**SQL Query Export Report Examples**

Key:

**Title here** *(Detail here)*

(Query Here)

**Example:**  
(Image of example query here)

**Aggregated Credential Status** *(Node Fingerprint + IP + Hostname + Asset ID + Credential Status)*

WITH max\_certainty AS (

SELECT asset\_id, max(certainty) AS certainty

FROM dim\_asset\_operating\_system

GROUP BY asset\_id

),

asset\_cred\_status AS (

SELECT DISTINCT fa.asset\_id,

CASE WHEN dacs.aggregated\_credential\_status\_id IN ('1','2') THEN 'FAIL'

WHEN dacs.aggregated\_credential\_status\_id IN ('3','4') THEN 'SUCCESS'

ELSE 'N/A' END AS auth\_status

FROM fact\_asset fa

JOIN dim\_aggregated\_credential\_status dacs ON (fa.aggregated\_credential\_status\_id = dacs.aggregated\_credential\_status\_id)

)

SELECT acs.asset\_id,

da.ip\_address,

da.host\_name,

acs.auth\_status,

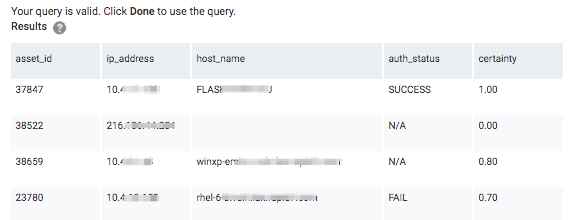
ROUND(mc.certainty::numeric, 2) AS certainty

FROM asset\_cred\_status acs

JOIN dim\_asset da ON (da.asset\_id = acs.asset\_id)

JOIN max\_certainty mc ON (mc.asset\_id = da.asset\_id)

**Example:**



**Asset/Scan/Site + Certainty and Credential status** *(Certainty + Site Name + Credential Status + Date of last scan)*

SELECT asset\_id, scan\_id, date, name, credential\_status\_description, certainty

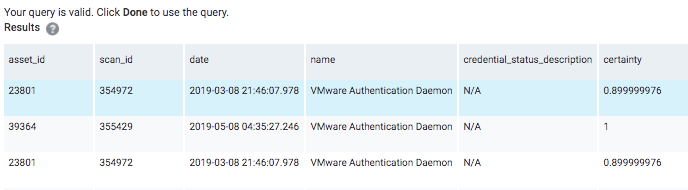
FROM fact\_asset\_scan\_service

JOIN dim\_credential\_status USING(credential\_status\_id)

JOIN dim\_service USING(service\_id)

JOIN dim\_asset\_operating\_system USING(asset\_id)

**Example:**



**Search for various Software** *(Site name + IP + MAC + DNS Hostname + Vendor + Software Name/Family/Class ~ This example is searching for ‘Cyber’ & ‘Crowd’ so change the second and third to last line to change the target software you are looking for)*

SELECT da.sites AS "Site\_Name",

da.ip\_address AS "IP\_Address",

da.mac\_address AS "MAC\_Address",

da.host\_name AS "DNS\_Hostname",

ds.vendor AS "Vendor",

ds.name AS "Software\_Name",

ds.family AS "Software\_Family",

ds.version AS "Software\_Version",

ds.software\_class AS "Software\_Class"

FROM dim\_asset\_software das

JOIN dim\_software ds USING(software\_id)

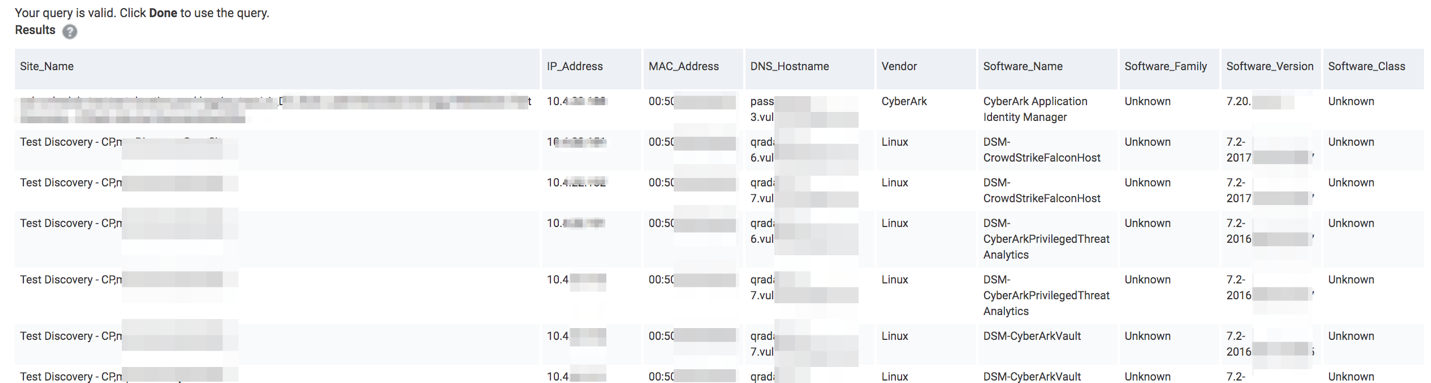
JOIN dim\_asset da ON da.asset\_id = das.asset\_id

WHERE ds.name LIKE '%Cyber%'

OR ds.name LIKE '%Crowd%'

ORDER BY ds.name ASC

**Example:**



**All Dynamic Asset Groups: Count/Vulns by date/severity** *(Dynamic Asset Group + total asset count + vulnerability data from 30-60-90 days out broken down by severity + total vulnerability count in DAG)*

WITH

asset\_vuln\_finding\_age AS (

-- List the age of vuln findings in scope, along with their asset information

SELECT avd.asset\_id,

CASE WHEN (avd.age < 30 AND dv.severity\_score < 4) THEN 1 ELSE 0 END AS "<30m",

CASE WHEN (avd.age < 30 AND dv.severity\_score >= 4 AND dv.severity\_score < 8) THEN 1 ELSE 0 END AS "<30s",

CASE WHEN (avd.age < 30 AND dv.severity\_score >= 8) THEN 1 ELSE 0 END AS "<30c",

CASE WHEN (avd.age < 60 AND avd.age >= 30 AND dv.severity\_score < 4) THEN 1 ELSE 0 END AS "30-60m",

CASE WHEN (avd.age < 60 AND avd.age >= 30 AND dv.severity\_score >= 4 AND dv.severity\_score < 8) THEN 1 ELSE 0 END AS "30-60s",

CASE WHEN (avd.age < 60 AND avd.age >= 30 AND dv.severity\_score >= 8) THEN 1 ELSE 0 END AS "30-60c",

CASE WHEN (avd.age < 90 AND avd.age >= 60 AND dv.severity\_score < 4) THEN 1 ELSE 0 END AS "60-90m",

CASE WHEN (avd.age < 90 AND avd.age >= 60 AND dv.severity\_score >= 4 AND dv.severity\_score < 8) THEN 1 ELSE 0 END AS "60-90s",

CASE WHEN (avd.age < 90 AND avd.age >= 60 AND dv.severity\_score >= 8) THEN 1 ELSE 0 END AS "60-90c",

CASE WHEN (avd.age >= 90 AND dv.severity\_score < 4) THEN 1 ELSE 0 END AS "90+m",

CASE WHEN (avd.age >= 90 AND dv.severity\_score >= 4 AND dv.severity\_score < 8) THEN 1 ELSE 0 END AS "90+s",

CASE WHEN (avd.age >= 90 AND dv.severity\_score >= 8) THEN 1 ELSE 0 END AS "90+c"

FROM (

-- Find earliest finding date for a vuln, coupled with the most recent instance count for the vuln

SELECT fasv.asset\_id, fasv.vulnerability\_id, date\_part('days', (CURRENT\_DATE - MIN (fasv.date)) + interval '1 day') AS age

FROM fact\_asset\_scan\_vulnerability\_instance fasv

-- Filter to only include vuln findings present in the latest scan

JOIN fact\_asset\_vulnerability\_instance fav ON fasv.asset\_id = fav.asset\_id

AND fasv.vulnerability\_id = fav.vulnerability\_id

AND fasv.service\_id = fav.service\_id

AND fasv.port = fav.port

AND fasv.proof = fav.proof

GROUP BY fasv.asset\_id, fasv.vulnerability\_id

) avd

JOIN dim\_vulnerability dv ON dv.vulnerability\_id = avd.vulnerability\_id

)

SELECT \*

FROM (

SELECT dag.name AS group\_name,

COUNT(DISTINCT vfa.asset\_id) AS asset\_count,

SUM(vfa."<30m") AS "<30\_moderate",

SUM(vfa."<30s") AS "<30\_severe",

SUM(vfa."<30c") AS "<30\_critical",

SUM(vfa."30-60m") AS "30-60\_moderate",

SUM(vfa."30-60s") AS "30-60\_severe",

SUM(vfa."30-60c") AS "30-60\_critical",

SUM(vfa."60-90m") AS "60-90\_moderate",

SUM(vfa."60-90s") AS "60-90\_severe",

SUM(vfa."60-90c") AS "60-90\_critical",

SUM(vfa."90+m") AS "90+\_moderate",

SUM(vfa."90+s") AS "90+\_severe",

SUM(vfa."90+c") AS "90+\_critical",

SUM(vfa."<30m") + SUM(vfa."<30s")+ SUM(vfa."<30c") + SUM(vfa."30-60m")+ SUM(vfa."30-60s") + SUM(vfa."30-60c") +

SUM(vfa."60-90m") + SUM(vfa."60-90s") + SUM(vfa."60-90c") + SUM(vfa."90+m") + SUM(vfa."90+s") + SUM(vfa."90+c") AS vuln\_count

FROM (

SELECT \*

FROM asset\_vuln\_finding\_age

UNION ALL

-- Include zero counts for assets that have no vuln findings

SELECT da.asset\_id, 0 AS "<30m", 0 AS "<30s", 0 AS "<30c", 0 AS "30-60m", 0 AS "30-60s", 0 AS "30-60c",

0 AS "60-90m", 0 AS "60-90s", 0 AS "90+m", 0 AS "60-90c", 0 AS "90+s", 0 AS "90+c"

FROM dim\_asset da

WHERE asset\_id NOT IN (SELECT DISTINCT asset\_id FROM asset\_vuln\_finding\_age)

) vfa

JOIN dim\_asset\_group\_asset daga ON daga.asset\_id = vfa.asset\_id

JOIN dim\_scope\_asset\_group USING (asset\_group\_id)

JOIN dim\_asset\_group dag USING (asset\_group\_id)

GROUP BY dag.name

) site\_vuln\_counts

UNION ALL

-- Include zero counts for asset groups in scope with no assets

SELECT dag.name AS group\_name, 0 AS asset\_count, 0 AS "<30m", 0 AS "<30s", 0 AS "<30c", 0 AS "30-60m", 0 AS "30-60s", 0 AS "30-60c",

0 AS "60-90m", 0 AS "60-90s", 0 AS "90+m", 0 AS "60-90c", 0 AS "90+s", 0 AS "90+c", 0 AS vuln\_count

FROM dim\_scope\_asset\_group dsag

JOIN dim\_asset\_group dag USING(asset\_group\_id)

WHERE dsag.asset\_group\_id NOT IN (

SELECT DISTINCT daga.asset\_group\_id

FROM dim\_asset da

JOIN dim\_asset\_group\_asset daga USING(asset\_id)

)

ORDER BY group\_name

**Example:**  
