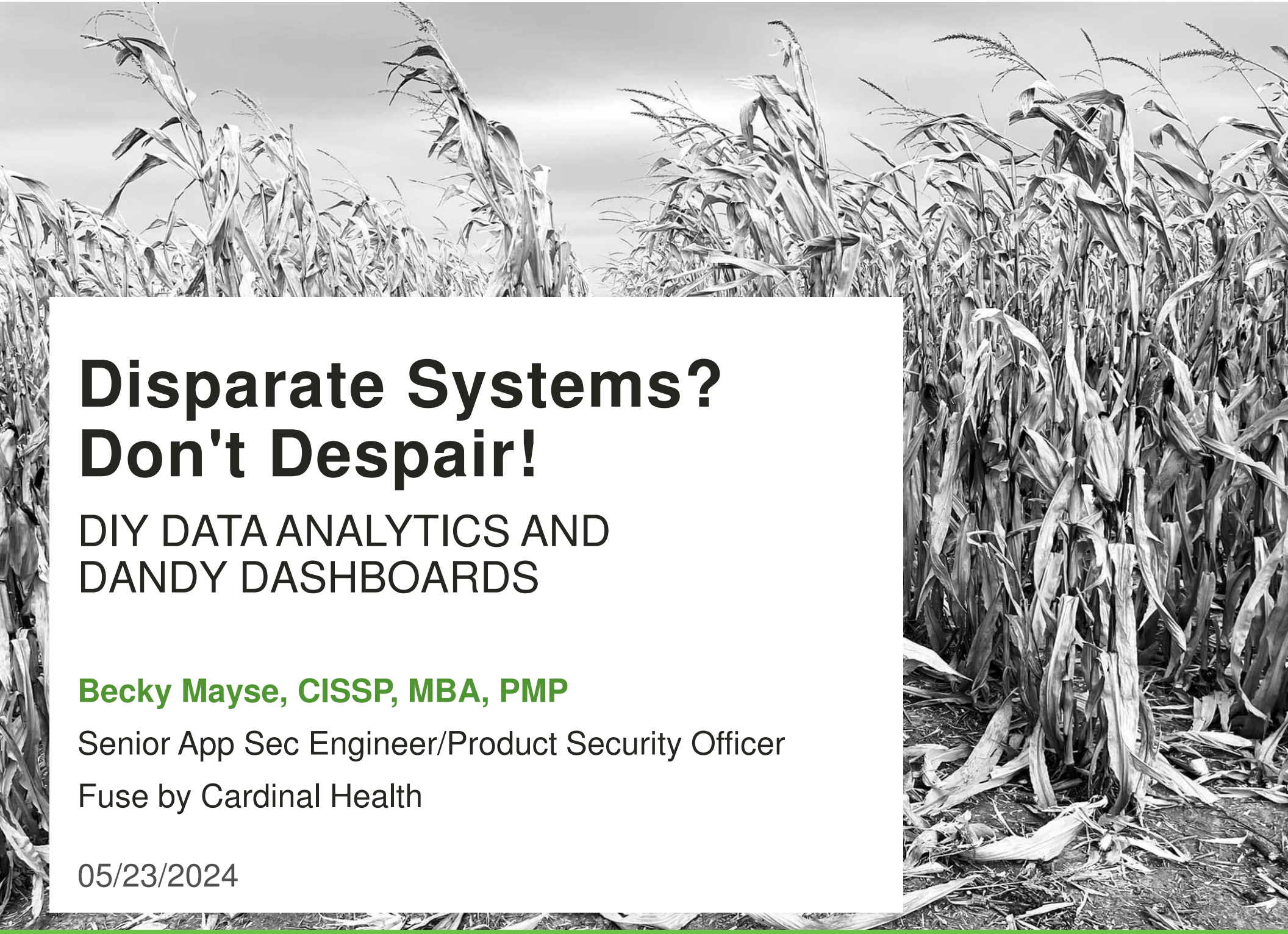


Disparate Systems? Don't Despair!

DIY DATA ANALYTICS AND DANDY DASHBOARDS

Becky Mayse, CISSP, MBA, PMP

Senior App Sec Engineer/Product Security Officer

Fuse by Cardinal Health

05/23/2024

Topics

- About Me
- Product Security Officer
- Single Pane of Glass
- Why Use PowerBI
- Defining your Objective
- Dashboard Layers
- Diving for Data
- Make a Map
- Powering up in PowerBI
- Metrics
- Sample Dashboards
- Going Further
- Questions

About Me

Career

- Product Security Officer at Fuse by Cardinal Health
- DHL Supply Chain
- Ohio State University
- Ascena Retail Group
- Interhack
- Concert Production

Community Involvement

- Security MBA
- DefCon Goon
- Hak4Kidz
- Cool Tech Girls Columbus
- InfoSec Mentor

What is a Product Security Officer?

Full Stack InfoSec

- AppSec
- Audits
- Alerts
- Business Advocate
- CMDB
- Container Sec
- Consult on Contracts
- Define Requirements
- Design New Products
- Everything Crypto
- Harden Environments
- Incident Response
- Interface with Customers
- Interface with Vendors
- Logging & Monitoring
- Network Access
- Pair with Developers
- Pen Testing
- Policy Compliance
- PAM
- Product Assessments
- Reporting
- Risk Assessments
- Security Architecture
- Infra Vuln Management
- SIEM
- Strategic Roadmaps
- Teach Security Mindset
- Threat Hunting
- Threat Modeling
- WAF
- *+ So Much More!*

What is a Product Security Officer?

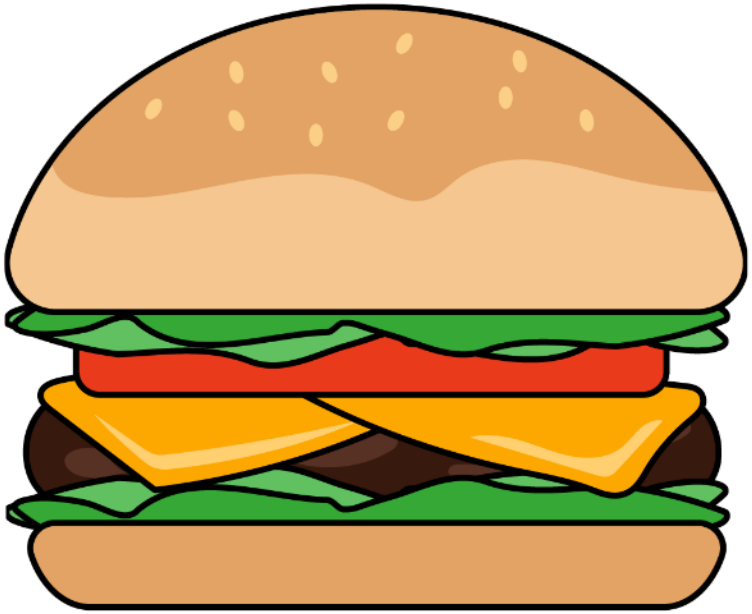
Full Stack InfoSec

- AppSec
- Audits
- Alerts
- Business Advocate
- CMDB
- Container Sec
- Consult on Contracts
- Define Requirements
- Design New Products
- Everything Crypto
- Harden Environments
- Incident Response
- Interface with Customers
- Interface with Vendors
- Logging & Monitoring
- Network Access
- Pair with Developers
- Pen Testing
- Policy Compliance
- PAM
- Product Assessments
- Reporting
- Risk Assessments
- Security Architecture
- Infra Vuln Management
- SIEM
- Strategic Roadmaps
- Teach Security Mindset
- Threat Hunting
- Threat Modeling
- WAF
- *+ So Much More!*

What is a Product Security Officer?

Full Stack InfoSec

- AppSec
- Audits
- Alerts
- Business Advocate
- CMDB
- Container Sec
- Consult on Contracts
- Define Requirements
- Design New Products
- Everything Crypto
- Harden Environments
- Incident Response
- Interface with Customers
- Interface with Vendors
- Logging & Monitoring
- Network Access
- Pair with Developers
- Pen Testing
- Policy Compliance
- PAM
- Product Assessments
- Reporting
- Risk Assessments
- Security Architecture
- Infra Vuln Management
- SIEM
- Strategic Roadmaps
- Teach Security Mindset
- Threat Hunting
- Threat Modeling
- WAF
- *+ So Much More!*



Single Pane of Glass

Why don’t we have a single pane of glass?

- Each product is varying in complex and uniqueness
- Each product has their own built in
- Proprietary and territorial over data
- Lack of standardization
- Maintaining an accurate CMDB is difficult.
- Focused on specialized areas
- etc, etc, etc.

So, what your saying is, it’s a pain.

- Won’t AI fix this?
- Isn’t there a product out there?

Why Use PowerBI

- Cost Effective
- Easy to learn (many free resources online)
- Powerful
- Vendor agnostic
- Easy implementation (O365)
- Access controls/row level security
- Automation
- Mobile platform available
- Simple integrations
- Highly customizable

Defining your Objective

Ask The Right Question (ATRQ)

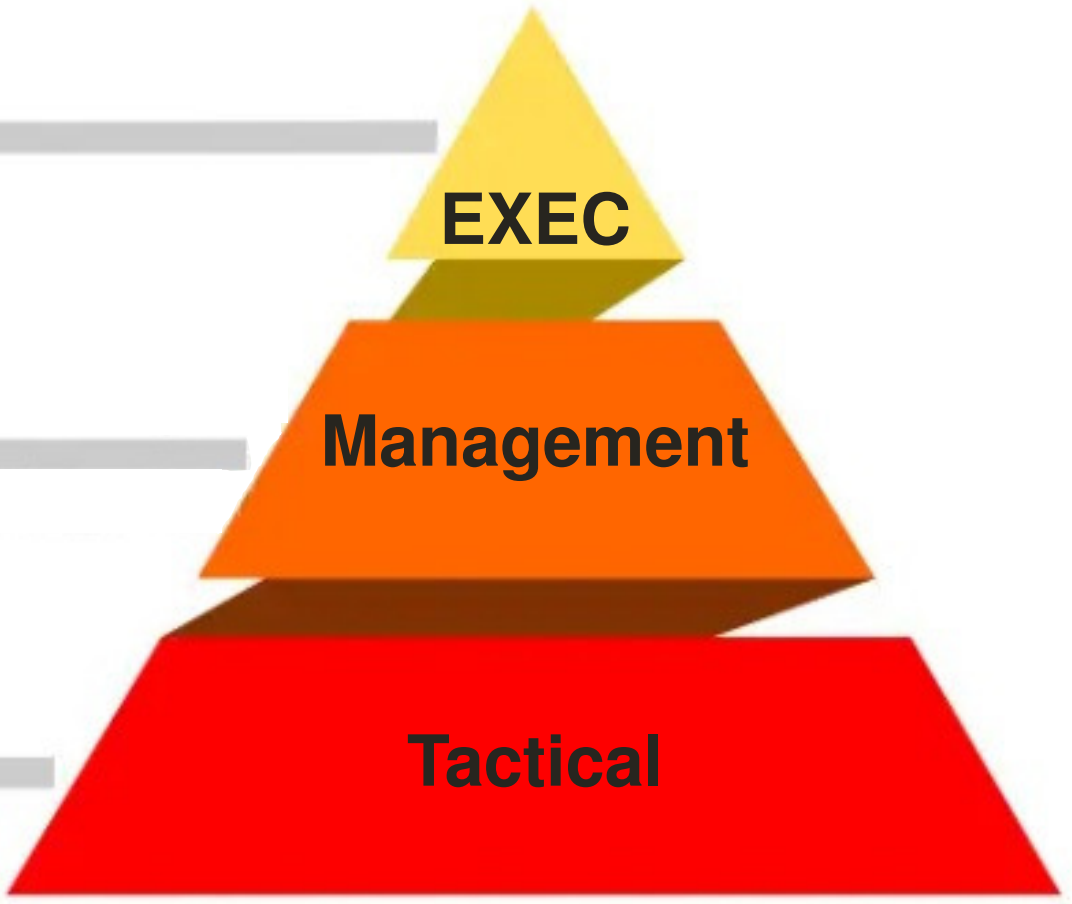
- What in the data is actionable?
- What does the data mean?
- Why does it matter?
- Are we doing a good job?
- What should I be planning for?
- **Does this matter?**
- **How bad is this?**
- **What is the risk?**
- **It this an emergency?**
- **Am I exposed?**

Dashboard Layers

Who:	C Suite/Board
What:	Division level roadmaps, budget allocations, overall status.
When:	Quarterly/6 Months

Who:	Tech Directors, Business Partners
What:	Product level sprint planning, resource alignment, backlog.
When:	Monthly

Who:	Tech Leads, Developers, etc.
What:	Technical details that are directly actionable.
When:	Weekly/Daily/Constant

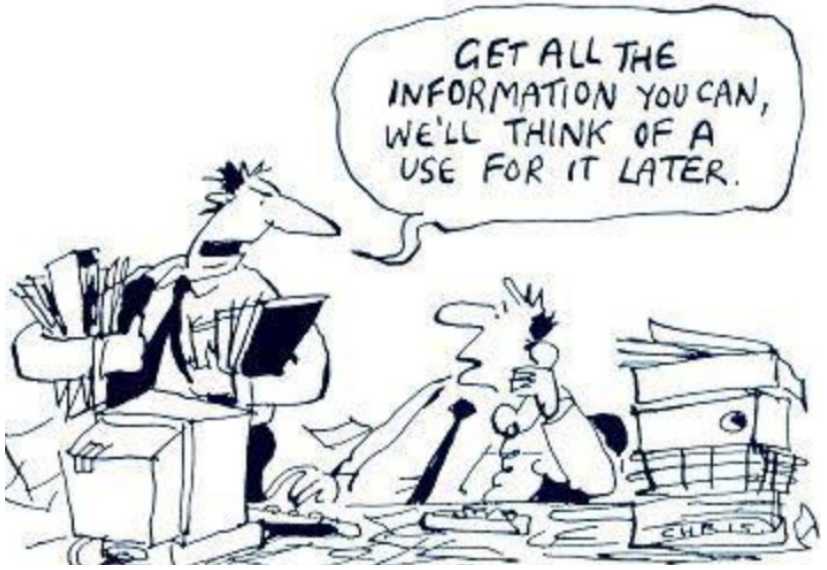


Diving for Data

Category	Data
AppSec	Scan Results
Code Repository	Library Listing
CMDB	Asset Inventory
Benchmarks	Configuration Violations
HR	Employee List
LMS	Training Compliance
Network Access	Firewall Rules
Server Sec	Scan Results
WAF	Configurations

**Not an exhaustive list*
Items in red will be focus areas

- Map your tools and the data you get out of them
- Consider how they all tie together and what's important
- Use standard exports, .csv, etc
- Save report format
- Make sure the process is repeatable
- Use automation where possible



Make A Map

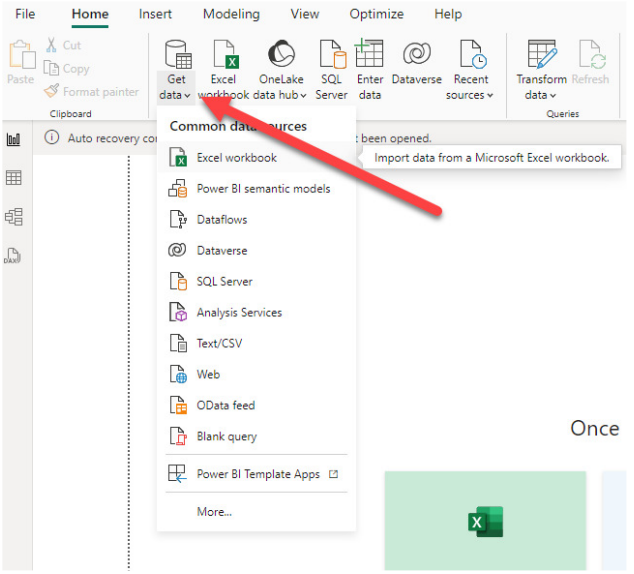
Is your CMDB a little lacking?

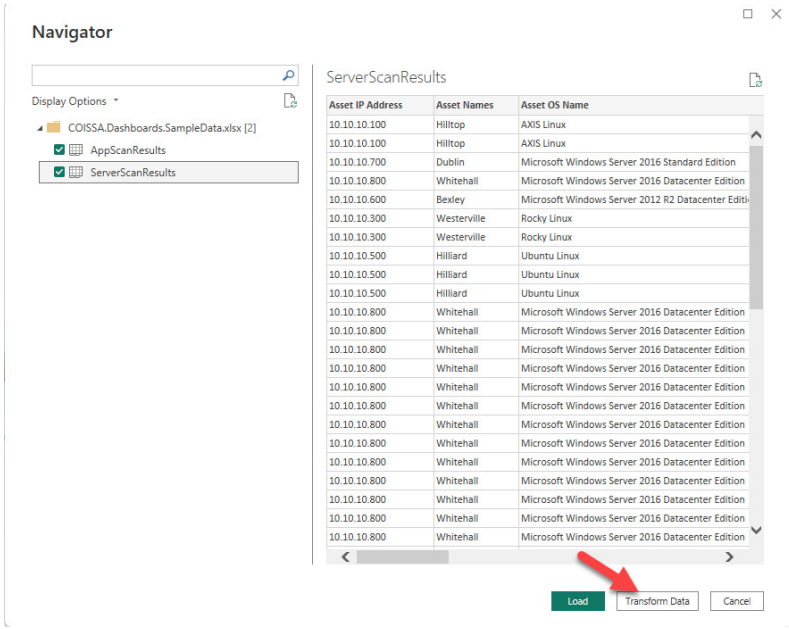
- Use your server vulnerability data to create a server list.
- Use your app scans to create an application list.
- Tie it together!

	Produc	Application Name	Environment	Server	Server IP	Database	Database IP	Team	Division
2	CBUS	Cbus1	Prod	10.10.10.600	Bexley	10.10.10.800	Whitehall	Chewbacca	Rebels
3	CBUS	Cbus2	Prod	10.10.10.600	Bexley	10.10.10.800	Whitehall	Chewbacca	Rebels
4	CBUS	CbusPortal	Prod	10.10.10.400	Blacklick	10.10.10.800	Whitehall	Chewbacca	Rebels
5	CBUS	Cbus1-S	Stage	10.10.10.700	Dublin	10.10.10.800	Whitehall	Chewbacca	Rebels
6	CBUS	Cbus2-S	Stage	10.10.10.700	Dublin	10.10.10.800	Whitehall	Chewbacca	Rebels
7	CBUS	CbusPortal-S	Stage	10.10.10.400	Blacklick	10.10.10.800	Whitehall	Chewbacca	Rebels
8	Eclipse	Eclip1	Prod	10.10.10.300	Westerville	10.10.10.800	Whitehall	Darth Vader	Empire
9	Eclipse	Eclip2	Prod	10.10.10.300	Westerville	10.10.10.800	Whitehall	Darth Vader	Empire
10	Eclipse	EclipPortal	Prod	10.10.10.400	Blacklick	10.10.10.800	Whitehall	Darth Vader	Empire
11	Hello	HW1-D	Dev	10.10.10.500	Hilliard	10.10.10.800	Whitehall	Yoda	Jedi
12	Hello	HW2-D	Dev	10.10.10.500	Hilliard	10.10.10.800	Whitehall	Yoda	Jedi
13	Hello	HWPortal-D	Dev	10.10.10.400	Blacklick	10.10.10.800	Whitehall	Yoda	Jedi
14	Hello	HW1	Prod	10.10.10.200	Reynoldsburg	10.10.10.800	Whitehall	Yoda	Jedi
15	Hello	HW2	Prod	10.10.10.200	Reynoldsburg	10.10.10.800	Whitehall	Yoda	Jedi
16	Hello	HWPortal	Prod	10.10.10.400	Blacklick	10.10.10.800	Whitehall	Yoda	Jedi
17	Hello	HW1-S	Stage	10.10.10.100	Hilltop	10.10.10.800	Whitehall	Yoda	Jedi

Getting Data into PowerBI

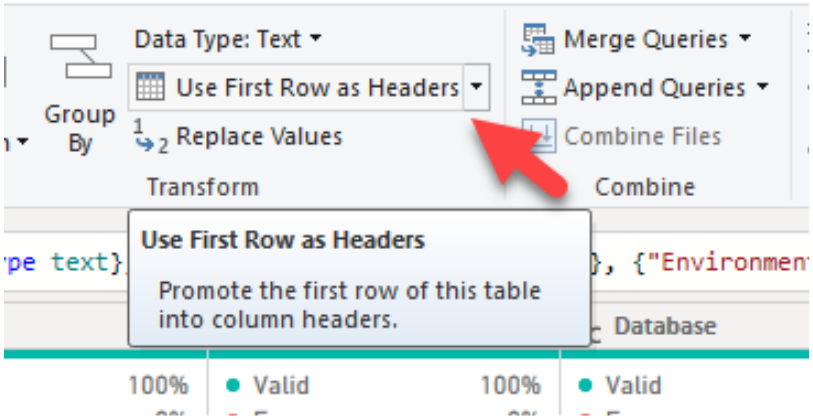
- Use “Get Data” to import
- Select Tables
- Use the “Transform Data” function on initial setup to clean up data instead of “Load”

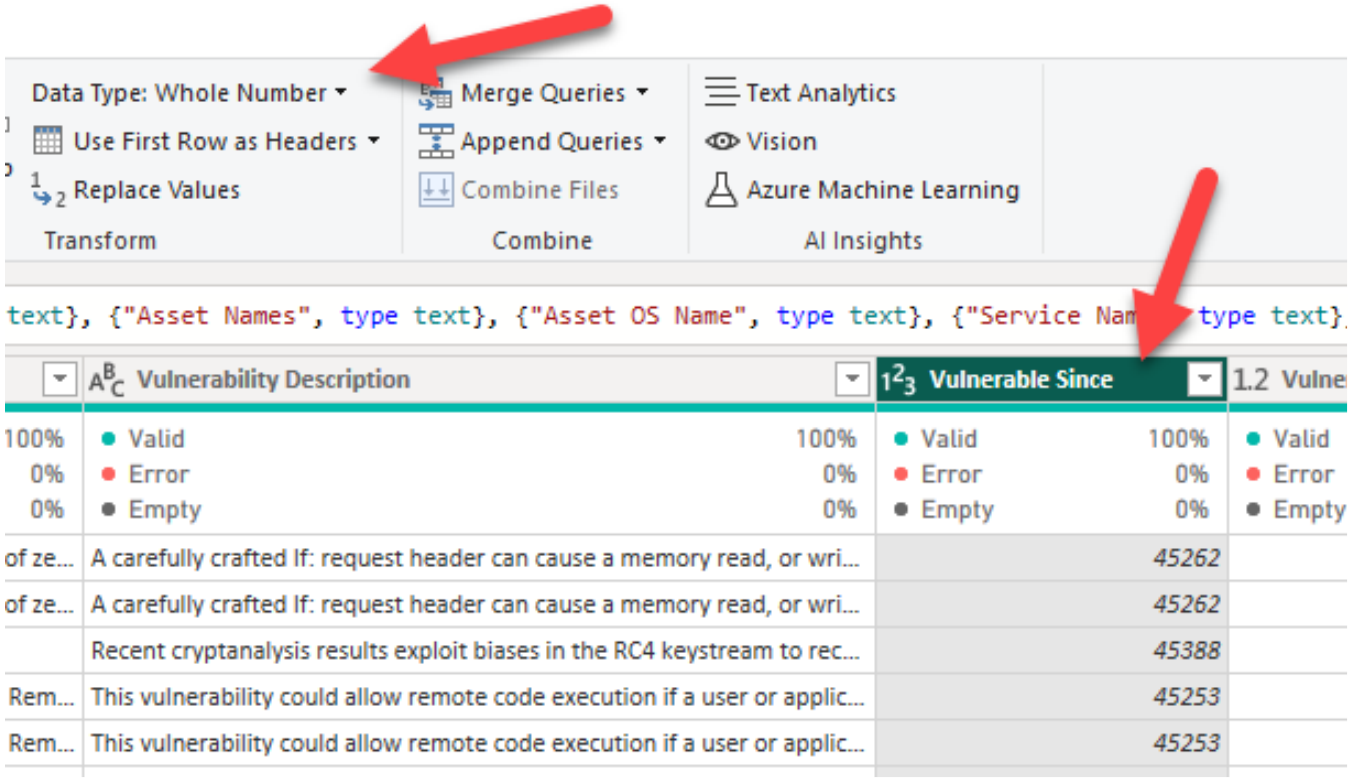




Transform Data

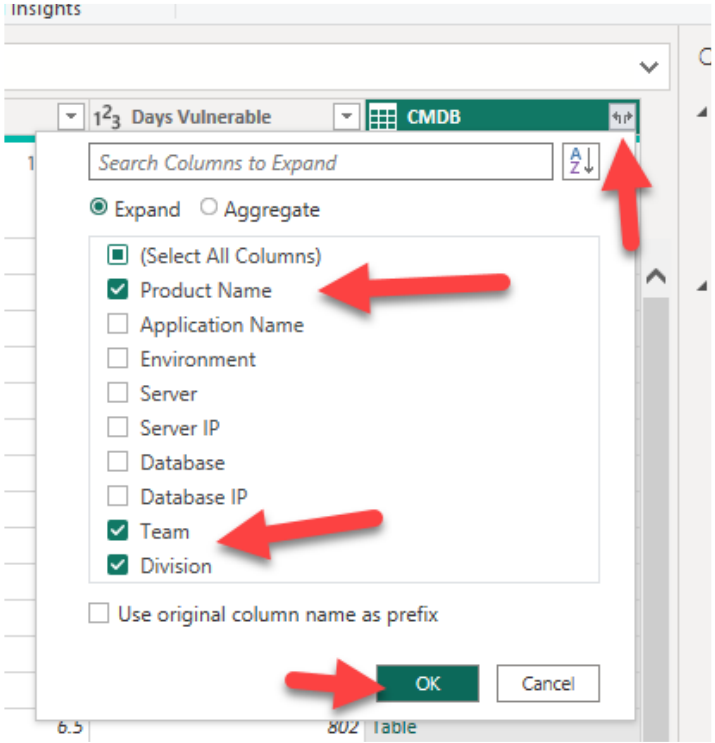
- Correct any formatting issues.
- Promote headers
- Name Sheets

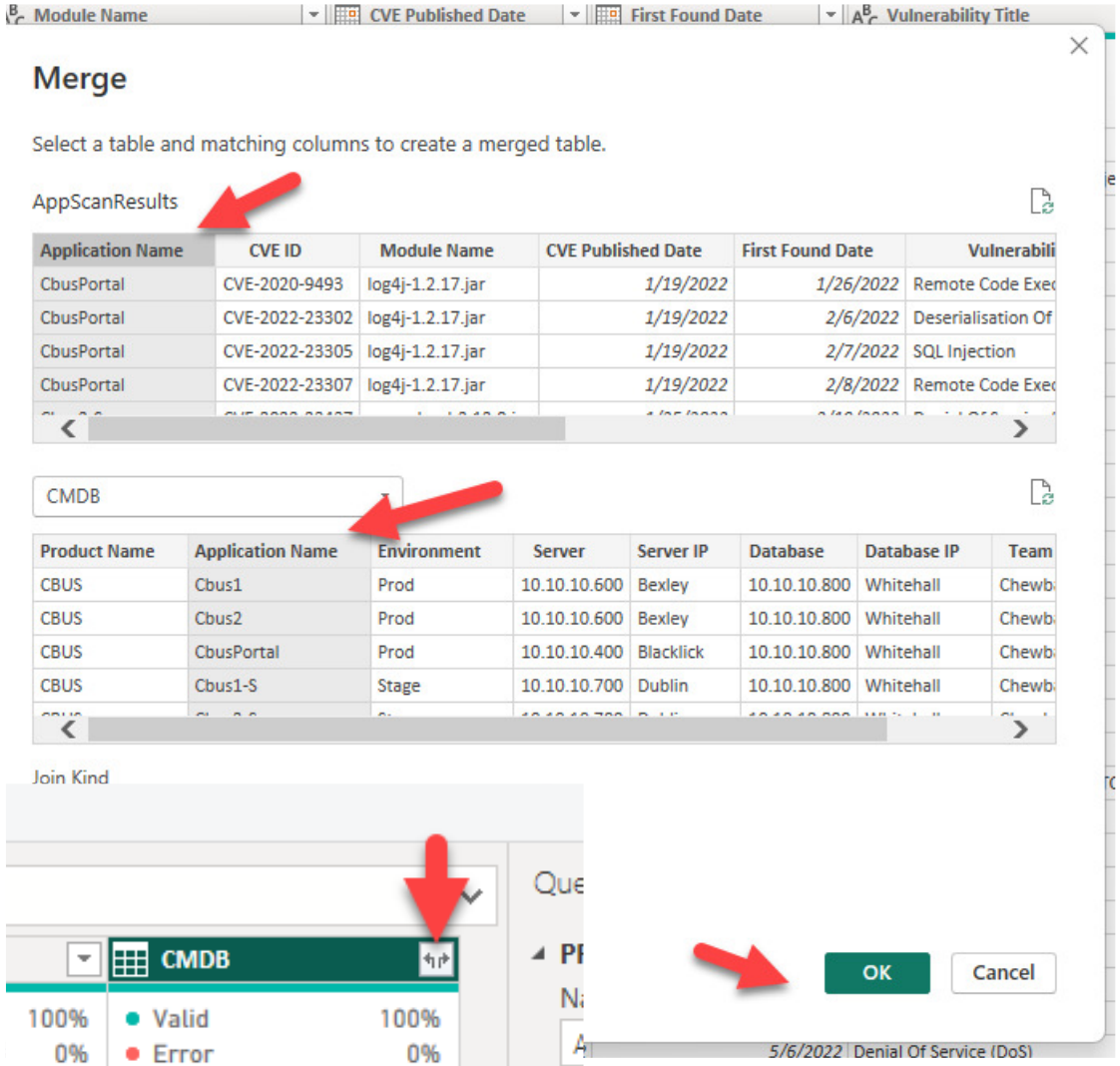




Transform Data

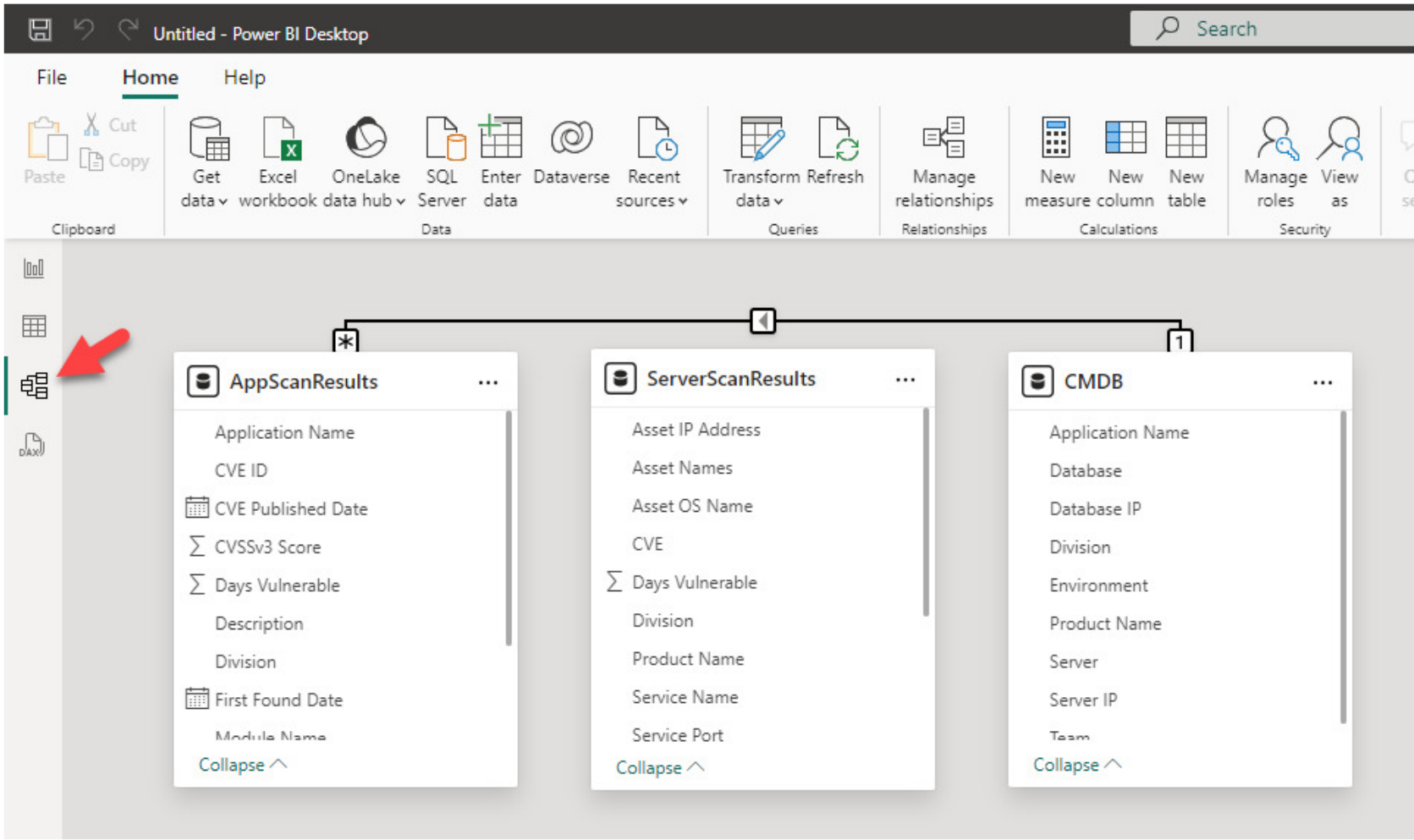
- Merge Tables to tie together.
- Select Column with common criteria.
- Expand the query.





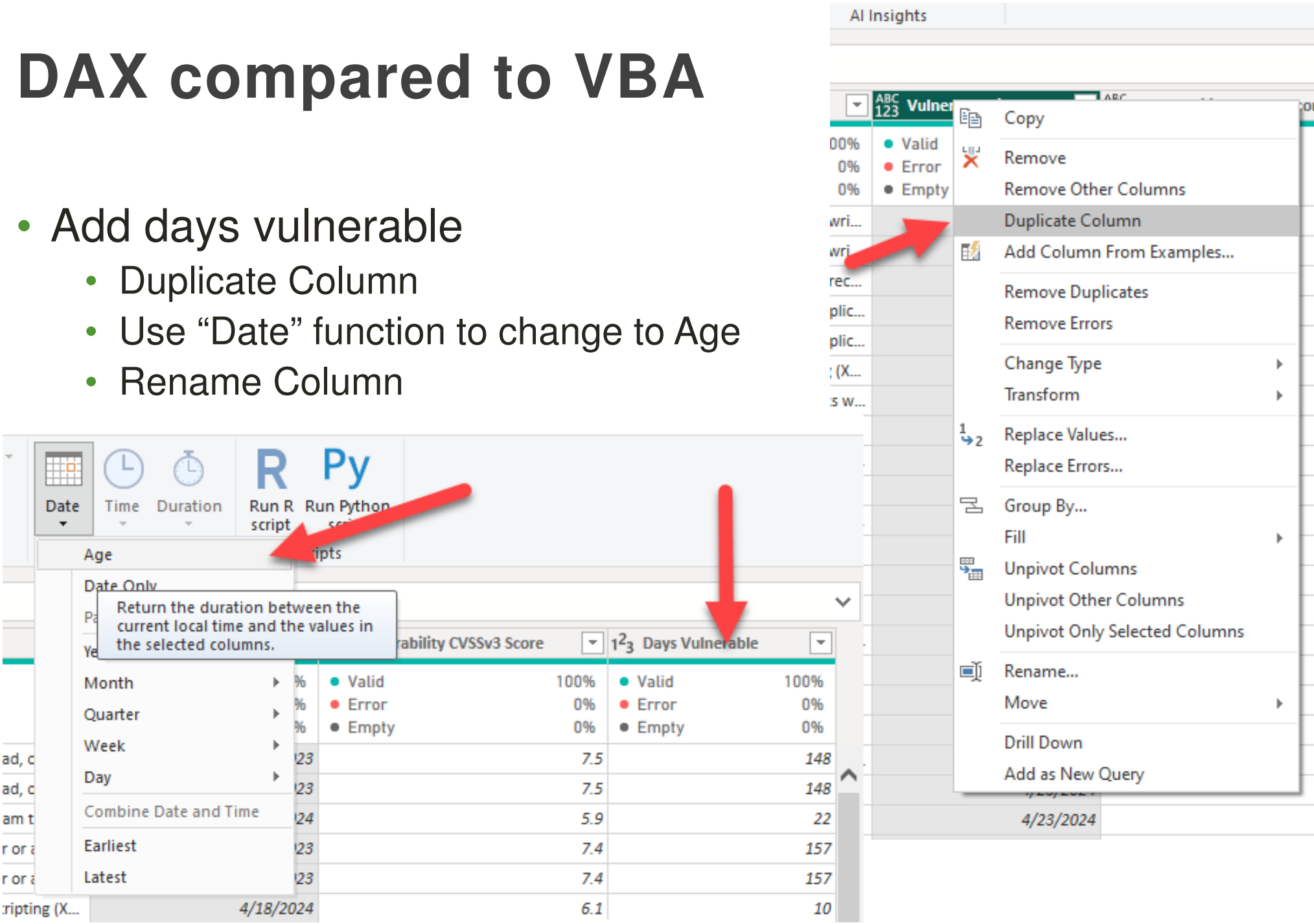
Transform Data

- You can also link tables in the Model View.



DAX compared to VBA

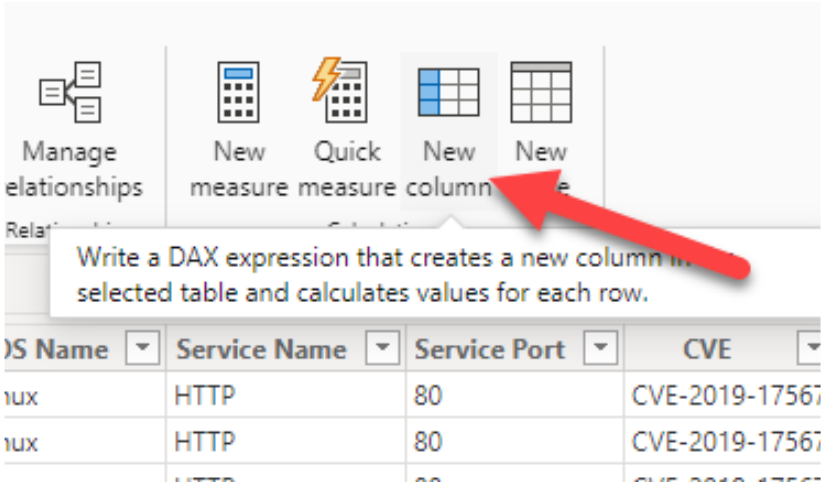
- Add days vulnerable
  - Duplicate Column
  - Use “Date” function to change to Age
  - Rename Column



DAX compared to VBA

- Use Table view to add a custom severity
- Add Column
- Smaple Formula

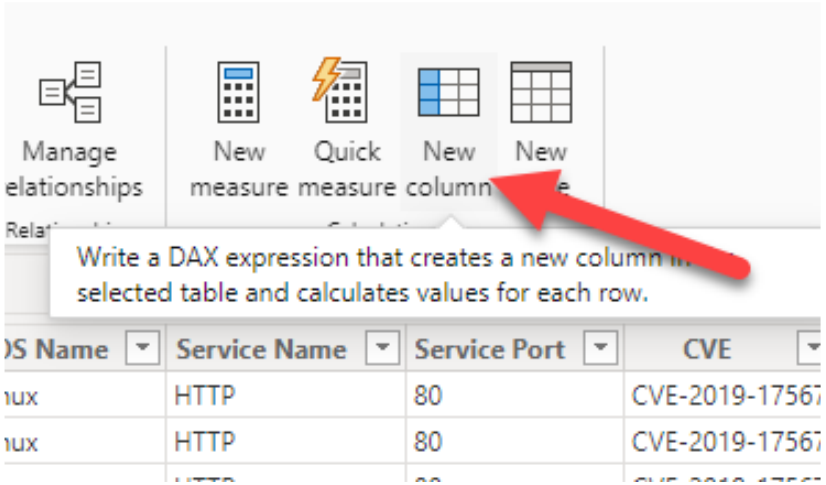
```
Custom Severity =
if('AppScanResults'[CVSSv3 Score] > 9.0, "Critical",
if('AppScanResults'[CVSSv3 Score] > 7.0, "High",
if('AppScanResults'[CVSSv3 Score] > 4.0, "Medium",
if('AppScanResults'[CVSSv3 Score] > 0, "Low",
"Informational"))))
```



DAX compared to VBA

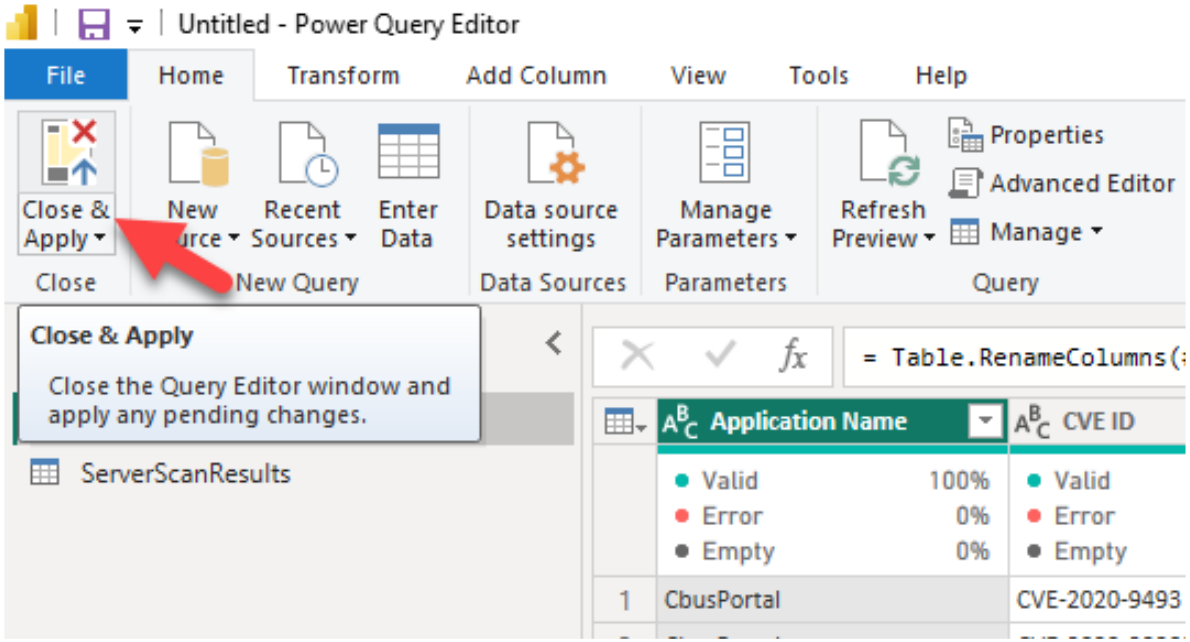
- Add an SLA
- Add Column
- Sample Formula

```
SLA =
if(AND('ServerScanResults'[Custom Severity]= "Critical",
'ServerScanResults'[Days Vulnerable]>15), "Incompliant",
if(AND('ServerScanResults'[Custom Severity] = "High", 'ServerScanResults'[Days
Vulnerable]>15), "Incompliant",
if(AND('ServerScanResults'[Custom Severity] = "Medium",
'ServerScanResults'[Days Vulnerable]>31), "Incompliant",
 "Compliant")))
```



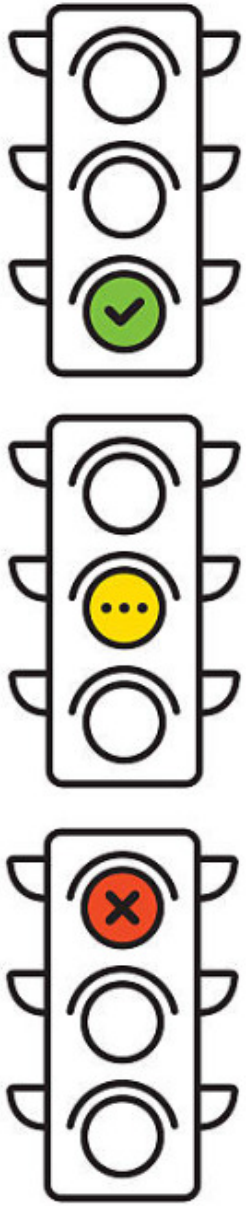
Transform Data

- When done, use “Close & Apply”
- Refresh when back in editor



Metrics

- Many infosec professionals agree, this is hard.
- Almost every infosec professional has a different opinion on what the metrics should be.
- **If you don't have defined metrics, make up your own!**
- Draw a line in the sand and stick to it, until it makes sense to move it.
  - How many vulnerabilities per _____?
  - How many of them are outside the SLA to remediate?
  - Critical or High Vulnerabilities over ___ days old?
- Make a stoplight
  - 20+ per ___ = Red
  - 10+ per ___ = Yellow
  - 10- per ___ = Green



Metrics - Yea, but…hi Angela!

- You're not wrong.
- When everything is a priority, nothing is.
- Stop over thinking it.
- Don't sit at 0% trying to solve for 100%, get the 80% win and make incremental improvements.
- We all have vulnerabilities; we're all going to **always** have vulnerabilities. It's never going to be perfect.
- Imperfect action is better than perfect inaction.
- Use good judgement.

Just Do It!

Sample Dashboard - Tactical

Division
- [ ] Empire

Team
- [ ] Chewbacca
- [ ] Darth Maul
- [x] Darth Vader

Application Vulnerabilities

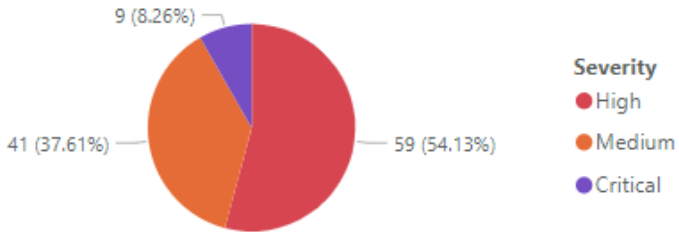
Application Vulnerabilities by App

Application Name	Critical	High	Medium	Total
Eclip1	3	23	13	**39**
Eclip2	3	19	10	**32**
EclipPortal	3	17	18	**38**
Total	**9**	**59**	**41**	**109**

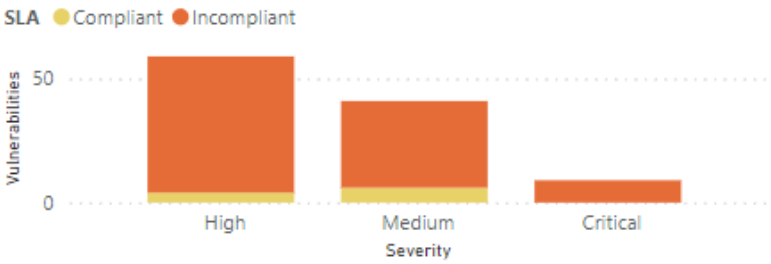
New This Week

Application Name	Custom Severity	Vulnerability Title
Eclip1	High	Open Redirect
Eclip2	High	Open Redirect
EclipPortal	High	Open Redirect
EclipPortal	Medium	Denial Of Service (DoS)
EclipPortal	Medium	Observable Discrepancy

Vulnerabilities by Severity



Vulnerabilities by Severity and SLA



Application Vulnerability Export

Division	Product Name	Application Name	Team	Module Name	Custom Severity	Days Vulnerable	CVE ID	Vulnerability Title	Description
Empire	Eclipse	Eclip1	Darth Vader	amqp-client-5.17.1.jar	High	174	CVE-2023-46120	Denial Of Service (DoS)	amqp-client is vul `ConnectionFactor Of-Memory (OOM
Empire	Eclipse	Eclip2	Darth Vader	amqp-client-5.17.1.jar	High	183	CVE-2023-46120	Denial Of Service (DoS)	amqp-client is vul `ConnectionFactor Of-Memory (OOM
Empire	Eclipse	EclipPortal	Darth Vader	amqp-client-5.17.1.jar	High	176	CVE-2023-46120	Denial Of Service (DoS)	amqp-client is vul `ConnectionFactor Of-Memory (OOM
Empire	Eclipse	Eclip1	Darth Vader	antisamy-1.5.8.jar	Medium	58	CVE-2024-23635	Cross Site Scripting (XSS)	antisamy is vulner

3
Application Count

263.39
Average Days Old

Sample Dashboard - Tactical

Division
- [ ] Rebels

Team
- [x] Chewbacca
- [ ] Darth Maul
- [ ] Darth Vader

Server Vulnerabilities

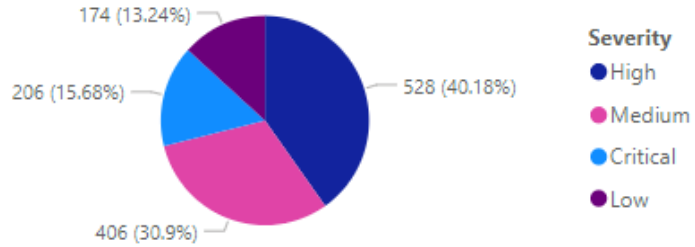
Server Vulnerabilities by Product

Product Name	Critical	High	Low	Medium	Total
Bye	98	208	48	154	**508**
CBUS	4	46	26	34	**110**
CLE	4	46	26	34	**110**
Eclipse	1	10	13	15	**39**
Hello	98	208	48	154	**508**
Moon	1	10	13	15	**39**
Total	**206**	**528**	**174**	**406**	**1314**

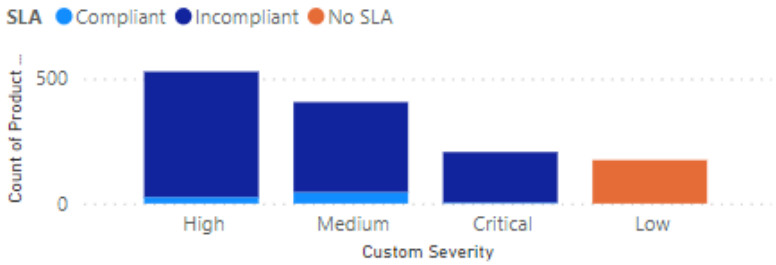
New This Week

Product Name	Custom Severity	CVE

Product by Severity



Count of Product Name by Custom Severity and SLA



Server Vulnerability Export

Division	Product Name	Team	Asset IP Address	Asset Names	Custom Severity	Days Vulnerable	CVE	Vulnerability Title
Empire	Eclipse	Darth Vader	10.10.10.300	Westerville	Medium	10	CVE-2014-6071	jQuery Vulnerability: CVE-2014-6071
Empire	Eclipse	Darth Vader	10.10.10.300	Westerville	Medium	10	CVE-2015-9251	jQuery Vulnerability: CVE-2015-9251
Empire	Eclipse	Darth Vader	10.10.10.300	Westerville	Medium	10	CVE-2020-11022	jQuery Vulnerability: CVE-2020-11022
Empire	Eclipse	Darth Vader	10.10.10.400	Blacklick	Critical	150	CVE-2023-37920	Red Hat: CVE-2023-37920: python-certifi: Removal of
Empire	Eclipse	Darth Vader	10.10.10.400	Blacklick	High	12	CVE-2023-4408	Red Hat: CVE-2023-4408: bind9: Parsing large DNS m

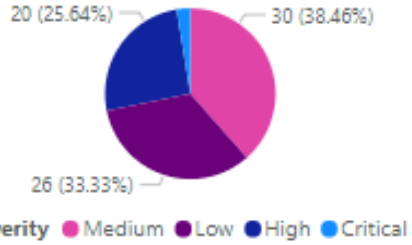
14
Count of Asset IP Add...

376.32
Average of Days Vulne...

Sample Dashboard - Management

Server Vulnerabilities

Vulns by Severity

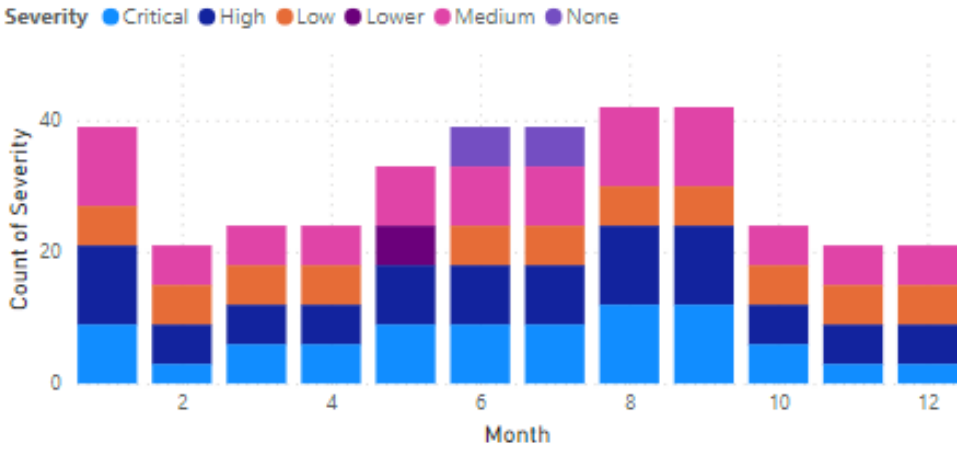


Team	Critical	High	Total
Darth Maul	150	1251	**1401**
Darth Vader	150	1251	**1401**
Total	**300**	**2502**	**2802**

SLA Status

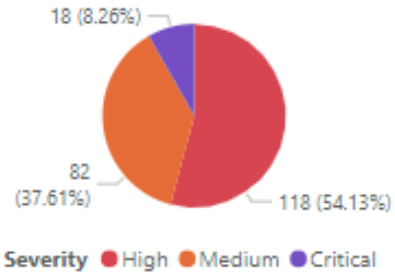
Team	Critical	High	Total
Darth Vader	150	1239	**1389**
Darth Maul	150	1239	**1389**
Total	**300**	**2478**	**2778**

Historical Server Vulns Severity by Month



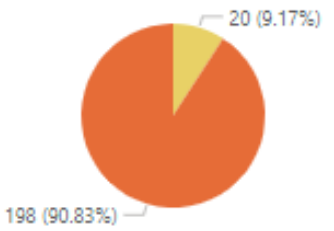
Application Vulnerabilities

Vulns by Severity



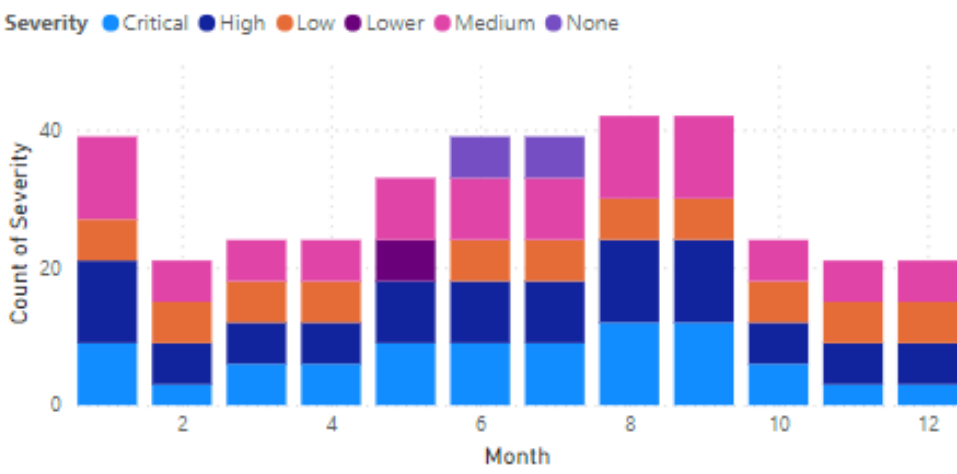
Team	Critical	High	Total
Darth Maul	9	59	**68**
Darth Vader	9	59	**68**
Total	**18**	**118**	**136**

SLA Status

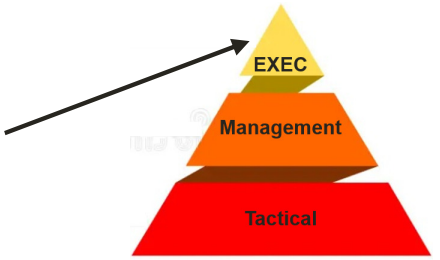


Team	Critical	High	Total
Darth Maul	9	55	**64**
Darth Vader	9	55	**64**
Total	**18**	**110**	**128**

Historical App Vulns Severity by Month

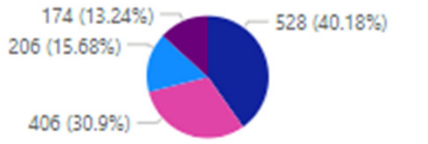


Sample Dashboard - Executive



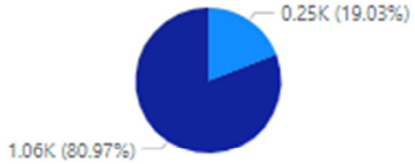
Server Vulnerabilities

Vulns by Severity



Division	Critical	High	Total
Empire	300	2502	**2802**
Rebels	1036	9732	**10768**
Jedi	121372	191708	**313080**
Total	**122708**	**203942**	**326650**

SLA Status



Division	Critical	High	Total
Empire	300	2478	**2778**
Jedi	121332	191452	**312784**
Rebels	1036	9684	**10720**
Total	**122668**	**203614**	**326282**

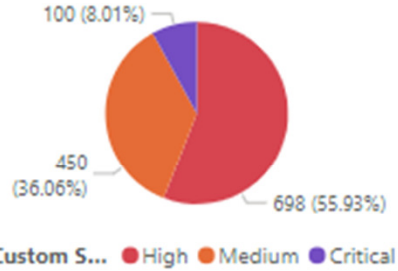
Highest Risk Servers

Asset IP Address	Asset Names	Team
10.10.10.100	Hilltop	Yoda
10.10.10.200	Reynoldsburg	Yoda
10.10.10.400	Blacklick	Chewbacca
10.10.10.400	Blacklick	Darth Vader

Empire Jedi Rebels

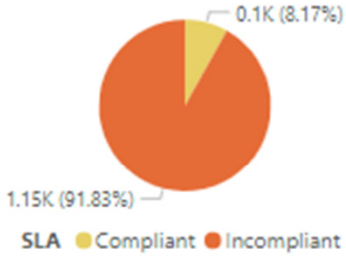
Application Vulnerabilities

Vulns by Severity



Division	Critical	High	Total
Empire	18	118	**136**
Jedi	54	390	**444**
Rebels	28	190	**218**
Total	**100**	**698**	**798**

SLA Status



Division	Critical	High	Total
Empire	18	110	**128**
Jedi	54	364	**418**
Rebels	28	170	**198**
Total	**100**	**644**	**744**

Highest Risk Apps

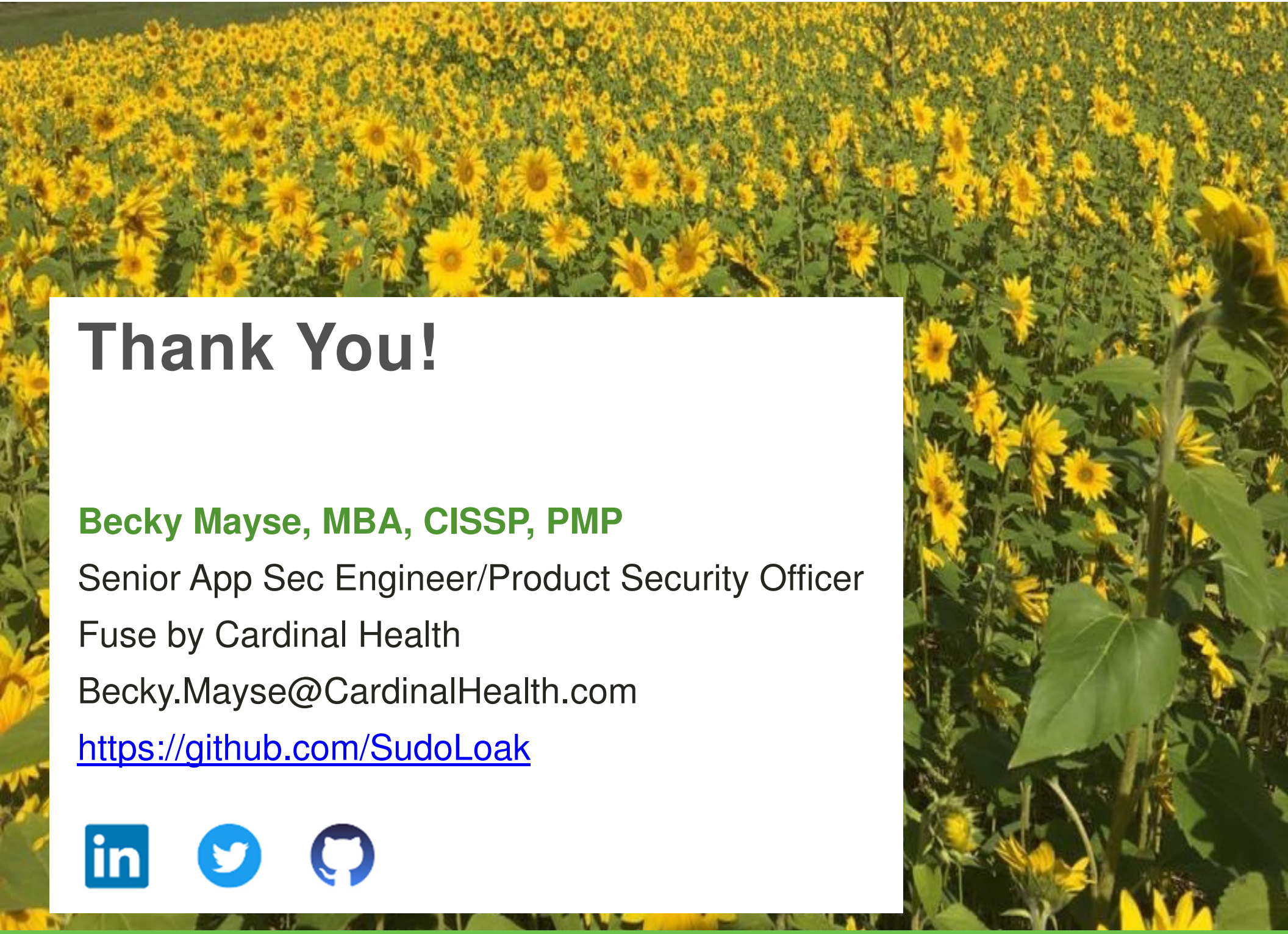
Application Name	Division	Team
Cbus1	Rebels	Chewbacca
Cbus2-S	Rebels	Chewbacca
CbusPortal	Rebels	Chewbacca
CLE1	Rebels	Han Solo

Empire Jedi Rebels

Going Further

- Row Level Permissions
- Trend Tracking
- Embedding
  - PowerPoint
  - Internal Team Sites
- Automatic Sprint Card Creation
- Automation
- Microsoft Learn - PowerBI Training

Get your starter kit at: https://github.com/SudoLoak



Thank You!

Becky Mayse, MBA, CISSP, PMP

Senior App Sec Engineer/Product Security Officer

Fuse by Cardinal Health

Becky.Mayse@CardinalHealth.com

https://github.com/SudoLoak