Using Security Operations Center Metrics to Develop Awareness Programs

My Objectives

Multiple Benefits

- I am trying to encourage three things herein: all are intended to improve your cyber defensive posture

1. You to verify and improve metrics (and all reporting) from your SOC to your organization
2. You develop data centric messaging suitable for delivery to employees and customers
3. You help the organization understand what the SOC can do: gracefully minimize damage in uncertainty

Starting Point:
SOC-Class Functional Areas

Functional Areas of a SOC

Steering Committee

Command Center

Security Awareness

Monitoring

Threat Intelligence

Incident Handling

Forensics

Security Awareness

Self-Assessment

Metrics: Appropriate Audience

Metric Types

Who receives the metrics?

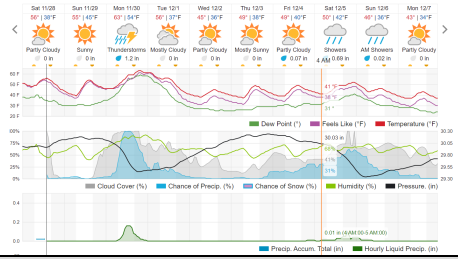
- External scope are reported metrics to management / Steering Committee (SC) / Board
- Service Level Objective (SLOs) with constituents for performance capability (implies reporting)
- Internal scope are used for SOC self-assessment
- User messaging: employees (maybe tailored based on role and risk) and customers (maybe tailored)

User Messaging

Metrics Aren't Good for Users

An End User Needs Forecasting and Metrics

- Individuals need *forecasting* and metrics
- Employees and Customers would be most benefit by a forecast based in recent data
- Precipitation = ???; Temperature = ???
- I don't have these exact parallels, but your SOC probably has some data you could use to forecast



wunderground.com 10 day forecast

Forecasting Team

Steering Committee

Command Center

Monitoring ★

Threat Intelligence ★

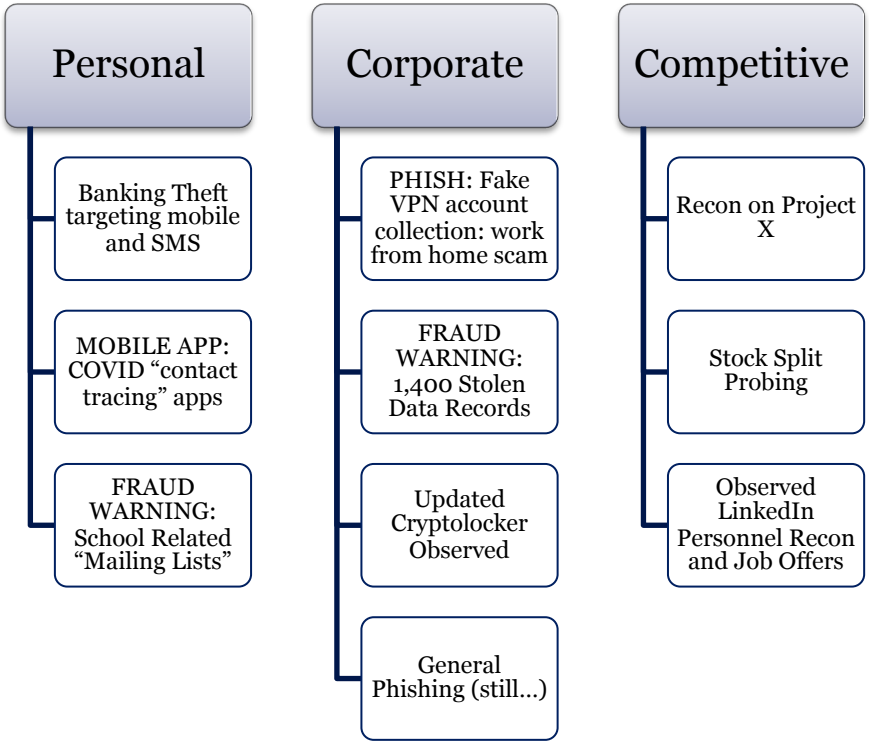
Incident Handling ★

Forensics

Self-Assessment ★

Cyber Forecast: Intel + Incidents

Forecast Might Be Imprecise at First



Threat Landscape

No newly identified threat groups

Ongoing Phishing and Social manipulation waves at sustained levels

Self-Assessment

IT Teams continue to be challenged with staffing shortages, cloud migrations, and personally owned devices introducing risk

Severe Weather

None forecast

Bi-Directional Flow of Information: User Awareness Training

User Awareness Training

As in, Make the SOC Aware of the Information System Users

- In addition to working on forecasting reports for people
- Bring stories into the SOC about people who the SOC works to protect, because the SOC often loses visibility
- Use Cases / Hunting is how I discuss engineered and ad hoc detection development (see my youtube for video)
- Hunts I encourage
  - Hunting our organization's systems in open source information
  - Identifying people responsible for systems
  - Identify value of systems to organization (more on this in a few slides)
- Check if these are done, and help remind that the information systems to defend are: computers, data, networks, people, and processes

SOC Statement of Success: The Guiding Principal

What Is Success for an SOC?

Define Success Carefully

- Is success defined as zero incidents detected?
  It is easy, *but not helpful*, to fail to find compromises
- Security Operations success is defined as: minimizing damage from threats to the organization's operations
- Detecting isn't good enough
- Preventing isn't feasible
- We succeed *by minimizing damage from threats*

What Is Success for an SOC?

Statement of Success

SOC is successful when it intervenes in adversary efforts to impact the availability, confidentiality, and integrity of *organization's* information assets. It does this by proactively making systems more resilient to impact and reactively detecting, containing, and eliminating adversary capability.

Call to Action

Return to Work and Critique Your SOC's Statement of Success

- Please, help the SOC to make sure:
  - It has one;
  - It's a good one;
  - It believes in it;
  - Your organization approves and supports that statement of success

Perversion Through Metrics

What Behavior Does the Metric Reinforce?

- If a person is judged (baseball card / analyst judgement coming later) on metrics that encourage bad behavior, the person will be driven to that behavior
- Incident count is a good example of this. More or fewer incidents handled isn't necessarily advancing success
- Metrics are measurements; Service Level Objectives are proposed levels of performance; until there's a basis, resist the urge to assert performance requirements

Metrics: Reported

Steering Committee Reported Metric

Crowley Incident Avoidability – 1,2,3

- On a scale of 1,2,3, was it avoidable?
- 1 - a measure, already available in the environment wasn't applied and resulted in the incident
- 2 - a measure is available in the larger environment and something (economic, political) prevents implementing it within the organization
- 3 - nothing is available to prevent that method of attack
- Discrete scale: only choices 1,2,or 3. There's no 2.6 or 1.7.
- Largely measures **Self-Assessment**

User Reported Metrics

Crowley Incident Avoidability – 1,2,3

Biz Unit 1	Biz Unit 2	Biz Unit 3	Biz Unit 4
Type1: 2	Type1: 0	Type1: 8	Type1: 2
Type2: 0	Type2: 4	Type2: 3	Type2: 0
Type3: 0	Type3: 1	Type3: 0	Type3: 1

Metrics: Service Level Objectives

Service Level Objective

SOC's Contract with the Business

- Service level objectives dictate the performance levels required by the organizations
- If the SOC is not able to meet SLOs, look for optimizations that favor the shortest path to accomplish the objective
- No optimizations available? Seek additional resources
- SLO: no monetary penalty for failure
- SLA: monetary penalty for failure

Reporting to Affected Business Unit

- Status information will be delivered to the affected Business Unit (BU) at a specified frequency
- Initial notification within 1 hour of suspected impact to BU's resources (not from alerts in SIEM)
- Minimum of daily updates on moderate(+) incidents
- More reporting instances to consider:
  - Vulnerability scanning and pen test (bad) results
  - Threat intelligence: targeting of BU's systems

Metrics: SOC Internal Health and Performance

Internal Metrics

- Lots of metrics are to track within the SOC, but aren't reported outward from SOC
- Primarily for internal performance improvement

Measurement and Metrics

Baseball Card

- Each analyst is assessed on same measures
- Carson Zimmerman's 2018 SOC Summit Keynote has a good baseball card
- BTW, I am not a sports spectator, flavor it for your company's culture, this is the gist

Analyst Baseball Card	
Christopher Crowley	Name
Chris	Preferred first name
TwoGuns	Callsign
2015-11-17	Join Date
NSM Analyst - Senior	Current Role
1 year, 1 month	Time in Role
38	Alerts Triaged in last 30 days
91.40%	Percent True Positive Rate
82.70%	Response rate percent for customer escalation
19	Escalated cases handled in last 30 days
1:34	Mean time to close case
7	Number analytics created currently in production
28	Number detection modified currently in production
423	Total lines committed to SOC code repository in last 90 days
91.40%	Success rate of queries against SIEM in last 30 days
0:09	Median run time per query
0.23	Mean lexical structure similarity in queries run in last 30 days

More Ideas

- Zimmerman / Crowley talk: https://mgt517.com/first-metrics

- Many more specific examples there

Impact

Impact Definition

Incident Impact Levels

Low

- Few systems (or only a specific type)
- Unimportant systems
- Unimportant data

Moderate

- More systems (or many types, or a common type)
- Important or high value person's, account, or system
- Important data at risk

High

- Most systems (or almost all types)
- Highest level accounts, users, and systems
- Business critical data

Impact Definition

Incident Impact Categories (simplified US-CERT)

Functional

- Low – minimal function disruption
- Moderate – substantial disruption
- High – complete disruption

Informational

- Intellectual Property (L/M/H)
- Integrity Manipulation (L/M/H)
- Privacy violated (such as PII / PHI)

Recoverable

- Regular – predictable using resources on hand
- Supplemented – predictable with augmented resources
- Unrecoverable – data breach which cannot be undone

Incident Impact Quantification Charts

Takes a lot of Work

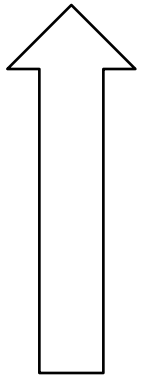
- The chart on the next pages is something I created to articulate impact
- This is both for during (status) and after (final report) of an incident
- Produces a quantitative impact scale (3-300)
- I'm going to show a stepwise build up
- Then an incident impact view

Impact Quantification

Incident Impact Quantification

System #8 – Accounts Payable – Check Writing

- Start with a list of systems (hunt later)
- For each system define a quantity for impact
- The quantities are relative to all the systems in the organization

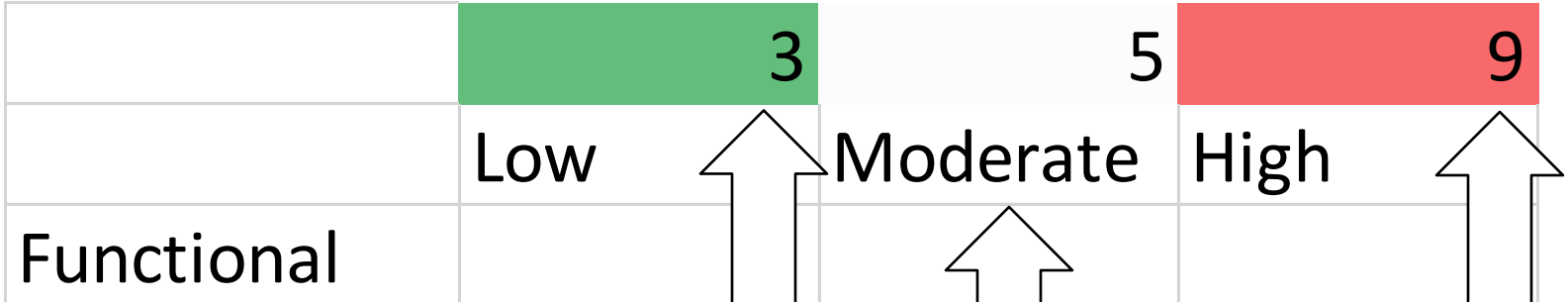


- Start with broad containers (workstations and servers) then develop specific sub-containers (domain controllers, DNS servers, accounts receivable, web commerce system, …)

Incident Impact Quantification Example

System #8 – Accounts Payable – Check Writing

For levels low, moderate, high: assign point values (1-10) for the system relative to other systems



Pro-tip: Start with 3,5,9 as generic default for all, and adjust from there

Impact Quantification

Incident Impact Quantification Example

Repeat (1-10)for impact to mission of this system: functional, informational, and recovery difficulty

		3	5	9
		Low	Moderate	High
5	Functional			
7	Informational			
9	Recoverable			

Pro-tip: Start with 5,7,9 as default then adjust on a per system basis

Impact Quantification

Math is Magic!

System #8 – Accounts Payable – Check Writing

		3	5	9
		Low	Moderate	High
5	Functional	15	25	45
7	Informational	21	35	63
9	Recoverable	27	45	81

Color coding shifts because overall scale is now 3 - 81

Incident Impact Quantification Charts

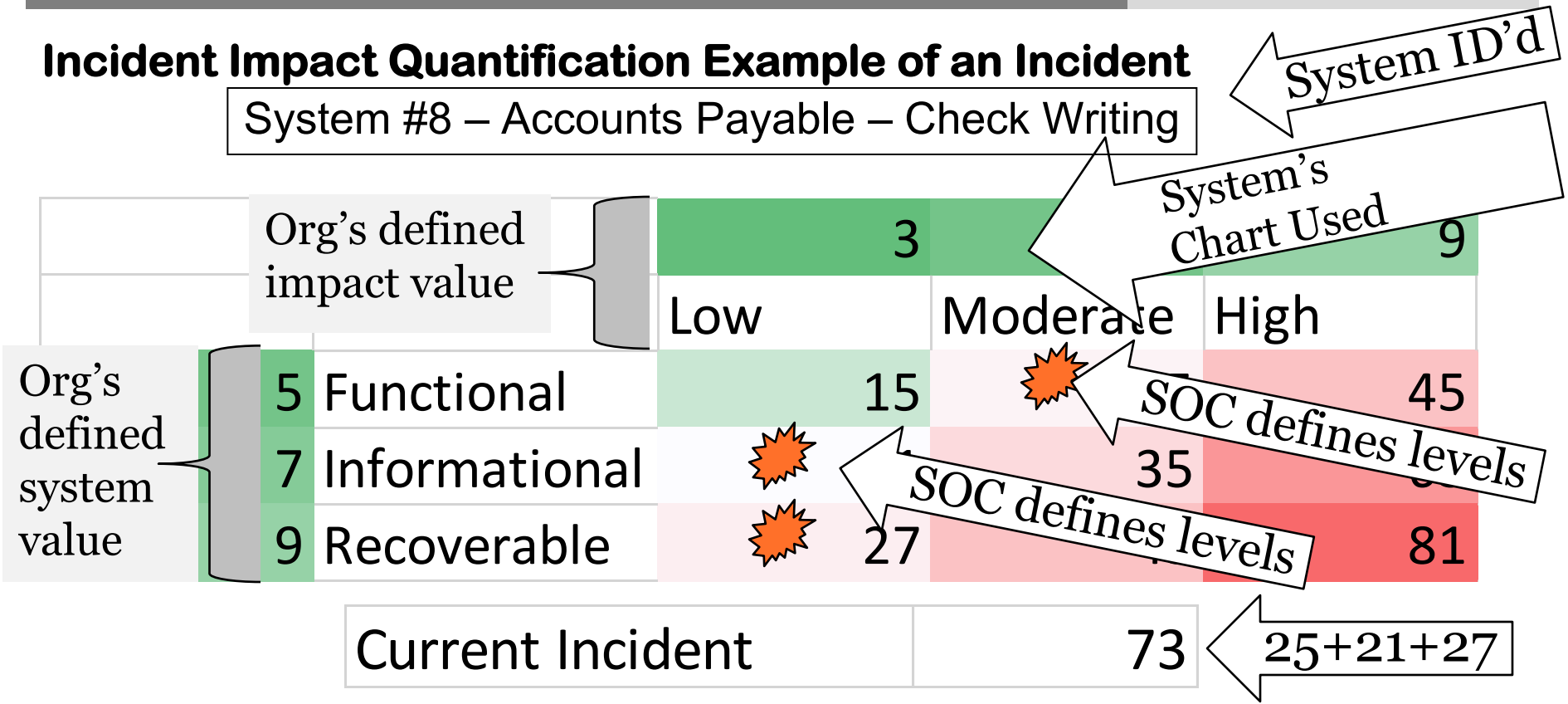
Guidance for Impact Assessment

- SOC staff and Steering Committee informed of and trained on meanings of
  - Low, Moderate, High
  - Functional, Information and Recoverable
- There should be guidance written, examples provided, specific examples

Impact Quantification

Incident Impact Quantification Example of an Incident

System #8 – Accounts Payable – Check Writing



- The risk decisions need to be shared with the SOC, and the SOC needs to provide situational awareness about the change of the risk to the systems
  - Change in threats or vulnerabilities
- My preferred way to discuss risk is using the metonymy of Alex Honnold

Impact Reporting to Users

- Users of systems should be aware of the impact quantification system
- Users affected by or involved in an incident should informed of the impact (73/300)
- In addition to “avoidability” metric report, perhaps Business Unit based incident impact metric report

User Reported Metrics

Crowley Incident Avoidability – 1,2,3 and Impact (More is Worse)

BU 1: 127

- Type1: 2
  - 31, 86
- Type2: 0
- Type3: 0

BU 2: 367

- Type1: 0
- Type2: 4
  - 48,21,126,80
- Type3: 1
  - 92

BU 3: 985

- Type1: 8
  - 102,34,16,201, 74,51,118,29
- Type2: 3
  - 49,201,110
- Type3: 0

BU 4: 403

- Type1: 2
  - 93,231
- Type2: 0
- Type3: 1
  - 79

Want to Hear More?

Measurement, Metrics, and More…

PDFs, PPTs, Videos, …

- This and many other talks:
  https://mgt517.com/soc
  https://mgt517.com/youtube
- https://www.montance.com
- 2020 SOC Survey Results
  To be released December, 18th
  https://soc-survey.com