FIREEYE™

CYBER DEFENSE SUMMIT 2019

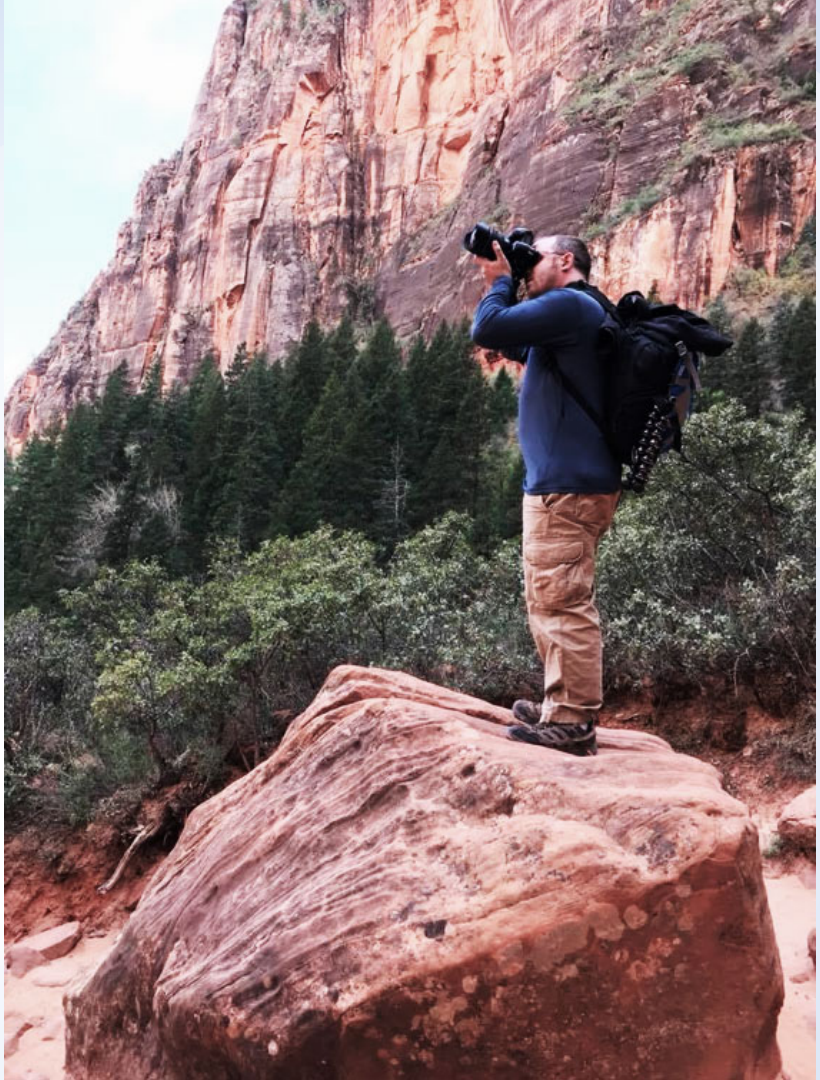
Practical SOC Metrics

Presented by Carson Zimmerman

In collaboration with Chris Crowley

About Carson

- Worked in Security Operations for ~15 years
- SOC Engineering Team Lead @ Microsoft
- Previously SOC engineer, analyst & consultant @ MITRE
- Check out my book if you haven't already: https://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center



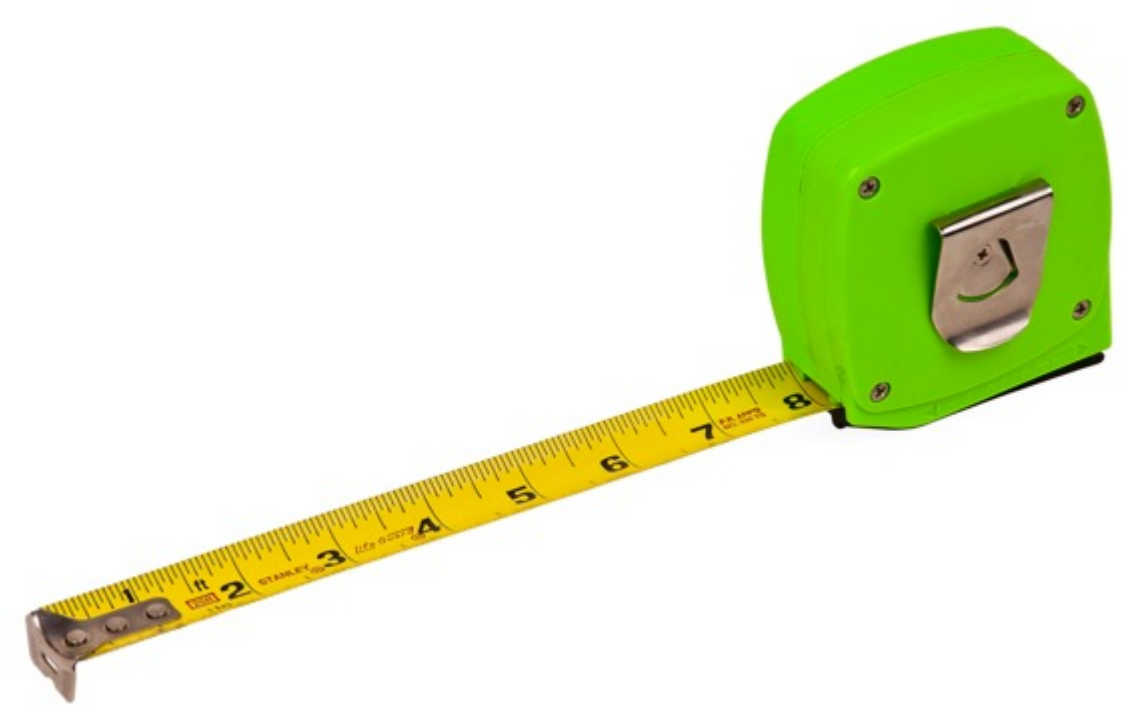
About Chris

- Independent Consultant (Montance.com)
- SANS Institute
  - Senior Instructor & Course Author
  - SOC Survey Author (2017, 2018, 2019)
  - Security Operations Summit Chair
- SOC-class.com – Security Operations Class on building & running a SOC
- Engagements with Defense, Education, Energy, Financial, IT, Manufacturing, Science, Software Development, …

Pick Something You Love…

http://disney.wikia.com/wiki/File:TS2_Jessie_hugs_Woody.jpg

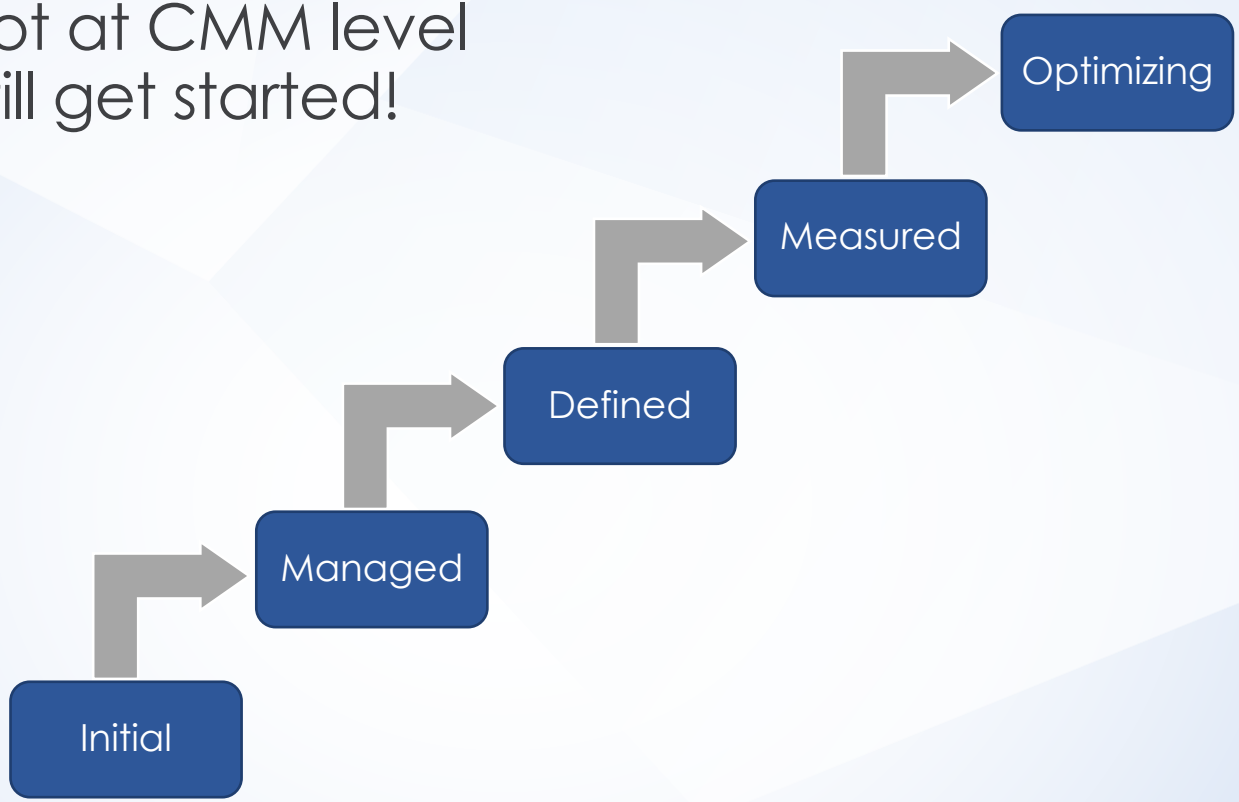
…And Measure It



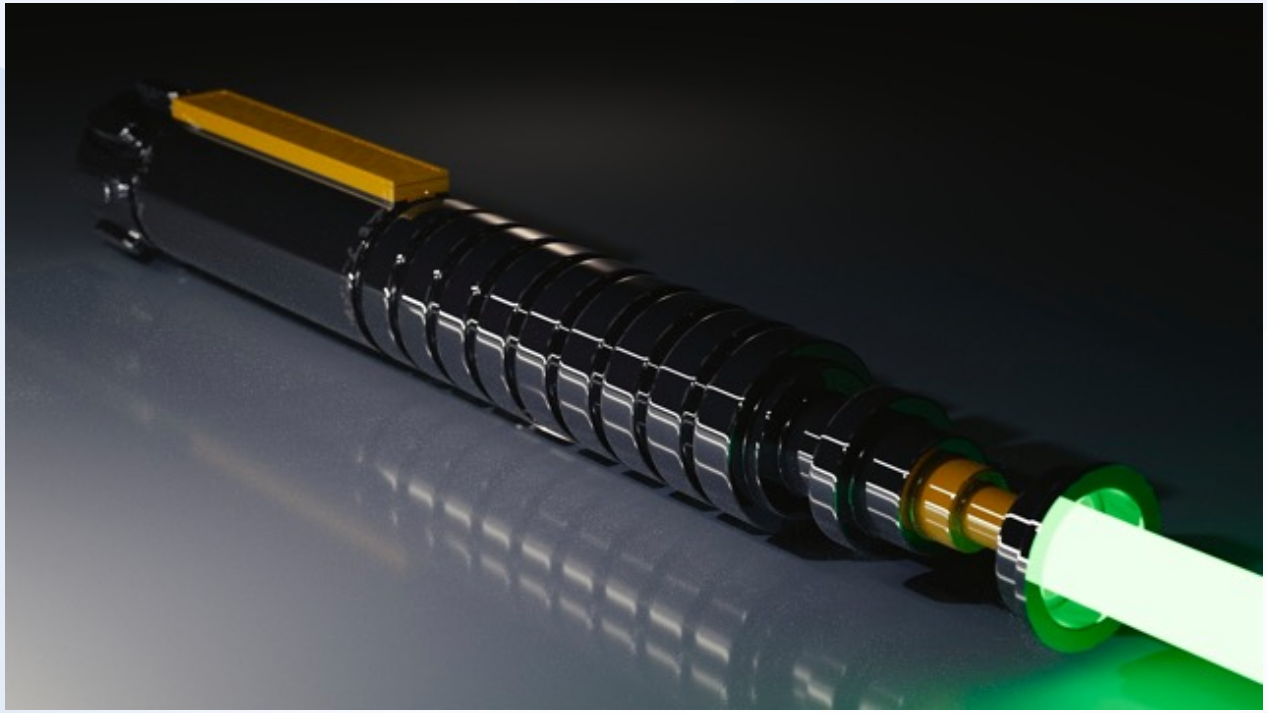
https://en.wikipedia.org/wiki/Tape_measure#/media/File:Measuring-tape.jpg

Measuring Things Usually Drives Change

Even if you're not at CMM level >= 3, you can still get started!



Metrics are Like Lightsabers



https://www.maxpixel.net/Laser-Sword-Lightsaber-Green-Science-Fiction-Space-1675211

They Can Be Used for Good…

https://www.scifinow.co.uk/blog/top-5-star-wars-scenes-we-want-to-see-on-blu-ray/

…And for Evil

http://starwars.wikia.com/wiki/File:UnidentifiedClan-RotS.jpg

Top Tips

- Metric data should be free and easy to calculate
  - ½ of all SOCs collect metrics according to SANS SOC survey 2017 & 2018
- There should be a quality measure that compensates for perversion
  - Especially when there's a time based metric!
- Metrics aren't (necessarily) Service Level Objectives (SLOs)
  - The metric is there to help screen, diagnose, and assess performance
  - Don't fall into a trap of working to some perceived metric objective
  - Any metric should have an intended effect, and realize the measurement and calculation isn't always entirely valid
- Expectations, messaging, objectives- all distinct!

Data Sources

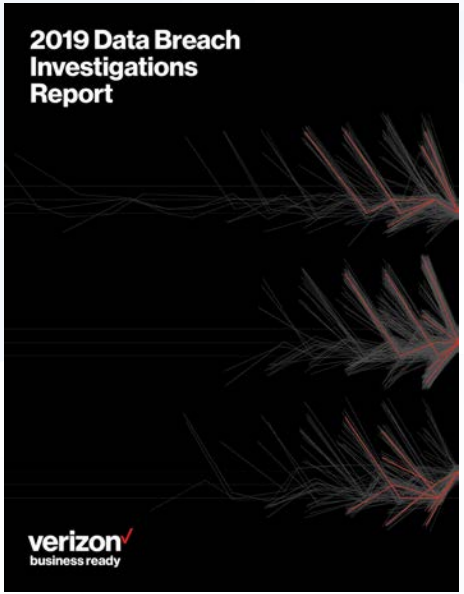
- SOC Ticketing/case management system
- SIEM / analytic platform / EDR- anywhere analysts create detections, investigate alerts
- SOC code repository
- SOC budget
  - CAPEX including hardware & software
  - OPEX including people & cloud
- Enterprise asset management systems
- Vulnerability management

https://video-images.vice.com/articles/5b02e43f187df600095f5e7c/lede/1526917810059-GettyImages-159825349.jpeg

Existing Resources

- SOC CMM: measure your SOC top to bottom
- VERIS Framework: track your incidents well
- SANS SOC Survey: recent polls from your peers

https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

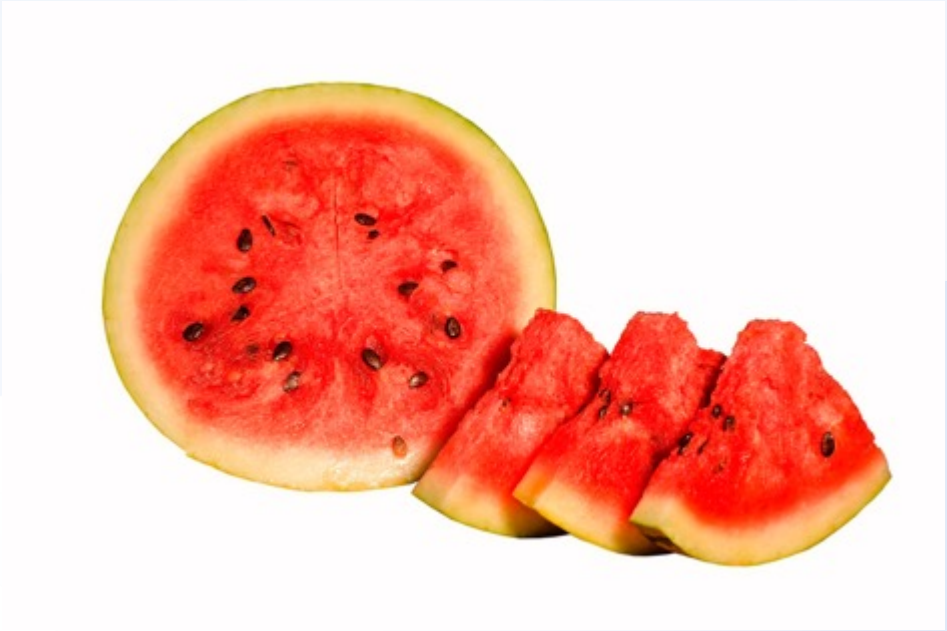


https://enterprise.verizon.com/resources/reports/dbir/

Example Metrics

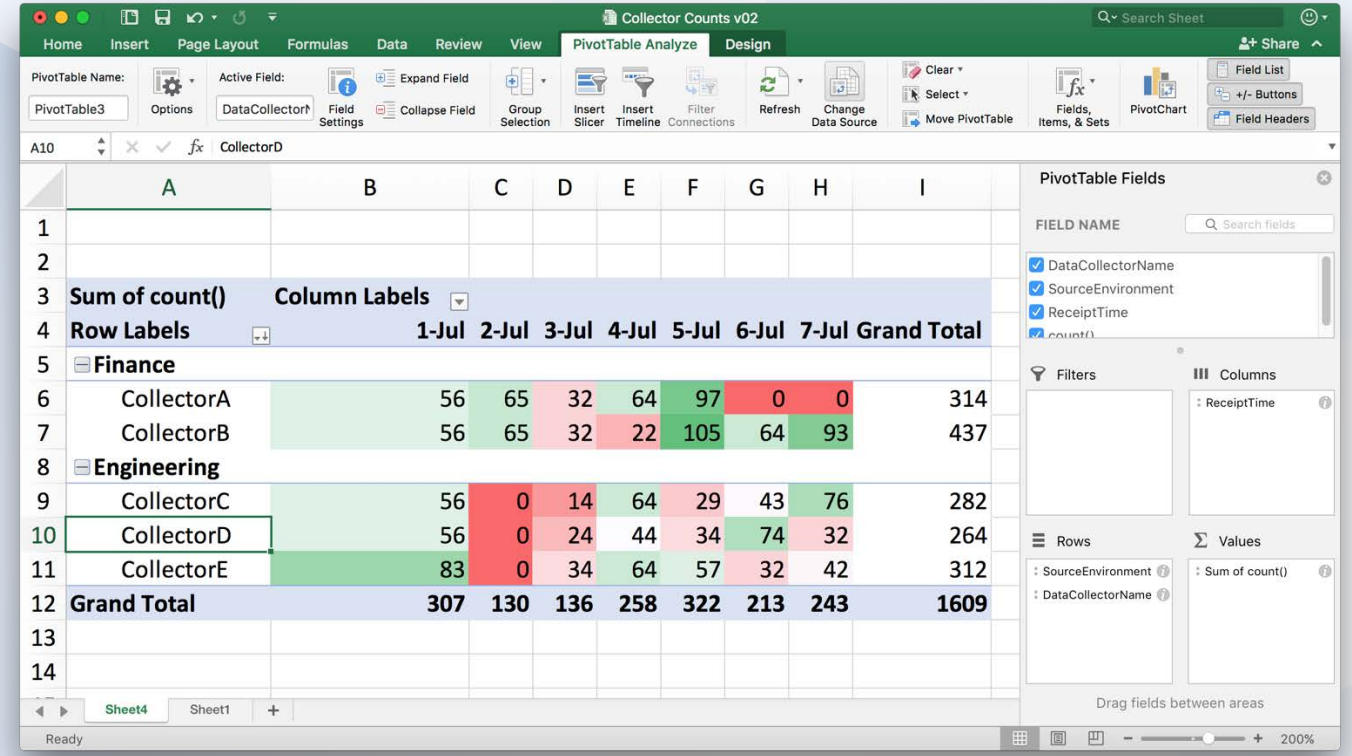
Metric Focus 1: Data Feed Health

- Is it "green"
- What is green anyway?
- Just because it's up doesn't mean all is well
  - Delays in receipt
  - Drops
    - Temporary
    - Permanent
  - Blips



https://en.wikipedia.org/wiki/Watermelon#/media/File:Watermelon_cross_BNC.jpg

5 Minutes' of Work: Which Sensors are Down



Sum of count()	Column Labels							
Row Labels	1-Jul	2-Jul	3-Jul	4-Jul	5-Jul	6-Jul	7-Jul	Grand Total
Finance								
CollectorA	56	65	32	64	97	0	0	314
CollectorB	56	65	32	22	105	64	93	437
Engineering								
CollectorC	56	0	14	64	29	43	76	282
CollectorD	56	0	24	44	34	74	32	264
CollectorE	83	0	34	64	57	32	42	312
Grand Total	307	130	136	258	322	213	243	1609

15 Minutes' More Work: Automated Detection of Downed Feeds

	OLD COUNT	NEW COUNT	OLD DEVICES	NEW DEVICES	IS BROKEN
Collector A	2230	2120	1002	934	No
Collector B	1203	1190	894	103	Yes
Collector C	3203	3305	342	325	No
Collector D	1120	305	569	234	Yes
Collector E	342	102	502	496	Yes

- Automate detection of dead, slow or lagging collectors
  - Query for old data (1-7 days ago) vs recent data (last 24 hours)
  - Look for major dips or drops: done through query logic
- Consider human eyes on: daily or weekly

Metric Focus 2: Coverage

Dimensions:

1. Absolute number *and* percentage of coverage per compute environment/enclave/domain
2. Kill chain or ATT&CK cell
3. Layer of the compute stack (network, OS, application, etc.)
4. Device covered (Linux, Windows, IoT, network device)

Tips:

1. Never drive coverage to 100%
   - You don't know what you don't know
   - Always a moving target
2. There is always another environment to cover, customer to serve
3. There will always be more stones to turn over; don't ignore any of these dimensions

Managed vs Wilderness

- Percentage of systems "managed":
  - Inventoried?
  - Tied to an asset/business owner?
  - Tied to a known business/mission function?
  - Subject to configuration management?
  - Assigned to a responsible security team/POC?
  - Risk assessed?
- If all are yes: it's managed
- If not: it's "wilderness"
- SOC observed device counts help identify "unknown unknowns" in the wilderness

Monitoring SLAs/SLOs

- SLA: Agreement = monetary (or other penalty) for failing to meet
- SLO: Objective = no specific penalty agreed to for failing to meet
- Institution & missions specific where these need to be set in place
- Don't monitor everything the same way!
  - Instrumentation, custom detections, response times, retention

Basic Service

- Host EDR
- Network logs
- Standard mix of detections
- Yearly engagement

Advanced Service

- Basic, plus:
- 3 application logs
- 1 focused detection/quarter
- Quarterly engagement

Metric Focus 3: Scanning and Sweeping

Basic

- # + % of known on prem & cloud assets scanned for vulns
- Amount of time it took to compile vulnerability/risk status on covered assets during last high CVSS score "fire drill"
- Number of people needed to massage & compile these numbers monthly

Advanced

- Time to sweep and compile results for a given vuln or IOC:
  - A given domain/forest identity plane
  - Everything Internet-facing
  - All user desktop/laptops
  - Everything
- # + % of assets you can't/don't cover (IoT, network devices, etc.)

Metric Focus 4: Your Analytics

Basics:

1. Name
2. Description
3. Kill chain mapping
4. ATT&CK cell mapping
5. Depends on which data type(s) (OS logs, Netflow, etc.)
6. Covers which environments/enclave
7. Created- who, when

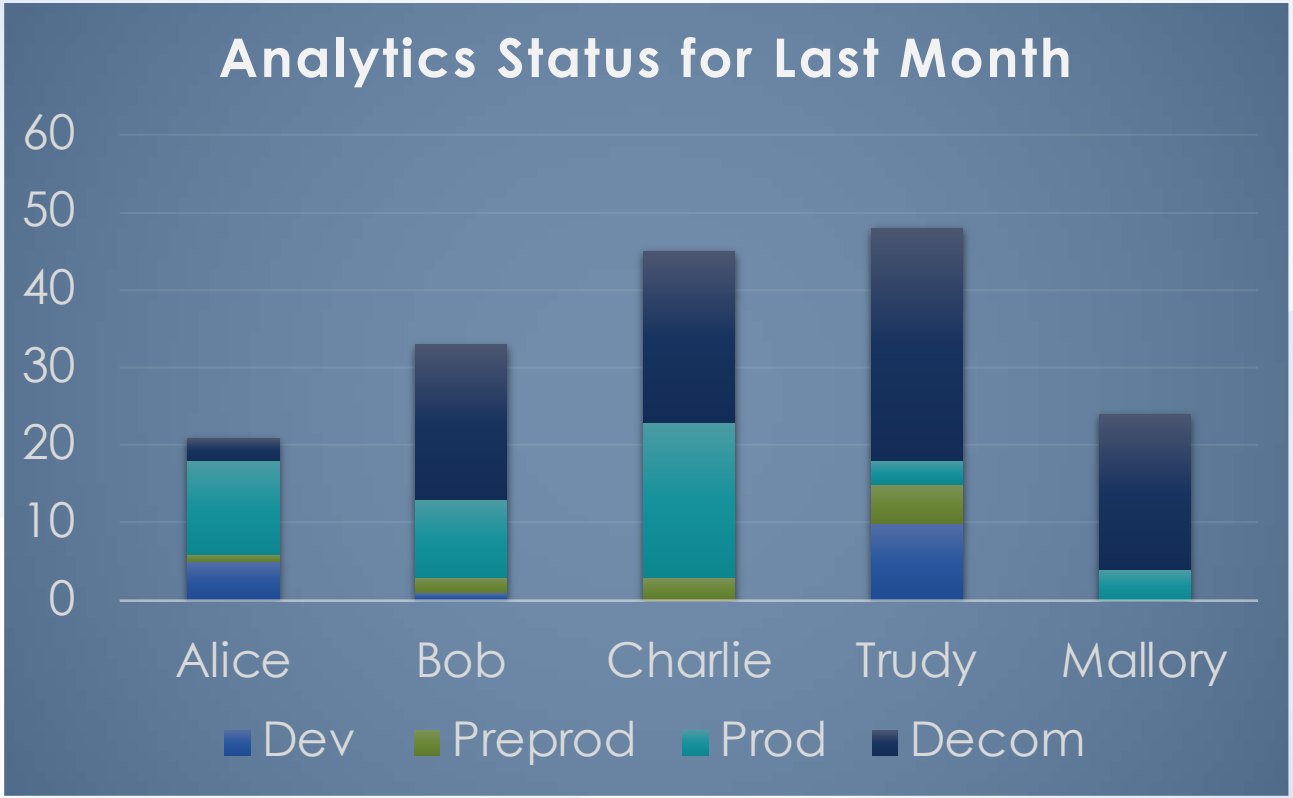
Advanced:

8. Runs in what framework (Streaming, batched query, etc.)
9. Last modified- who, when
10. Last reviewed- who, when
11. Status- dev, preprod, prod, decom
12. Output routes to… (analyst triage, automated notification, etc.)

Measure Analyst Productivity

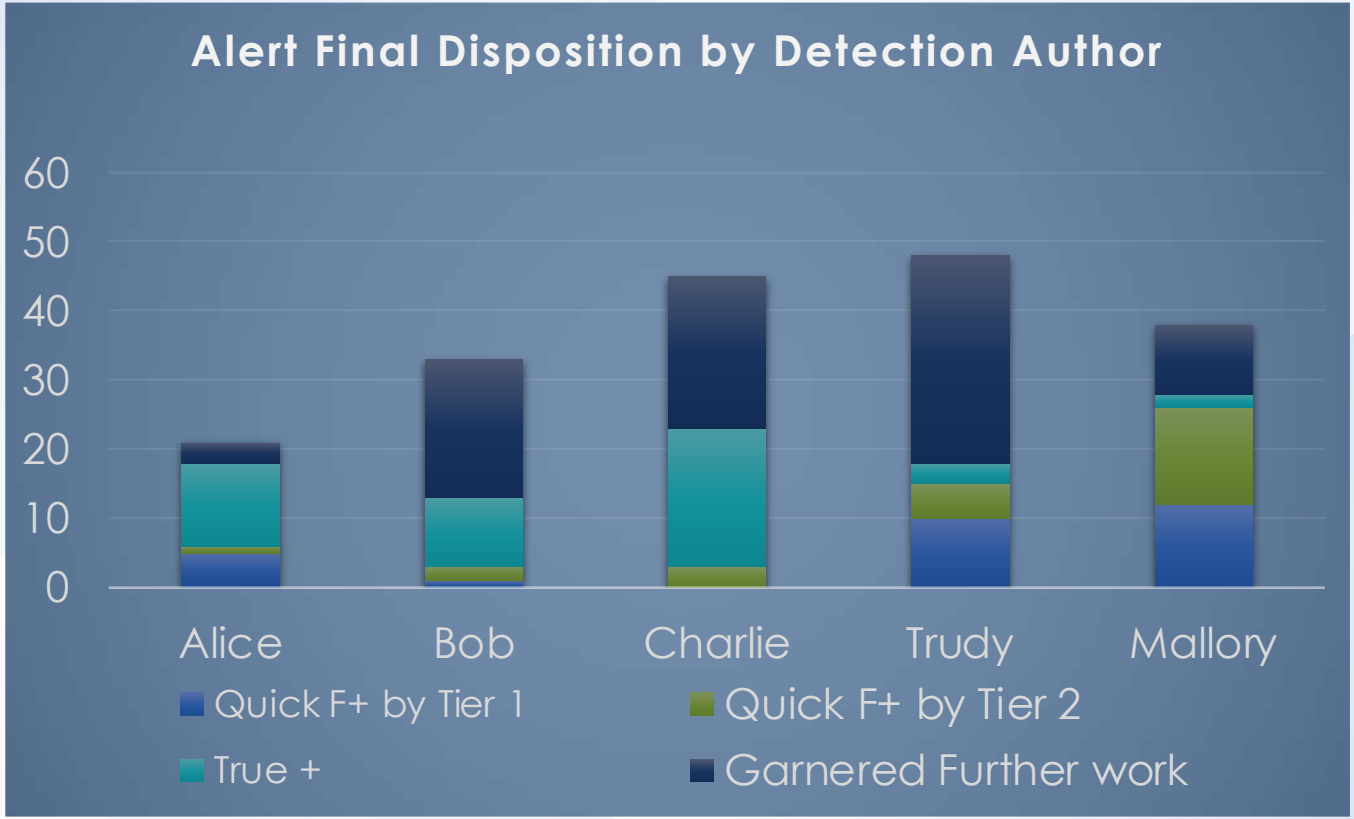
Is this good or evil?

Can this be gamed?

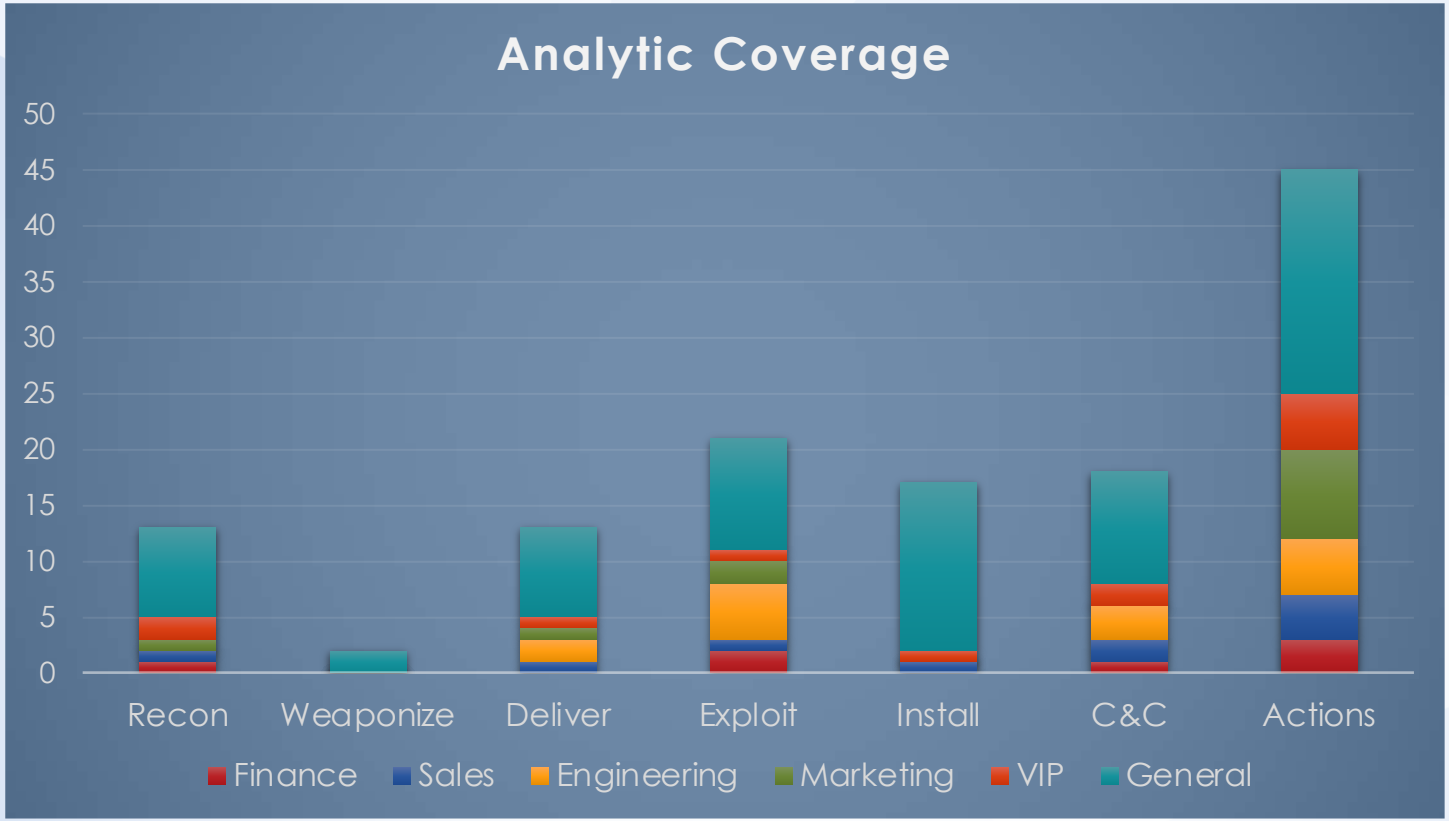


How Fruitful are Each Author's Detections?

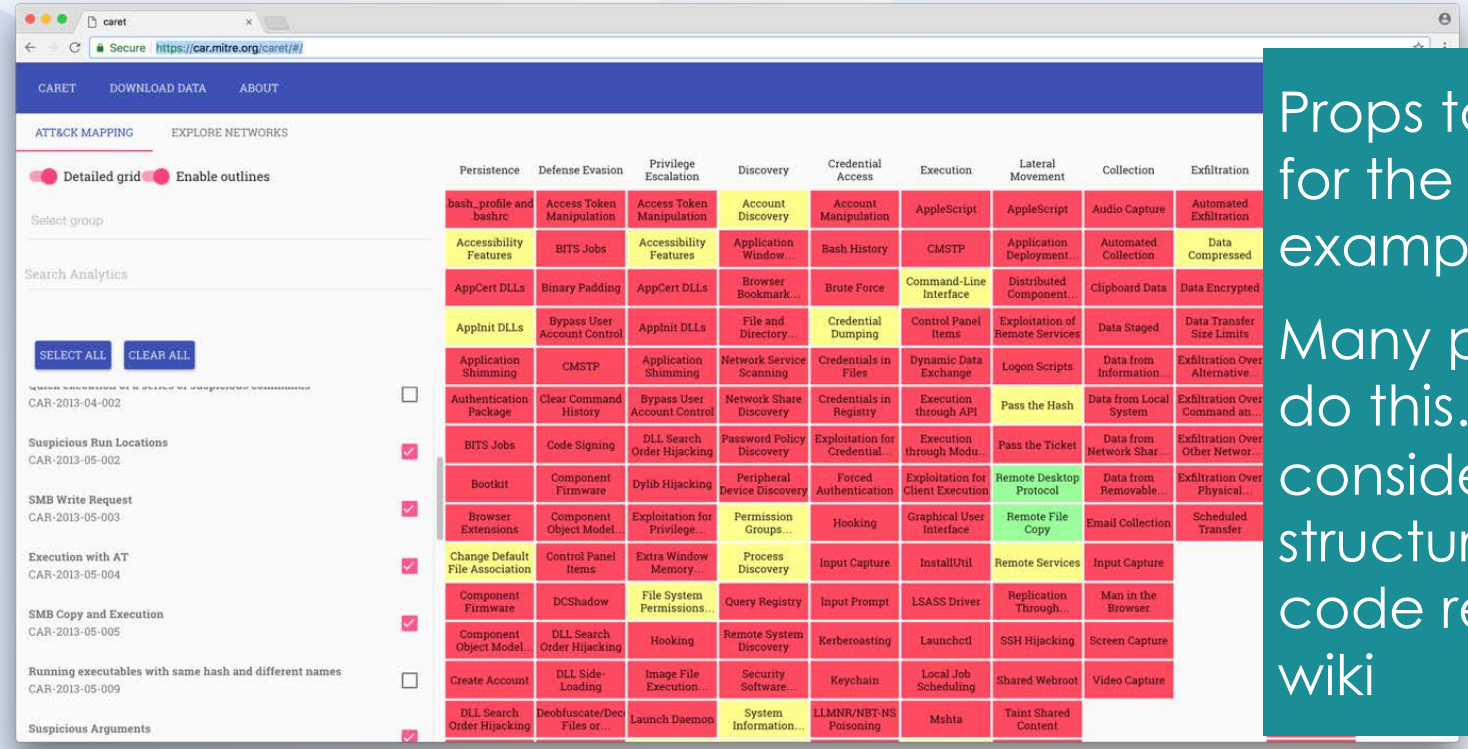
- # of times a detection or analytic fired, *attributed to the detection author*
- Is this evil?
- How can this be gamed?



How are You Supporting Your Customers?



Map Your Analytics to ATT&CK



Props to MITRE for the great example

Many places to do this… consider any structured code repo or wiki

https://car.mitre.org

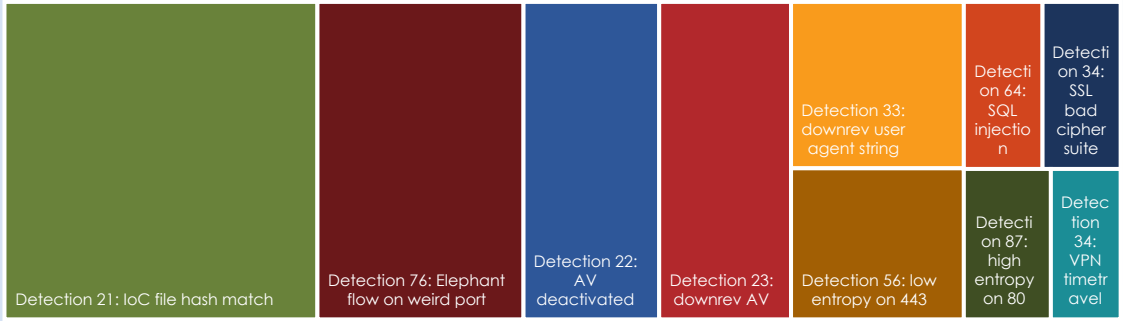
Metric Focus 5: Analyst Performance

1. Name
2. Join date
3. Current role & time in role
4. Number of alerts triaged in last 30 days
5. % true positive rate for escalations
6. % response rate for customer escalations
7. Number of escalated cases handled in last 30 days
8. Mean time to close a case

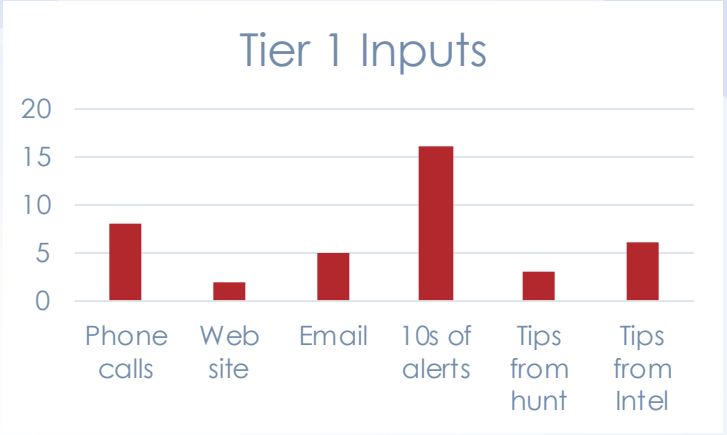
1. Number of analytics/detections created that are currently in production
2. Number of detections modified that are currently in production
3. Total lines committed to SOC code repo in last 90 days
4. Success/fail rate of queries executed in last 30 days
5. Median run time per query
6. Mean lexical/structural similarity in queries run

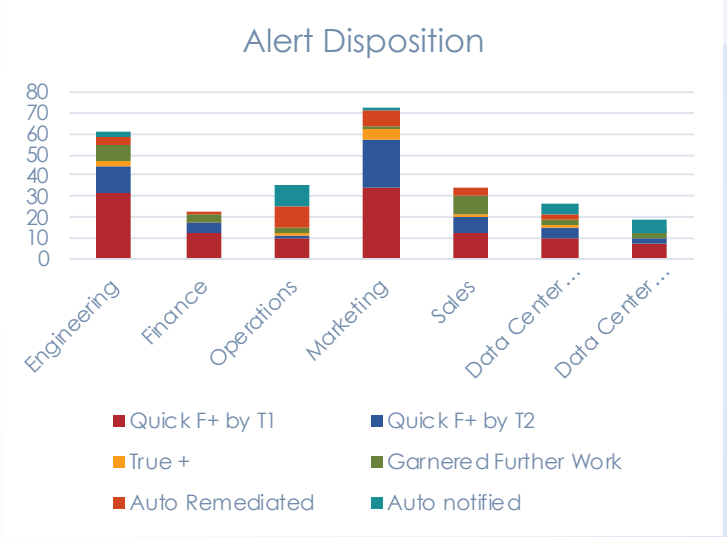
Daily Review Dashboard

Top firing detections



Top time spent per case





Metric Focus 6: Incident Handling

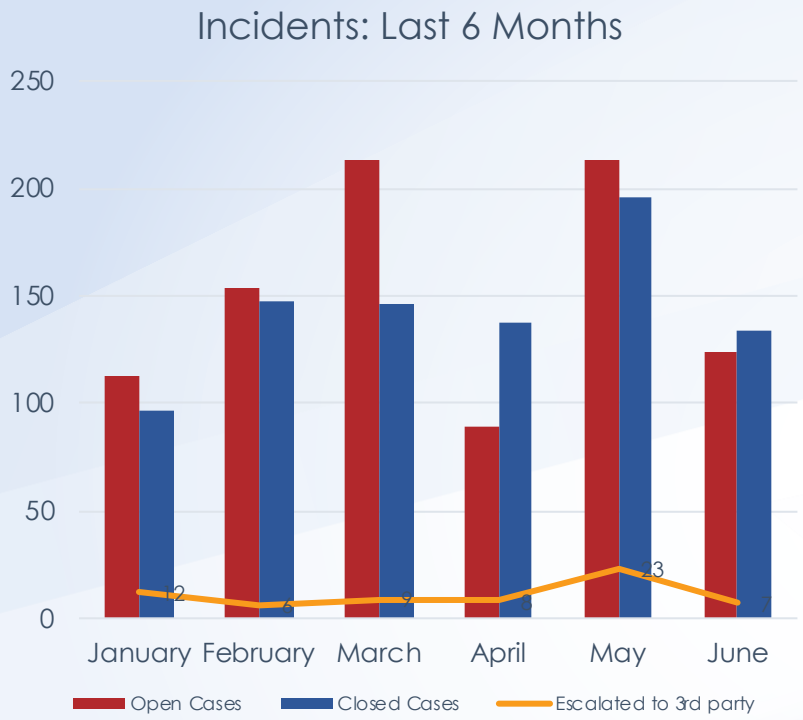
- Mean/median adversary dwell time
- Mean and median time to…
  - Triage & Escalate
  - Identify
  - Contain
  - Eradicate & recover
- Divergence from SLA/SLO?
- Insufficient eradication?
- Threat attributed?

- Top sources of confirmed incidents
- Proactive? Reactive?
- User reports? SOC monitoring?

Data & "anecdata": unforced errors and impediments

- Time waiting on other teams to do things
- No data/bad data/ data lost
- Incorrect/ambiguous conclusions
- Time spent arguing

Typical Incident Metrics



- More ideas:
- Mean/median time to respond
- Cases left open > time threshold
- Cases left open by initial reporting/detection type
- Stacked bar chart by case type

Incident Avoidability

- Most incidents are avoidable… everyone realizes this
  - Collect metrics on how avoidable, what could have been done to prevent
- Crowley's Incident Avoidability metric
  - A measure, already available in the environment, is applied to other systems/networks, but wasn't applied -> resulting in the incident
  - A measure is available (generally) and something (economic, political) prevents implementing it within the organization
  - Nothing is available to prevent that method of attack
- Attribution for measure/mechanism in 1 & 2 is critical

Metric Focus 7: Top Risk Areas & Hygiene

- Make vulnerability management data available to customers
  - Self service model
  - Scan results down to asset & item scanned
- But don't beat them over the head with every measure!
  - Pick classic ones they will always be measured on
  - Scanning, monitoring, patching
- Pick top risk items from own incident avoidability metrics and public intel reporting to focus on each year, semester, or quarter
  - Internet-exposed devices
  - Code signing enforcement
  - EDR deployment
  - Single factor auth
  - Non-managed devices & cloud resources

Conclusion

Closing

- Whatever you do, measure something
  - Include both internal and external measures
  - Behaviors and outcomes!
- You can do it, regardless of how mature, old, or big your SOC is
- Pick your investments carefully
- Iterate constantly

http://memeshappen.com/meme/custom/you-can-do-it-18134

Questions

“There are lies, damn lies, and statistics.” -- Unknown

FIREEYE™

CYBER DEFENSE SUMMIT 2019