Logan Wilkins
Cisco, USA

KPIs for CSIRTs

TLP:CLEAR

Agenda

1. General Introduction
2. Overview
3. 12 Best Practices
4. 6 Challenges
5. Samples
6. Class Exercise

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

- Are measurable / quantifiable
- Assess progress & performance in achieving specific goals
- Evaluate the effectiveness or 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

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…

Building a KPI Program

Twelve Best Practices

1. *Define Your Objectives*

- Determine what aspects of CSIRT performance to measure & improve
- Align these objectives with the overall goals of your organization

Building a KPI Program

Twelve Best Practices

1. ***Define Your Objectives*** *examples*

- Ensure that our critical data collection systems are appropriately available
- Reduce amount of time analysts spend on specific detections

Building a KPI Program

Twelve Best Practices

2. *Select Relevant KPIs*

- Identify KPIs that align with your objectives & measure the desired performance aspects
- Make your KPIs
  - meaningful
  - measurable
  - actionable
- Consider categories such as threat detection, incident response, incident handling, & team performance

Building a KPI Program

Twelve Best Practices

2. ***Select Relevant KPIs*** *examples*

- Number of data collection systems that have criticality (or SLA) defined
- Availability trend and summary for critical systems
- Amount of analyst time required for each detection (play, report)

Building a KPI Program

Twelve Best Practices

3. *Establish a Shared Taxonomy*

- Words matter
- Understand regulatory & compliance requirements
- Adapt from existing frameworks – ATT&CK, CVCC, NIST…
- Validate, socialize
- Examples
  - “incident” vs. “case”
  - Category, Visibility, Sensitivity, Severity, …

Building a KPI Program

Twelve Best Practices

4. *Establish Baselines & Targets*

- Set baseline values
- Derive baselines from historical data, industry benchmarks, or internal performance expectations
- Set realistic targets or goals

Building a KPI Program

Twelve Best Practices

4. ***Establish Baselines & Targets*** *examples*

- 100% data collection systems that have criticality (or SLA) defined
- Critical systems availability target is 99.99%
- Current median analyst time for each each detection is 27 minutes. Target 33% improvement in next 6 months

Building a KPI Program

Twelve Best Practices

5. *Define Data Collection Methods*

- Determine how you will collect the necessary data to measure each KPI
- Establish accurate, reliable, & consistent data collection methods & sources
- Automate, automate, automate, streamlining data collection processes where possible

Building a KPI Program

Twelve Best Practices

6. *Establish Data Analysis & Reporting Processes*

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

Building a KPI Program

Twelve Best Practices

7. *Set Regular Evaluation Intervals*

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

Building a KPI Program

Twelve Best Practices

8. *Use Compensating Controls*

- 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
- May require manual review

Building a KPI Program

Twelve Best Practices

8. ***Use Compensating Controls*** *examples*

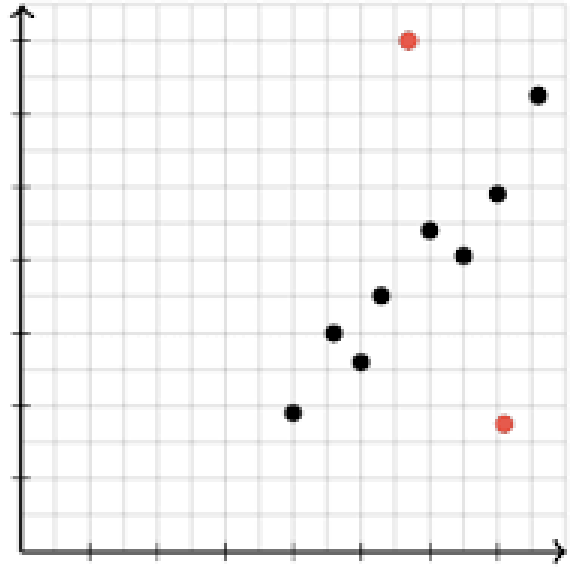
- Couple analyst Time To Complete with Analyst Escalation Ratio to ensure analysts aren't escalating to meet goal
- Manually sample Incident Categorization to ensure accuracy

Building a KPI Program

Twelve Best Practices

9. *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 & improve accuracy
- Watch sample size



Building a KPI Program

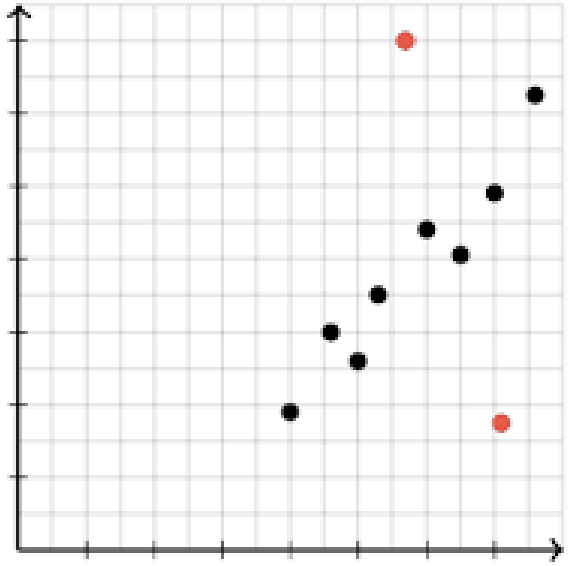
Twelve Best Practices

9. *Use Meaningful Statistics / Avoid Outliers* *example*

Time to
3
6
2
6
8
3
5
45
9
2

Mean: **8.9**

Median **5.5**



Building a KPI Program

Twelve Best Practices

10. Foster Stakeholder Engagement

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

Building a KPI Program

Twelve Best Practices

11. Improve, Act, Iterate

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

Building a KPI Program

Twelve Best Practices

12. *Document, Train, Support*

- Document the KPI framework, measurement methods, data sources, & analysis processes
- Maintain a record of results & insights
- Train CSIRT team on KPI importance & use
  - the specific KPIs being measured
  - how they are calculated
  - how their performance impacts CSIRT effectiveness

Challenges

Six Things to Keep in Mind

Challenges

Six Things to Keep in Mind

1. *Define Relevant & 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 & Quality*

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

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 & objectivity in measuring such metrics
- Avoid bias

Challenges

Six Things to Keep in Mind

4. *Balancing Quantity & Quality*

- Too many metrics can lead to information overload & diluted insights
- Strike the right balance between quantity & quality of KPIs.
- Keep it simple

Challenges

Six Things to Keep in Mind

5. *Organizational Support & 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

Base Rate Fallacy Example

Phish

You correctly flag 98% of actual phish emails (TP); incorrectly flag 2% (FP)

You assume an email flagged as a phish has a 98% chance of being a phish

Base Rate Fallacy Example

Phish

You correctly flag 98% of actual phish emails (TP); incorrectly flag 2% (FP)
You assume an email flagged as a phish has a 98% chance of being a phish

- 10,000 emails → 100 phish, 9,900 legitimate
- 100 * 98% = 98 TP alerts
- 9,900 x 2% = 198 FP alerts

} 296 alerts total

- 98 of 296 alerts = 33%

Your flagged email has a 33% chance of being a phish

Samples

Ideas for KPIs and Metrics

Sample KPIs

CSIRT KPI Categories

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

Sample KPIs

Threat Detection

1. *Threat Detection Coverage*

- Evaluate the extent & comprehensiveness of threat detection activities by measuring the percentage of the environment or specific systems covered detection

- This ensures adequate coverage across critical assets & areas of potential risk

Sample KPIs

Threat Detection

2. ***Detection Efficiency (FP / TP)***
   - Use the ratio of confirmed threats discovered through specific detection activities to the number of alerts to evaluate process or content efficiency
3. ***Threat Intelligence Utilization:***
   - Evaluate the integration & utilization of threat intelligence feeds, indicators, & analysis into the threat detection process

Sample KPIs

Threat Detection

4. Data Source Usage

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

Sample KPIs
Threat Detection

Using MITRE ATT&CK® as Coverage KPI

ATT&CK framework provides a comprehensive knowledge base of adversary tactics, techniques, & 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 Detection

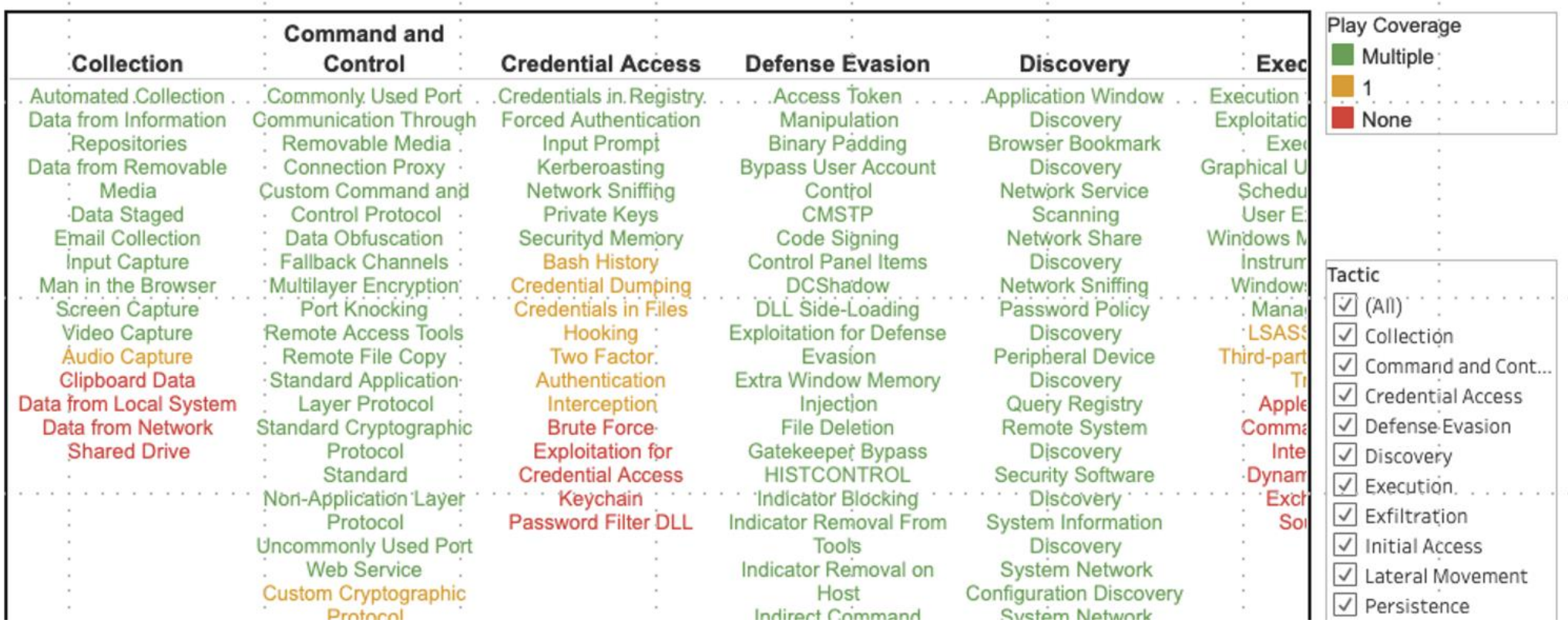
USING MITRE ATT&CK® AS COVERAGE KPI

1. ***Map Security Controls***
   - Map your detection mechanisms to the specific techniques & tactics defined in the ATT&CK framework
2. ***Analyze Coverage***
   - Assess security controls coverage against relevant ATT&CK techniques & tactics
   - Identify gaps in coverage or areas for improvement
3. ***Evaluate Detection Capability***
   - Evaluate the effectiveness of your detection mechanisms for each mapped technique

Sample KPIs

Threat Detection

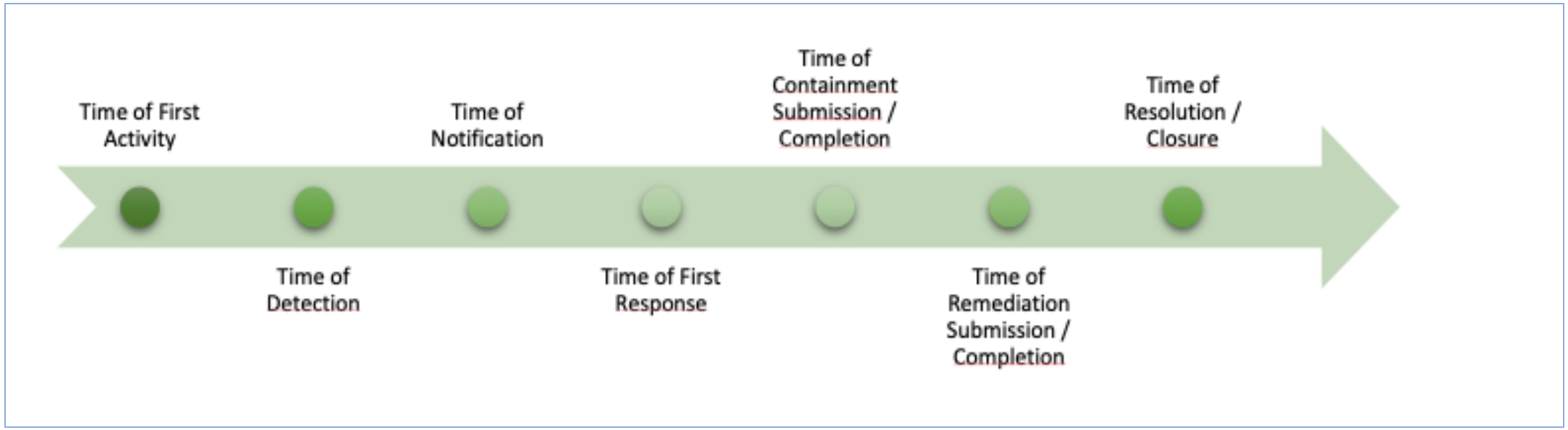
ATT@CK Coverage



Sample KPIs

Incident Timeline

"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 & 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, & 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, & recurring incidents
   - Uncover insights into the organization's security posture, highlight emerging threats, & support proactive mitigation efforts
3. ***Incident Backlog***
   - Monitor the number of open & unresolved incidents at any given time
   - Assess the team's capacity & 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 & severity of incidents & highlights potential areas for improvement in the incident handling process

5. *Incident Documentation Completeness*

- Measure the completeness & accuracy of incident documentation, including incident reports, post-incident reviews, & lessons learned
- Ensures that incidents are properly documented for future reference & continuous improvement

Sample KPIs
Categorization

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 & well-documented
2. ***Reference or Benchmark Categorization***
    - Select a set of historical or representative security incidents & perform a categorization by an experienced team
    - This is the reference or benchmark for accuracy comparison

Sample KPIs
Categorization

Sample Approach for Categorization Accuracy

3. *Comparison & Analysis*

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

4. *Create Accuracy Metrics*

- Calculate accuracy metrics based on the comparison results Commonly used metrics include:

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 & Feedback*

- Continuously monitor & 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 & guidance

Sample KPIs

Staff Management

1. ***Staff training & 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 & 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 & support
   - This KPI measures the quality of service provided by the team & identifies areas for improvement

Sample KPIs

Staff Management

3. *Employee Retention*

- Measure the rate of voluntary attrition at each role & seniority level
- Pair this KPI 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 & 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

Exercises

Two Exercises

Exercise 1

FIRST CSIRT Services Framework

The following exercise uses 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

Exercise 1

FIRST CSIRT Services Framework

Goal

- Develop useful metrics for specific CSIRT functions

Process

- Review the CSIRT Function
- Divide into groups
- Take 15 minutes to develop 2-3 metrics
- Present & review with larger group

Exercise 1

KPI Template

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

Exercise 1

5.1 Service: Monitoring & 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

Exercise 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.

Exercise 2

Threat Detection & Team Performance

Scenario:

- You manage a team of analysts that conduct threat detection (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.

Exercise 2

Threat Detection & Team Performance

- Develop a draft set of multiple KPIs that you might use to monitor this scenario (Consider brainstorming this draft)
- 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/

@loganw3.bsky.social

TLP:CLEAR