially suspicious login and network activity.

Successful and Failed Logins

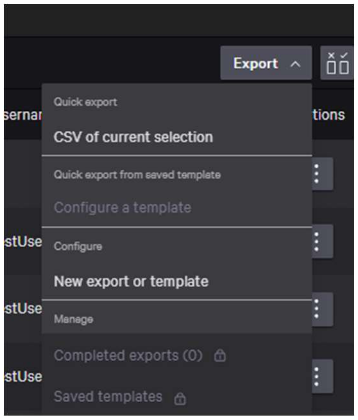
The Successful Logins page will show you successful logins that have occurred over the past 45 days. Results are broken out based on individual accounts on individual hosts and include login type, time, and location:



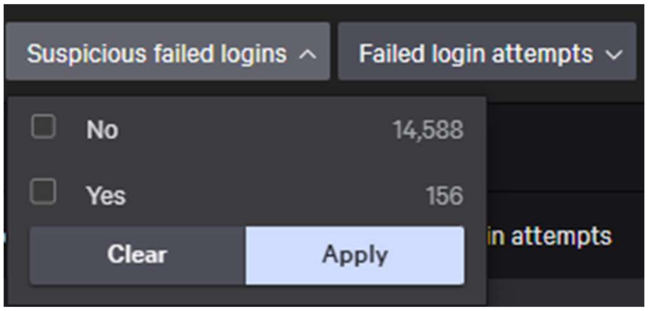
□	Account name	Account type	Last success…	Last failed lo…	Password las…	Admin accou…	Last success…	Username	Last login co…	Last login city	Actions
□	MCNC-ELEE-1\M…	Local	Interactive	--	--	Yes	Jul. 9, 2025 17…	MCNC	United States of …	Durham	⋮
□	SAIYAN\testUser1	Domain	Cached credenti…	Interactive	Jul. 17, 2025 1…	No	Jul. 18, 2025 1…	testUser1	United States of …	Durham	⋮
□	SAIYAN\testUser2	Domain	Interactive	Interactive	Jun. 4, 2025 18…	No	Jul. 17, 2025 1…	testUser2	United States of …	Durham	⋮
□	SAIYAN\testUser3	Domain	Interactive	Interactive	Jun. 4, 2025 18…	No	Jul. 17, 2025 1…	testUser3	United States of …	Durham	⋮
□	TURLES-SWALT…	Local	Interactive	--	May 27, 2025 14…	Yes	Jul. 25, 2025 1…	swalton	United States of …	Fayetteville	⋮
□	localhost.localdo…	Local	Interactive	Interactive	Jul. 16, 2025 2…	Yes	Jul. 17, 2025 1…	secops_user	United States of …	Durham	⋮
□	rocky8-2.localdo…	Local	Interactive	Interactive	--	Yes	Jul. 17, 2025 1…	elee	United States of …	Durham	⋮
□	rokku\root	Local	Interactive	--	--	Yes	Jul. 17, 2025 1…	root	United States of …	Durham	⋮

- **Login Type**: How this user is logging in. Types include ‘Interactive’ (physically typing a password), ‘Network’ (accessing a host over the network), ‘Service’ (A service or application logging in with those credentials), and ‘Remote Interactive’ (logging in with remote access like RDP).
- **Login Time**: These times are aggregated based on how long ago they occurred. Multiple logins within 24 hours will be aggregated to the nearest hour, while those older than 24 hours will be aggregated to the nearest day.
- **Login Location**: This data is based on registration data from the external IP used in the login attempt. This will give you a general area of where logins have originated.

All of this data can be filtered, sorted, or exported as needed.



The Failed Logins page allows you to track the same information for failed login activity. Crowdstrike also categorizes what they call ‘Suspicious failed logins’, which they explain in documentation as “based on several factors, including failed logins within a certain period of time.”



Looking Ahead

Account and login data is a great example of the visibility that Crowdstrike provides. Today we’ve seen the tools available to interact with this data in Exposure Management, but that’s not the only option. For instance, you could utilize the Custom Dashboard functionality to create a view of everything you care about in Crowdstrike, including Account data, Vulnerabilities, recent Detections, etc. In future guides we’ll do a deep dive into the Custom Dashboard creation and Scheduled Reporting capabilities built into Crowdstrike.

For more information about Exposure Management – Accounts, reference this Crowdstrike Article (login required): https://falcon.laggar.gcw.crowdstrike.com/documentation/page/d20b51a1/asset-management-accounts