#FIRSTCON24

KPIs for CSIRTs

Logan Wilkins, Cisco, USA

Agenda

1. General Introduction
2. Overview of KPIs
3. Best Practices
4. Challenges
5. Sample KPIs for CSIRTs
6. Class Exercise
7. Sample Charts

Class Overview

- Mostly lecture, with discussion
- Some in-class exercises
- Questions are OK - actually appreciated - at any time
- Take bio / stretch breaks as you like
- 15 min break in middle
- Questions?

Key Performance Indicators

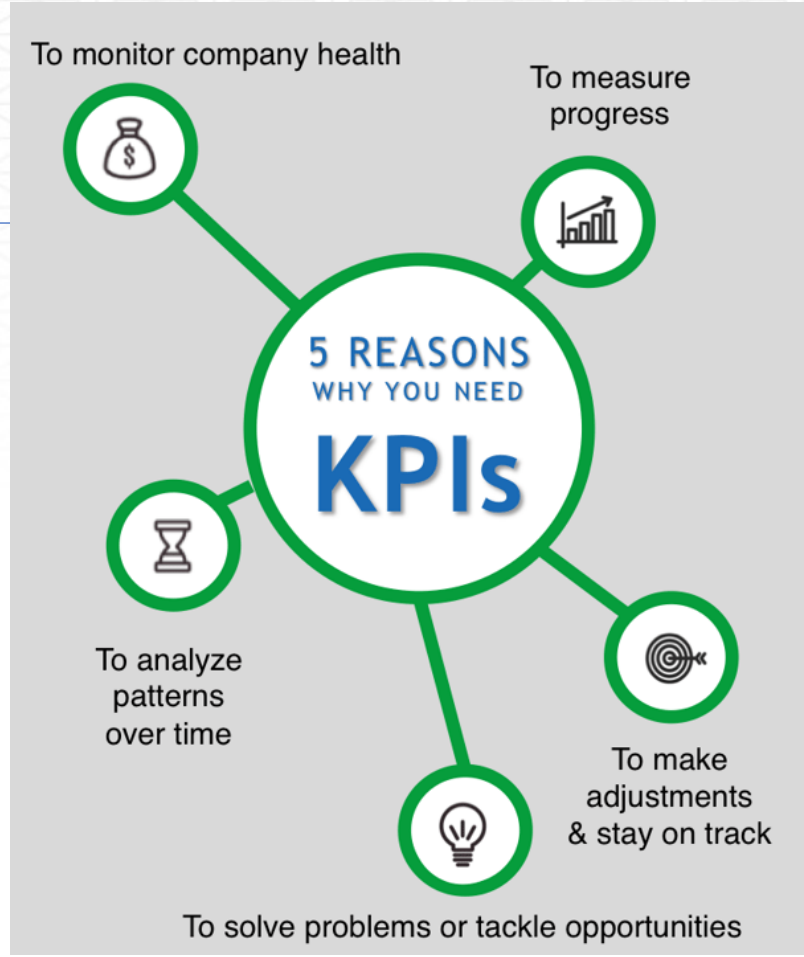
But first – About CSIRTs

- Protect critical digital assets
- Minimize the impact of security breaches
- Collaborate with various stakeholders:
  - IT, Businesses, Management,
  - Legal, External entities, …
- Ensure effective incident handling
- Facilitate a coordinated response to cybersecurity threats

Key Performance Indicators

Characteristics

- Are measurable / quantifiable
- Assess progress and performance in achieving specific objectives or goals.
- Evaluate the effectiveness and efficiency of a process
- Identify areas for improvement
- Ensure alignment with organizational objectives



Key Performance Indicators

Three Definitions

1. *Measure / Metric*

- A measure is a single unit (e.g., number of incidents in a given month) .
- A metric may be made of multiple units (e.g., percentage increase or decrease in incidents year over year).
- These terms are often used interchangeably throughout the cybersecurity community.

https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Key Performance Indicators

Three definitions

2. ***KPI***
   - Measure/metric used to demonstrate how an organization is achieving key business objectives
3. ***Assessment***
   - An approach, process, or way of evaluating something that results in measures/metrics

https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Building a KPI Program

Twelve Best Practices

1. ***Define Your Objectives***
   - Determine what aspects of CSIRT performance to measure and improve.
   - Align these objectives with the overall goals of your organization.

Building a KPI Program

Business Objectives

Sample from 11 Strategies of a World Class Cybersecurity Operations Center:

- Assess and close gaps in detection and prevention for adversary TTPs
- Improve effectiveness and quality of analyst efforts
- Ensure quality, stability, and service delivery of internal SOC tools and systems
- Understand and demonstrate readiness for certain objectives, services, mission areas the SOC is considering undertaking
  - (e.g., is the SOC ready to perform hunting, does it need in-house malware analysis, should it consider purchasing a deception product).

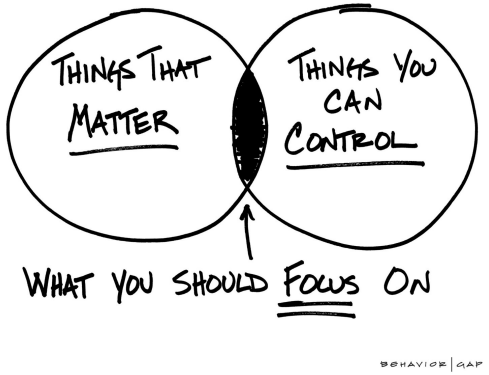
https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Building a KPI Program

Twelve Best Practices

2. *Select Relevant KPIs*

- Identify KPIs that align with your objectives and that measure the desired aspects of CSIRT performance.
- Make your KPIs
  - meaningful,
  - measurable,
  - actionable



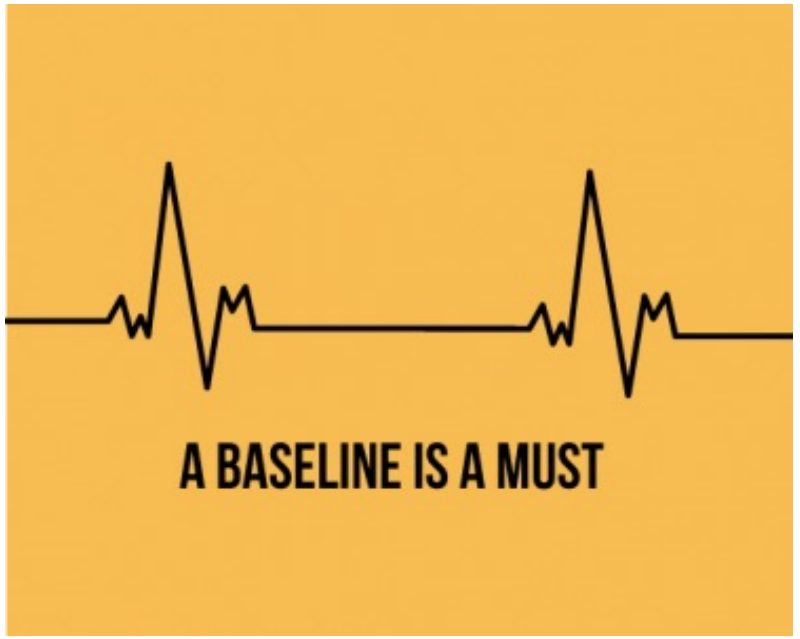
- Consider categories such as threat hunting, incident response, incident handling, and team performance.

Building a KPI Program

Twelve Best Practices

3. *Establish Baselines and Targets*

- Set baseline values for each KPI to establish a starting point for measurement.
- Derive baselines from historical data, industry benchmarks, or internal performance expectations.
- Set realistic targets or goals for each KPI, indicating the desired level of performance



Building a KPI Program

Twelve Best Practices

4. *Define Measurement Methods*

- Determine your data sources
- Determine how you will collect the necessary data to measure each KPI.
- Establish data collection methods and sources, ensuring they are accurate, reliable, and consistent.
- Automate, automate, automate; streamline data collection processes where possible.

Building a KPI Program

Data Sources

https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

From 11 Strategies of a World Class Cybersecurity Operations Center:

- SIEM/analytics/log management platforms
- SOC ticketing/case management system and SOAR platforms
- SOC code repository and task management DevOps support systems
- Enterprise asset management
- Vulnerability management/scanning systems
- Automated attack frameworks, phishing as a service, and breach and attack simulation (BAS) platforms
- Also:
  - Operational exercises and simulations:
  - Use of an established cybersecurity framework or capability maturity model

Building a KPI Program

Twelve Best Practices

5. *Establish Data Analysis and Reporting Processes*

- Define how you will analyze the collected data to derive meaningful insights.
- Use appropriate data analysis techniques and tools to track KPI trends, identify patterns, and assess performance.
- Establish reporting processes to communicate KPI results to relevant stakeholders in a clear and concise manner.

Building a KPI Program

Twelve Best Practices

6. *Set Regular Evaluation Intervals*

- Determine the frequency at which you will valuate and assess the KPIs.
- Plan for regular intervals - monthly, quarterly, annually…
- Consistently monitor and track the KPIs to observe performance trends and make data-driven decisions.

Building a KPI Program

Twelve Best Practices

7. *Use Compensating Controls Where Necessary*

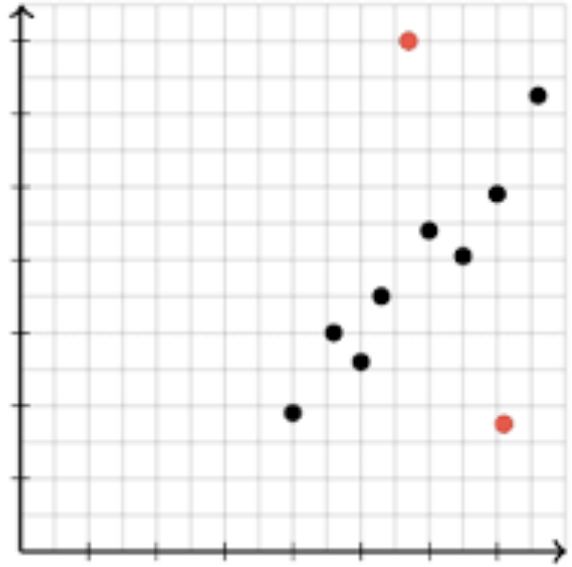
- Be careful that your KPI doesn't incentive bad behavior, for example closing cases just to meet a target number.
- Combine KPIs so that one controls for another; e.g., documentation completeness vs. case closure

Building a KPI Program

Twelve Best Practices

8. *Use Meaningful Statistics / Avoid Outliers*

- Mean / average is often used in KPIs but is only relevant for normal distributions (not timelines)
- Consider median, and/or percentiles to level your numbers and improve accuracy.



Building a KPI Program

Twelve Best Practices

9. *Foster Stakeholder Engagement*

- Engage relevant stakeholders, such as management, CSIRT team members, and other key personnel.
- Share relevant KPIs with the correct stakeholders.
- Charts and graphs work wonders.

Building a KPI Program

Twelve Best Practices

10. *Continuously Improve and Iterate / Take Action!*

- Use the insights gained from KPI analysis to drive continuous improvement.
- Identify areas for enhancement; take corrective actions.
- Regularly review and update the KPI framework to ensure its relevance and effectiveness.

Building a KPI Program

Twelve Best Practices

11. Provide Training and Support

- Offer training and guidance to the CSIRT team members on KPI importance and use.
- Ensure they understand the specific KPIs being measured, how they are calculated, and how their performance impacts the overall CSIRT effectiveness.

Building a KPI Program

Twelve Best Practices

12. *Maintain Documentation*

- Document the KPI framework, measurement methods, data sources, and analysis processes.
- Maintain an updated record of KPI results and related insights.

Building a KPI Program

Five Basic Elements

https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

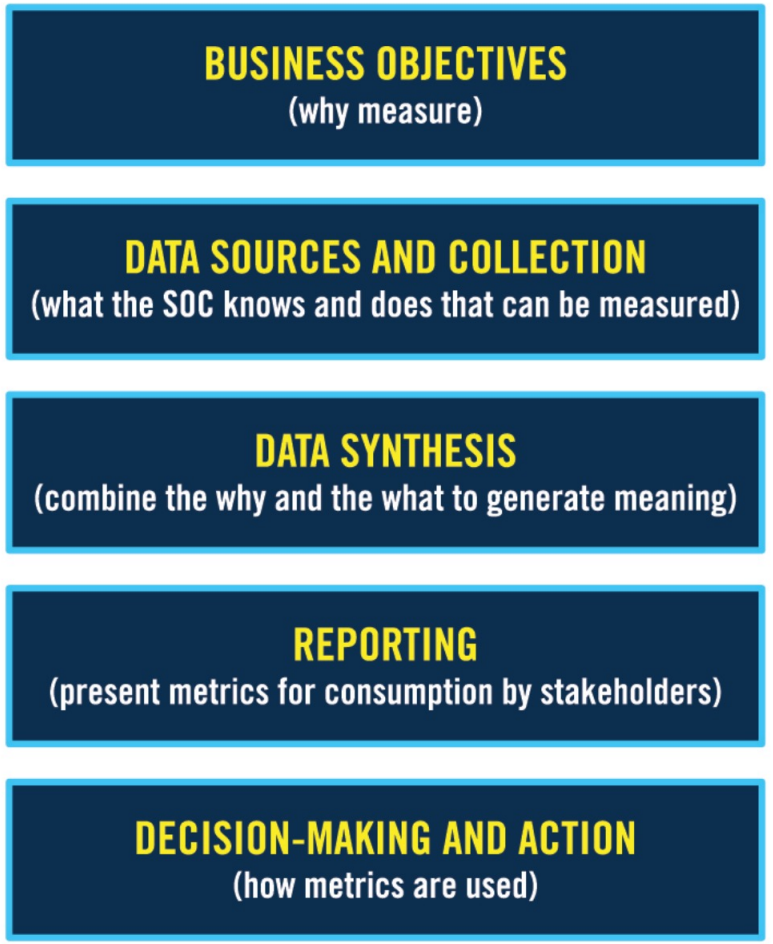


Figure 39. SOC Metrics Program

Challenges

Six Things to Keep in Mind

1. ***Defining Relevant and Measurable Metrics***
   - Start with thorough understanding of CSIRT operations
   - Align measurable outcomes accordingly

   - Keep it simple

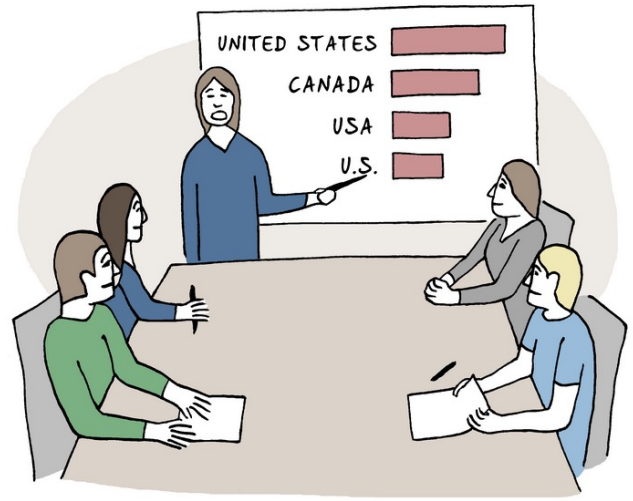
Challenges

Six Things to Keep in Mind

2. *Data Availability and Quality*

- Gathering accurate and reliable data
- Limitations in data collection tools
- Access to relevant data sources
- Inconsistent data quality

- Keep it simple



Challenges

Six Things to Keep in Mind

3. *Subjectivity in Measurement*

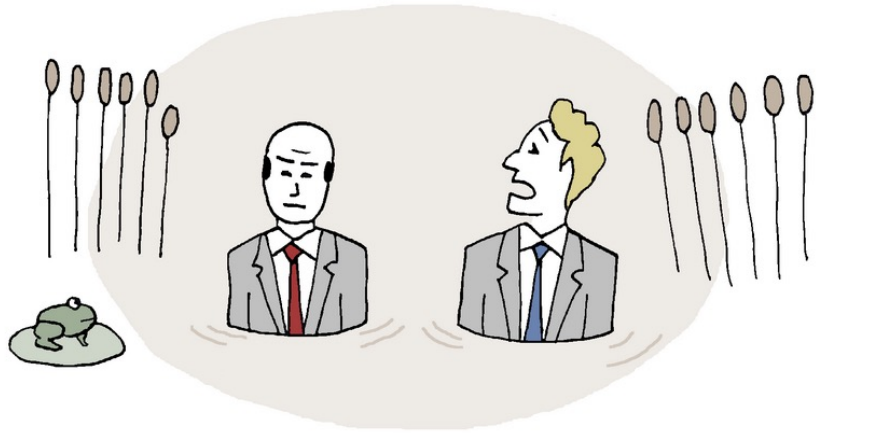
- Some aspects of CSIRT performance can involve subjective judgments (examples include incident severity, customer satisfaction, …).
- Ensure consistency andobjectivity in measuring such metrics.
- Avoid bias

Challenges

Six Things to Keep in Mind

4. *Balancing Quantity and Quality*

- Focusing on too many metrics can lead to information overload and diluted insights.
- Strike the right balance between quantity and quality of KPIs.
- Don’t take the fun out of IR
- Keep it simple



Challenges

Six Things to Keep in Mind

5. *Organizational Support and Buy-In*

- Provide clear communication of the benefits and value of KPIs
- Address any concerns or resistance to change

- Keep it simple

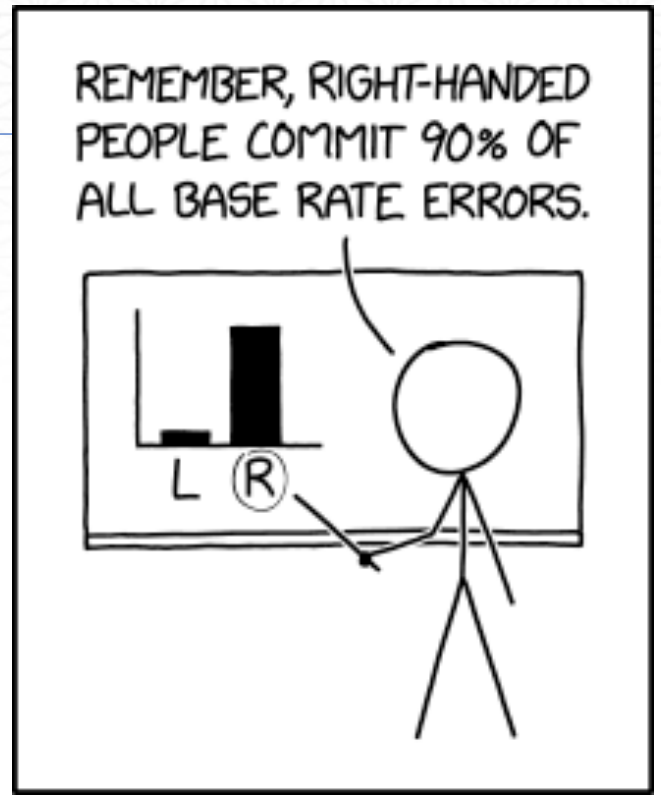
Challenges

Six Things to Keep in Mind

6. *Statistical Mistakes*

- Base Rate Fallacy
- Mean vs. Median (or other statistic)
- Sampling Error

- You may have to complicate things a little



Challenges

Base Rate Fallacy

Breathalyzer Example

- 100% True Positive
- 5% False Positive
- Driver tests positive. What are the odds they are actually drunk?

- 2%
- Out of 1,000 drivers on average:
- 1 TP, 49.95 FP
- Probability is (1 + 49.5) / 49.5 = 1.9

Sample KPIs

CSIRT KPI Categories

1. Threat Hunting
2. Incident Timeline
3. Incident Handling
4. Team Performance

Sample KPIs

Threat Hunting

1. ***Threat Detection Coverage:***
   - Evaluate the extent and comprehensiveness of threat hunting activities by measuring the percentage of the environment or specific systems covered by proactive hunting efforts.
   - This ensures adequate coverage across critical assets and areas of potential risk.

Sample KPIs
Threat Hunting

2. ***Hunting Efficiency (FP / TP)***
   - Use the ratio of confirmed threats discovered through hunting activities to the overall number of hunting engagements to evaluate process or content efficiency.
3. ***Threat Intelligence Utilization:***
   - Evaluate the integration and utilization of threat intelligence feeds, indicators, and analysis into the threat hunting process.
     - Per Indicator Source – TP / FP Ratio

Sample KPIs

Threat Hunting

4. *Data Source Usage*

- Evaluate your data sources for effectiveness and efficiency.
- e.g how many incidents can be attributed to each source? FP / TP Ratio, etc.

Sample KPIs
Threat Hunting

Using MITRE ATT&CK® as Coverage KPI

ATT&CK framework provides a comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs)

Tactics (why)

Name
Reconnaissance
Resource Development
Initial Access
Execution
Persistence

Techniques (how)

T1548 Abuse Elevation Control Mechanism
.001 Setuid and Setgid
.002 Bypass User Account Control
…
T1134 Access Token Manipulation
.001 Token Impersonation/Theft
.002 Create Process with Token
…
T1531 Account Access Removal
…

Sample KPIs
Threat Hunting

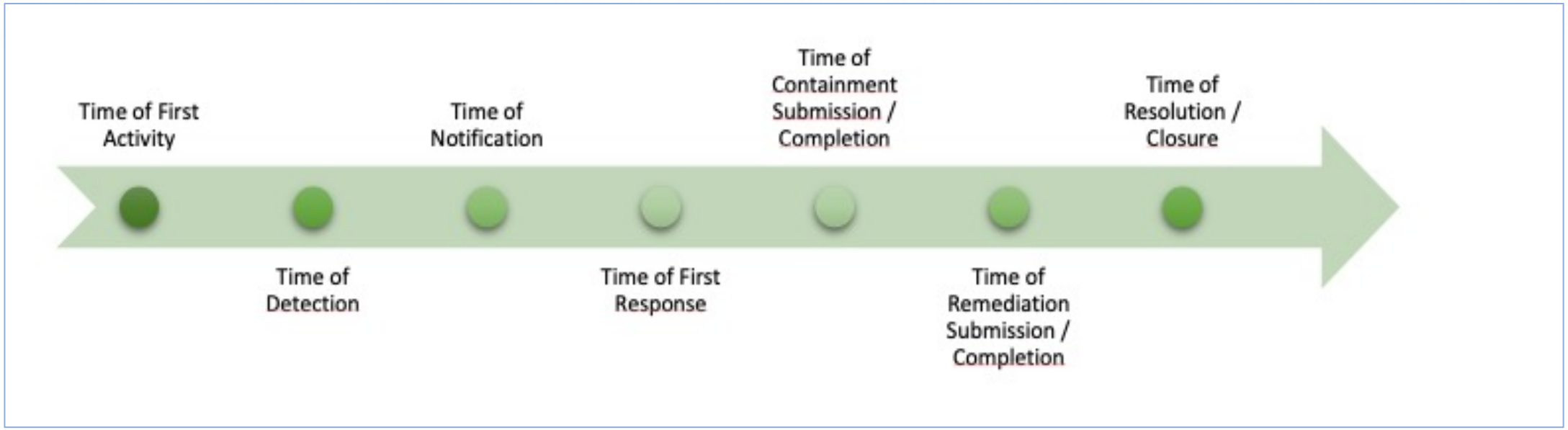
1. ***Map Security Controls***
   - Map your detection mechanisms to the specific techniques and tactics defined in the ATT&CK framework.
2. ***Analyze Coverage***
   - Assess the extent to which your security controls cover the various ATT&CK techniques and tactics.
   - This analysis helps identify any gaps in coverage or areas where improvements are needed.
3. ***Evaluate Detection Capability***
   - Evaluate the effectiveness of your detection mechanisms for each mapped technique and tactic.

Sample KPIs

Incident Timeline

[Link to Timing Document on first.org]

"Standard" Incident Timeline



- Capture timeline points
- Automate, automate, automate

Sample KPIs
Incident Timeline

TIMELINE RECORDS

1. ***First Activity***
   - The earliest event in a confirmed chain of events that led to the incident.
2. ***Detection***
   - A control, detection mechanism, or a human observer recognizes that an incident or suspicious activity has occurred
3. ***Notification***
   - The individuals responsible for investigating an event or incident are made aware of its detection

Sample KPIs

Incident Timeline

TIMELINE RECORDS

4. ***Notification***
   - The individuals responsible for investigating an event or incident are made aware of its detection
5. ***First Response***
   - Someone acts upon receiving a notification or alert related to the incident
6. ***Containment***
   - The incident is controlled and prevented from further spreading or causing damage

Sample KPIs
Incident Timeline

TIMELINE RECORDS

7. ***Time of Remediation***
   - An affected target asset is successfully restored to its pre-incident state or permanently removed from the environment
8. ***Closure***
   - When all necessary follow-up activities, analysis, reporting, and post-mortem processes related to the incident have been completed

Sample KPIs

Incident Timeline

Sample Metrics Derived from Timeline

Time of First Activity	*Time of Detection*	*Time of First Response*	*Time of Containment*	*Time of Remediation*
Time to Detect				
Time to Respond				
Time to Contain				
Time to Remediate				

Sample KPIs

Incident Timeline

KEY TIMELINE METRICS

Name	Importance	Goal (by tracking)	Formula
Time to Detect	High - Must-Have	Minimize the time it takes to identify and recognize potential security threats or incidents Enhance threat detection systems and reduce the dwell time of malicious activities	Time of Detection - Time of First Activity
Time to Respond	Medium - Recommended	Minimize the time it takes to mobilize incident response efforts and begin taking proactive steps to mitigate the impact of the incident. Enhance incident response efficiency, reduce the potential damage caused by the incident, and minimize the overall risk exposure..	Time of First Response - Time of First Activity

Sample KPIs

Incident Timeline

Key Timeline Metrics

Name	Importance	Goal (by tracking)	Formula
Time to Contain	High - Must-Have	Minimize the time it takes for an organization to halt the progression and impact of a security incident. Limit the potential damage caused by the incident, prevent further compromise of systems or data, and minimize the disruption to normal business operations.	Time of Containment - Time of First Activity
Time to Remediate	Medium - Recommended	Minimize the time it takes for an organization to restore normalcy and eliminate the root cause of the incident. Reduce the overall impact of the incident, minimize the potential for recurrence, and restore the affected systems or assets to their desired security posture.	Time of Remediation - Time of First Activity

Sample KPIs

Incident Handling

1. ***Incident Categorization Accuracy***
   - Measure the incident categorization accuracy can be done by comparing the categorization performed by the CSIRT with a reference or benchmark categorization (more later.)
2. ***Incident Trend Analysis***
   - Analyze incident data over time to identify patterns, trends, and recurring incidents.
   - Uncover insights into the organization's security posture, highlight emerging threats, and support proactive mitigation efforts.
3. ***Incident Backlog***
   - Monitor the number of open and unresolved incidents at any given time.
   - Assess the team's capacity and workload, ensuring that incidents are managed in a timely manner.

Sample KPIs

Incident Handling

4. ***Incident Escalation Rate***
   - Measure the percentage of incidents that require escalation to higher-level teams or external entities for resolution.
   - Identify the complexity and severity of incidents and highlights potential areas for improvement in the incident handling process.
5. ***Incident Documentation Completeness***
   - Measure the completeness and accuracy of incident documentation, including incident reports, post-incident reviews, and lessons learned.
   - Ensures that incidents are properly documented for future reference and continuous improvement.

Sample KPIs
Categorization Example

Sample Approach for Categorization Accuracy

1. ***Establish a Categorization Framework***
    - Define a standardized categorization framework that reflects the different types or classifications of security incidents relevant to your organization.
    - Make it comprehensive and well-documented.
2. ***Reference or Benchmark Categorization***
    - Select a set of historical or representative security incidents and perform an independent categorization by a knowledgeable and experienced team.
    - This is the reference or benchmark for accuracy comparison.

Sample KPIs
Categorization

Sample Approach for Categorization Accuracy

3. *Comparison and Analysis*

- Compare the categorization performed by the CSIRT for a sampled set of incidents with the reference or benchmark categorization.

4. *Create Accuracy Metrics*

- Calculate accuracy metrics, for example:

1. Accuracy Percentage: % of incidents correctly categorized by out of the total incidents evaluated.
2. True Positive Rate: Measure the proportion of incidents correctly categorized as belonging to a specific category out of all incidents in that category.
3. False Positive Rate: Measure the proportion of incidents incorrectly categorized as belonging to a specific category out of all incidents not in that category.

Sample KPIs
Categorization

Sample Approach for Categorization Accuracy

5. *Regular Monitoring and Feedback*

- Continuously monitor and assess incident categorization accuracy over time.
- Provide feedback to the CSIRT based on the results to help improve their categorization process, refine the categorization framework, or provide additional training and guidance.

Sample KPIs

Staff Management

1. *Staff training and certification*

- Measure the percentage of CSIRT team members who successfully complete required training programs, courses, or certifications within a specific timeframe.
- This KPI reflects the team's commitment to continuous learning and professional development.

2. *Customer Satisfaction*

- Obtain feedback from internal stakeholders, such as employees or system users, on their satisfaction with the CSIRT team's performance and support.
- This KPI measures the quality of service provided by the team and identifies areas for improvement.

Sample KPIs
Staff Management

3. *Employee Retention*

- Measure the rate of voluntary attrition at each role and seniority level.
- Pair this KPIs with exit interviews to identify issues or areas for improvement within the organization.
- This can also be used to work with senior management to provide evidence-based needs of training, additional staffing, or other team strengthening needs

4. *Skill Proficiency*

- Identify both strength and gaps in the various technical domains required to address the threats faced by the organization.
- Use this to work with senior management for additional training resources or to develop strategies to address gaps.
- Also showcase your skills!

Sample KPIs

Staff Management – Skills Matrix

SUBJECT
Operation Systems Basics
MacOS
Apple iOS
Linux
Android
Cisco IOS
Windows
Cloud Platform
Azure
Container Security
AWS
GCP
Kubernetes
Cloud Security Posture Management (J1, Wiz.io)
Infrastructure
Active Directory
Azure AD
Azure Cloud PC
Virtualisation - Citrix
Virtualisation - VMWare
SQL | Oracle
Virtualisation - M365
Exchange
Apache
Atlassian
Identitity Management (DUO/ Ping/ Okta)?

Endpoint Protection (log understanding)
Cisco Secure Endpoint (AMP)
OSQuery/ Orbital
Cisco XDR
MS INTUNE
Tanium
E-Mail
Office 365
Cisco Email Security Appliance
Networking
Networking Fundamentals
Routing and Switching
DNS & DHCP
NVM
IDS/ IPS
Netflow
Network Access Control (NAC)/Cisco Identity S
Cisco Secure Client (Anyconnect)
Web Proxy and Firewall
Malware and forensics
Windows Advanced/Forensics
Linux Advanced/Forensics
Sandbox/ (ThreatGrid)
Memory Forensics
Mac Advanced/Forensics
Mobile Forensic
Malware Reverse Engineering

Rating 1-10	
1	**Level 1-2: Novice**
2	•Understanding: Limited understanding of technical concepts, indicating a foundational knowledge base.
	•Autonomy: Requires significant guidance and supervision, suggesting a need for support and mentoring.
3	**Level 3-4: Beginner**
4	•Understanding: Basic understanding of key technical concepts, showing progress from the novice level.
	•Autonomy: Can perform simple tasks independently, demonstrating a growing ability to work autonomously.
5	**Level 5-6: Intermediate**
6	•Understanding: Demonstrates a good understanding of core technical concepts, showcasing a more advanced k
	•Autonomy: Can work independently on routine tasks, indicating increased self-sufficiency.
7	Level 7-8: Advanced
8	• Understanding: Possesses in-depth knowledge of technical domains, indicating a high level of expertise.
	• Autonomy: Can design and implement solutions independently, indicating a high degree of autonomy.
9	Level 9-10: Expert/Thought Leader
10	• Understanding: Achieves mastery of technical skills and concepts, indicating the highest level of proficiency.
	• Autonomy: Works with high degree of autonomy on highly complex and strategic initiatives. Recognized as a thc

Sample KPIs

From 11 Strategies of a World Class Cybersecurity Operations Center:

Table 24. Internal SOC Metrics

Metric	Example Measure and Target	Remarks
SOC tool health and welfare	% Uptime: 99.5 % Events successfully processed: 99%	The SOC should keep internal service availability metrics, not just based on OS uptime but the % of time that the service is available and working.
Data feed health	% Of sensors up: 98% % Of data feeds/collectors up: 98%	Data feed and sensor health is a constant challenge for the SOC. Things are always breaking. While rarely always 100%, the SOC should establish targets that keep most feeds running as expected.
Data latency through pipeline	Minutes from source to ingest (median): 5 minutes Minutes from ingest to data persistence (median): 5 minutes	The SOC is well-advised to measure the propagation of events and alerts through its pipeline. This will reveal issues that need to be addressed like gaps, throttling, backpressure, and time synchronization issues.
MITRE ATT&CK framework coverage	% Of tiles of interest for which the SOC has a detection: 25%	The SOC is strongly encouraged to ensure its detective, investigative and protective capabilities match adversaries of concern. For more, see: [208].
True/false positive ratio for detections	Ratio of alerts tagged by an analyst as true positive vs false positive: 50%	Different SOCs overall have different thresholds for what it considers to be “good enough” detection accuracy. Measuring this over time and by tool can be very revealing, especially of the SOC writes its own detections.

https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Exercises (1)

FIRST CSIRT Services Framework

The following exercises using materials from the FIRST CSIRT Services Framework which can be found at

https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

- Brainstorm a set of metrics for Function 5.1.2.
- Using the template, provide details for at least one of them

Exercises (1)

5.1 Service: Monitoring and Detection

5.1 Service: Monitoring and detection

Purpose: Implement automated, continuous processing of a wide variety of information security event sources and contextual data in order to identify potential information security incidents, such as attacks, intrusions, data breaches or security policy violations.

Description: Based on logs, NetFlow data, IDS alerts, sensor networks, external sources, or other available information security event data, apply a range of methods from simple logic or pattern matching rules to the application of statistical models or machine learning in order to identify potential information security incidents. This can involve a vast amount of data and typically, but not necessarily, requires specialized tools such as Security Information and Event Management (SIEM) or big data platforms to process. An important objective of continuous improvement is to minimize the number of false alarms that need to be analyzed as part of the Analyzing service.

Outcome: Potential information security incidents are identified for analysis as part of the Analyzing service.

The following functions are considered to be part of the implementation of this service:

- Log and sensor management
- Detection use case management
- Contextual data management

Exercises (1)

5.1.2 Function: Detection Use Case Management

- **5.12 Function: Detection Use Case Management**

Purpose: Manage the portfolio of detection use cases through their entire lifecycle.

Description:

- New detection approaches are developed, tested, and improved, and eventually onboarded into a detection use case in production.
- Instructions for analyst triage, qualification, and correlation need to be developed, for example in the form of playbooks and Standard Operating Procedures (SOPs).
- Use cases that do not perform well, i.e., that have an unfavorable benefit/effort ratio, need to be improved, redefined, or abandoned.
- The portfolio of detection use cases should be expanded in a risk-oriented way and in coordination with preventive controls.

Outcome:

A portfolio of effective detection use cases that are relevant to the constituency is developed.

Metrics Template

KPI	Values
Name	
Description	
Type	[Efficiency, Effectiveness, Implementation, Impact]
Data Required	
How is Data Collected	
Challenges	
Additional Notes	

Exercises (2)

1. Team Performance: Scenario

- You manage a team of analysts that conduct threat hunting (monitoring) through a well-defined process of systematic queries against your SIEM.
- These queries target specific threats, and each is run on pre-defined schedule (e.g., 4x daily).
- All analysts are expected to run any query as it comes up in schedule.
- Results/events are analyzed according to instructions and marked as True Positive, False Positive, Benign, or Duplicate.
- When analysis is inconclusive, the events are escalated to a next level team.

Exercises (2)

Team Performance: Exercise

- Brainstorm a set of KPIs that you might use to monitor this scenario.
- Select one or more of your KPIs and define it as per the previous exercise.
- Pay close attention to
    1. Why you are developing the metric. What does it tell you?
    2. What are the realistic challenges you may face implementing this metric?

Logan Wilkins

loganw@cisco.com

https://www.linkedin.com/in/loganw3/

Slide: