RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: 20651

SOC Metrics: Discovering the Key to SOC Nirvana

Ankush Baveja

PreSales Engineer
RSA
@socdefender

#RSAC

“If you don’t collect any metrics, you’re flying blind. If you collect and focus on too many, they may be obstructing your field of view.”
— Scott M. Graffius

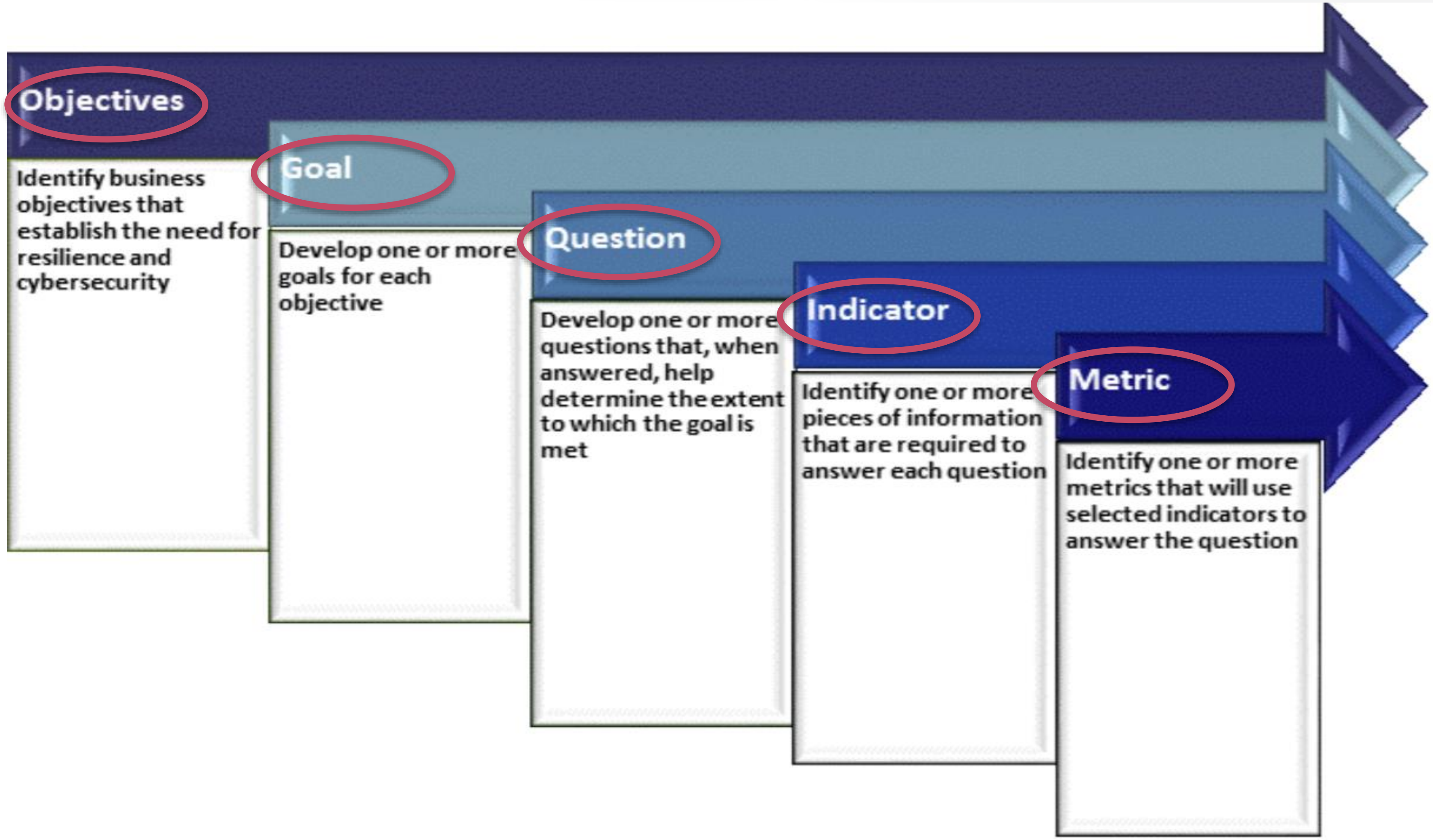
Agenda/Motivations for this session

- Problem Statement
  - Unable to measure because lack of a framework
- Solution - Framework
  - “What to measure” or rather “How to identify what to measure”
- Topics we will cover today
  - SOC Capabilities
  - Linking capabilities to metrics
  - Linking metrics to outcome
- Disclaimer
  - Not “how to measure”
  - My own views

Some of the Metrics we will discuss today

- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)
- False Positive List (FPL) and False Positive Rate (FPR)
- What are we detecting? – MITRE ATT&CK Coverage
- Device Coverage % and Content Requests Processed
- New Content Requests Created
- Attack Quotient (AQ)

Introducing GQIM – deriving metrics from capabilities



Objectives

Identify business objectives that establish the need for resilience and cybersecurity

Goal

Develop one or more goals for each objective

Question

Develop one or more questions that, when answered, help determine the extent to which the goal is met

Indicator

Identify one or more pieces of information that are required to answer each question

Metric

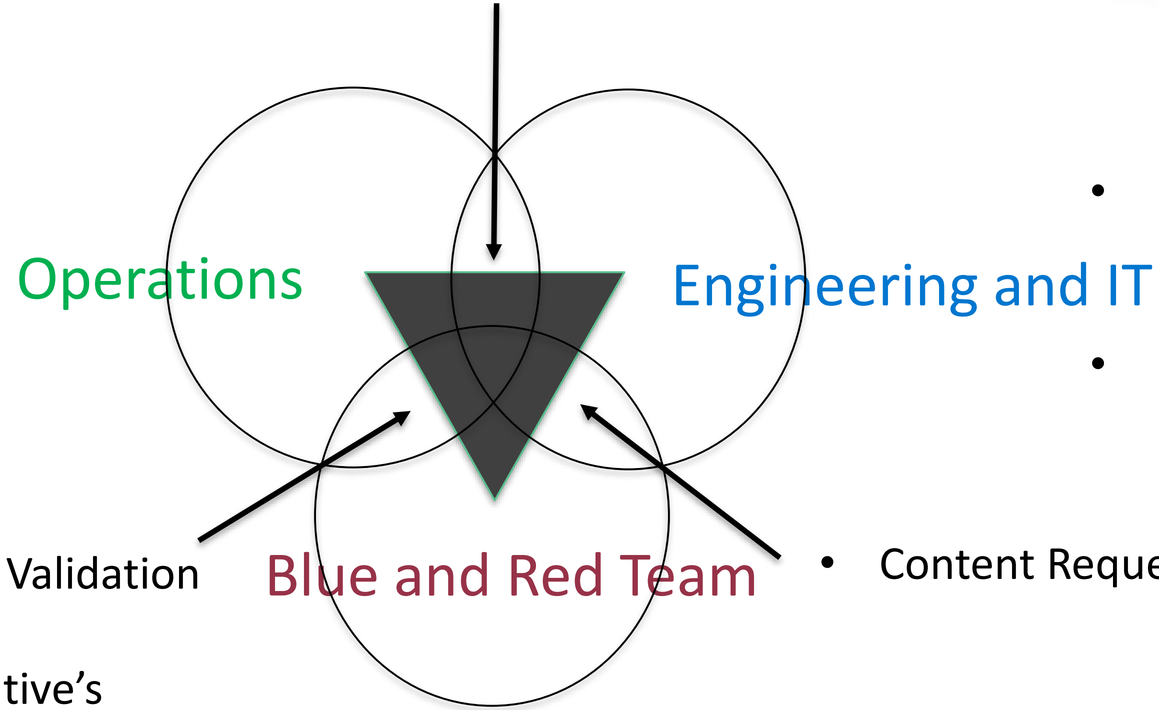
Identify one or more metrics that will use selected indicators to answer the question

GQIM Method [Stewart 2015]

SOC Capability Triad

- New Tech Onboarding
- Trainings

- 24/7 Incident Triage
- Incident Escalation & Containment



Operations

Engineering and IT

Blue and Red Team

- IT
  - Tech Evaluation
  - Stack Administration
- Engineering
  - Content Management

- Content Requests – Technical Validation (investigations)
- Content Requests – False Positive’s

- Content Requests – Tooling

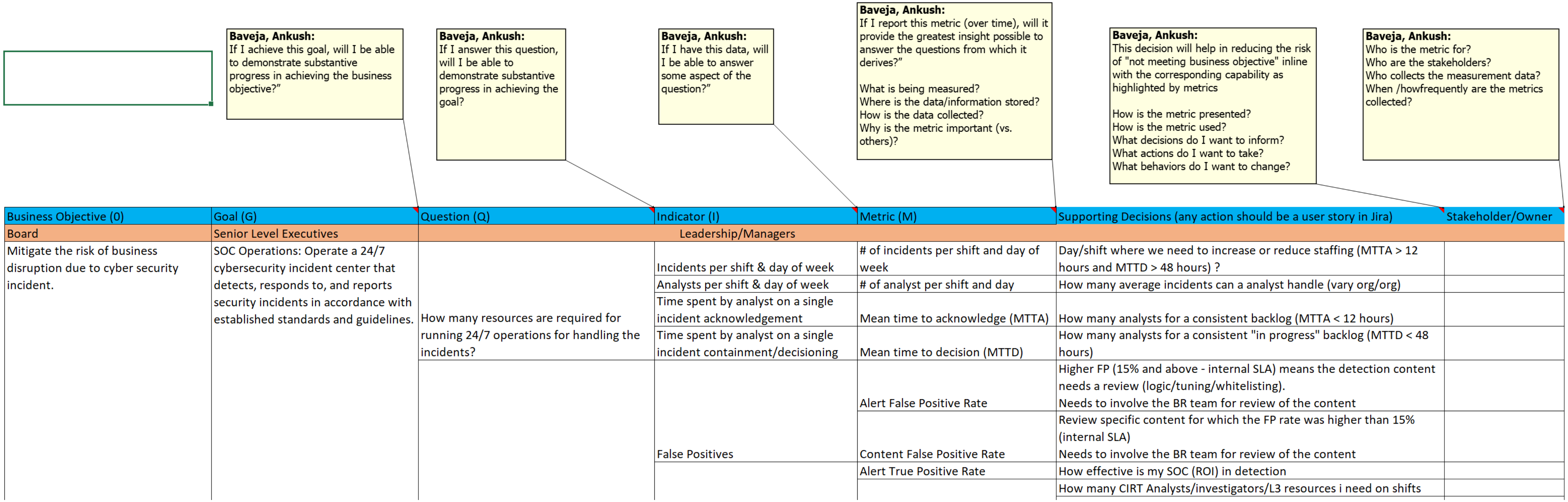
- Testing New and existing content

Governance and PMO

- Coordination with TI team

Using GQIM for SOC capability triad

Security metrics are the servants of risk management, and risk management is about making decisions. Therefore, the only security metrics we are interested in are those that support decision making about risk for the purpose of managing that risk.



Baveja, Ankush:
If I achieve this goal, will I be able to demonstrate substantive progress in achieving the business objective?"

Baveja, Ankush:
If I answer this question, will I be able to demonstrate substantive progress in achieving the goal?

Baveja, Ankush:
If I have this data, will I be able to answer some aspect of the question?"

Baveja, Ankush:
If I report this metric (over time), will it provide the greatest insight possible to answer the questions from which it derives?"

What is being measured?
Where is the data/information stored?
How is the data collected?
Why is the metric important (vs. others)?

Baveja, Ankush:
This decision will help in reducing the risk of "not meeting business objective" inline with the corresponding capability as highlighted by metrics

How is the metric presented?
How is the metric used?
What decisions do I want to inform?
What actions do I want to take?
What behaviors do I want to change?

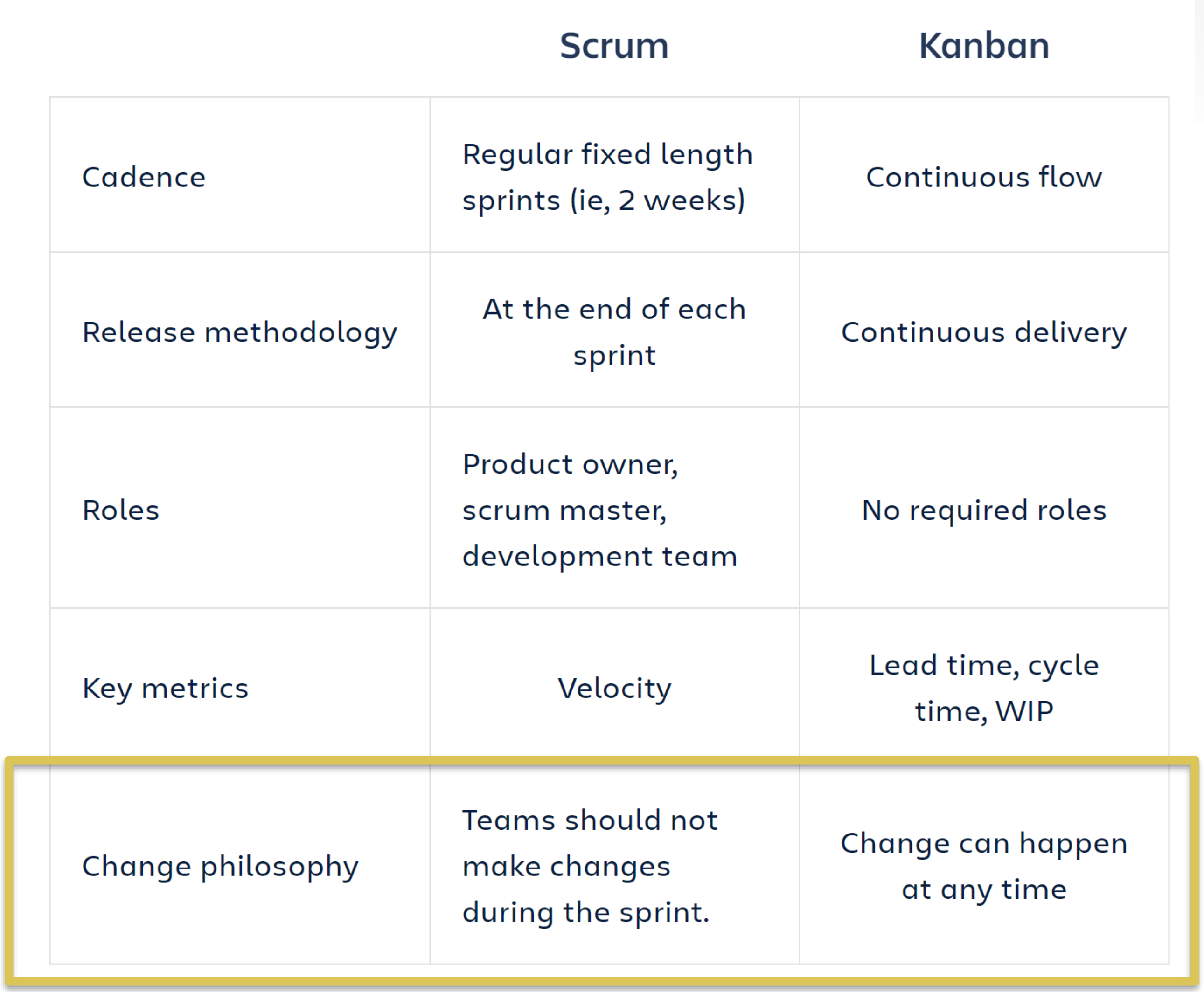
Baveja, Ankush:
Who is the metric for?
Who are the stakeholders?
Who collects the measurement data?
When /howfrequently are the metrics collected?

Business Objective (0)	Goal (G)	Question (Q)	Indicator (I)	Metric (M)	Supporting Decisions (any action should be a user story in Jira)	Stakeholder/Owner
Board	Senior Level Executives	Leadership/Managers				
Mitigate the risk of business disruption due to cyber security incident.	SOC Operations: Operate a 24/7 cybersecurity incident center that detects, responds to, and reports security incidents in accordance with established standards and guidelines.	How many resources are required for running 24/7 operations for handling the incidents?	Incidents per shift & day of week	# of incidents per shift and day of week	Day/shift where we need to increase or reduce staffing (MTTA > 12 hours and MTTD > 48 hours) ?	
			Analysts per shift & day of week	# of analyst per shift and day	How many average incidents can a analyst handle (vary org/org)	
			Time spent by analyst on a single incident acknowledgement	Mean time to acknowledge (MTTA)	How many analysts for a consistent backlog (MTTA < 12 hours)	
			Time spent by analyst on a single incident containment/decisioning	Mean time to decision (MTTD)	How many analysts for a consistent "in progress" backlog (MTTD < 48 hours)	
			False Positives	Alert False Positive Rate	Higher FP (15% and above - internal SLA) means the detection content needs a review (logic/tuning/whitelisting). Needs to involve the BR team for review of the content	
				Content False Positive Rate	Review specific content for which the FP rate was higher than 15% (internal SLA) Needs to involve the BR team for review of the content	
				Alert True Positive Rate	How effective is my SOC (ROI) in detection	
					How many CIRT Analysts/investigators/L3 resources i need on shifts	

Triad #1 - SOC Operations

Metric	Decision
• # of analyst per shift and day • # of incidents per shift and day of week	• Day/shift where we need to increase or reduce staffing (MTTA > 12 hours and MTTD > 48 hours) ? • How many average incidents can a analyst handle (vary org/org)
• Mean Time to Acknowledge (MTTA) • Mean Time to Decision (MTTD)	• How many analysts for a consistent backlog (MTTA < 12 hours) • How many analysts for a consistent "in progress" backlog (MTTD < 48 hours)
• Alert True Positive Rate • # of incident escalated • Content True Positive Rate • Type of Action Taken and time taken for implementation	• How effective is my SOC (ROI) in detecting attacks • How many CIRT Analysts/investigators/L3 resources on shift • Any specific type of behavior which requires user education or reporting to senior management (for eg: phishing, ELT targeted)? • Any specific type of control (preventative, detective, corrective, deterrent etc.) that can help reduce the risk • What is the ability of supporting functions to respond to SOC request (block/reimage/quarantine)
• Alert False Positive Rate • Content False Positive Rate	• Higher FP (> 15%) means detection content needs a review (logic/tuning/whitelisting) • Needs to involve the BR team for review of the content

Kanban v/s Scrum



	Scrum	Kanban
Cadence	Regular fixed length sprints (ie, 2 weeks)	Continuous flow
Release methodology	At the end of each sprint	Continuous delivery
Roles	Product owner, scrum master, development team	No required roles
Key metrics	Velocity	Lead time, cycle time, WIP
Change philosophy	Teams should not make changes during the sprint.	Change can happen at any time

https://www.atlassian.com/agile/kanban/kanban-vs-scrum

Triad #2 - SOC Engineering & IT

Metric	Decision
Build - Content Implementation (Scrum) • # of new content processed & blocked • Backlog # and future sprints roadmap	• New detections -> SOC run books and feedback • Blocked -> Engage with OEM • Higher backlog -> More resources required • Backlog prioritization with BR team
Build – Platform (Scrum) • # of new log sources onboarded • Total # of log sources being monitored • # of Platform/administrative requests processed & blocked (upgrades, tool onboarding, POC, hardware etc)	• Which log sources are pending integration and why (backlog prioritization) • What is my visibility % w.r.t to my roadmap - Risk • Budgeting exercise - Infrastructure and Tools • Platform related requirements – training, hardware, OEM support • Capabilities to be outsourced
Run – Content Tuning (Kanban) • # of tuning requests processed & backlog	• How many engineers required for run support and their training needs?
Run – Platform (Kanban) • # of adhoc/urgent requests – user, access etc • Issue support and troubleshooting	• Platform team rostering • OEM engagement and support model

Triad #3 - Blue and Red Team

Metric	Decision
• False Positive Rate (alert and content) • True positive rate	• Ineffective detections (false sense of security) • Success criteria for BR team
• MITRE ATT&CK Content Coverage • Attack Navigator dashboard • Content requests added to Run/Build backlog • Content requests WIP (Hypothesis, requirement gathering, lab tests, release to sprint backlog)	• What coverage is missing? • Content Pipeline – Detection Improvement plan
• Attack Quotient (high likelihood/high impact) • Threat Actor tracking and specific TTP’s • Pentests • New Vuln (Exploitable, Critical, Relevant) • Threat Intel team inputs	• What are our top threats? • Prioritized Content backlog • What critical threats are not being detected today?

https://mitre-attack.github.io/attack-navigator/enterprise/

Governance and PMO

Metric	Decision
• Training Program - NIST NICE Matrix* (Knowledge Skills Abilities)	• What training my team needs? • Training budget requirement? • Backup planning - Dependencies on any key resources?
• Quality Assurance and Audit • Audit Checklist and compliance • Eg: Triage Quality rating	• Internal Audit assessment and review the quality of functions • Incorporate process improvements
• SOC Dashboard and visualization • Jira Program backlog reporting for each SOC capability	• Complete view of SOC capabilities and functions for senior leadership • Performance incentive / Talent Management – Linking MBO's • Internal SOC maturity plan

https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

Apply What You Have Learned Today

- Next week you should:
  - Choose a framework
    - Download and use the framework sheet
  - Define capabilities for your SOC (current and roadmap)
- In the first three months following this presentation you should:
  - Identify metrics for each capability, use the GQIM methodology
  - Define how these measurements affect your decisions
    - For eg – 10% variation vs 40% variation
  - Define stakeholders and assign ownership to monitor/alert
- Within six months you should:
  - Create your SOC Dashboard
  - Set periodic checkpoints to review the goals
  - If "A" Metric doesn't add value or lead to any decision, dump it

Q/A

RSAConference2020

Thank you