### Communication Strategy

No one is going to care how good your team is if you can’t communicate how good your team is.

One of the more underrated aspects of designing and operating a threat hunting organization is developing a strategy to communicate with leadership how the investment into threat hunting is generating a positive impact on the organization. If the only message the threat hunt team delivers to key stakeholders and leadership is whether threat hunting identified malicious activity, it will be extremely difficult to realize the full value threat hunting is bringing to the organization.

Detecting malicious activity is clearly part of threat hunting and when malicious activity is discovered through threat hunting, it should immediately be presented to leadership however, threat hunting can also improve the general security posture of the organization by reducing attack surface, improving detection capabilities, improve security data quality, and identify enablers of an attack.

The first step is to identify and generate valuable metrics and KPIs (see the Metrics section of the OTHF for more details on metric generation) which underpin the communication strategy of the threat hunting program. Without good data to back up your communications strategy there is very little chance for success. At the same time, if all you have is good data the likelihood of that data making an impact on the perception of the threat hunting program to leadership will be reduced.

A communication strategy can help the threat hunt program by tying together the relevant metrics into unified story which stakeholders can not only easily understand the data but also understand why they should care.

A threat hunting communication strategy should include:

* Goal
* Key Messaging
* Target stakeholders
* Metric alignment

**Goal** – Desired results for the program delivering the communication. The goal should align with short-, medium-, or long-term goals of the program.

**Key Messaging** – Whenever you communicate, you want each receiver to understand the basic points and takeaways. The basic points and takeaways are the key messages, and each receiver should be able to sum up the point of what is being said within a sentence or two.

**Target Stakeholders** – A stakeholder is any individual or that has an interest in an organization and the outcomes of its actions. With regards to threat hunting, there will likely be a core set of stakeholders such as the CSO and CISO however depending on the content of the communications, there may be additional stakeholders that will need to be receive the communications as well. Identifying and including the appropriate stake holders for the information is a vital component to effective communication.

**Metric alignment** – Metrics should not be the main component of the communications, but they should underpin the story of the communications. Mapping the correct metrics, to key messaging, to the appropriate stakeholders enables the communicator to select the 1 or 2 metrics that quantify the value of a specific data point for the organization, specific business unit, or team.

|  |  |  |  |
| --- | --- | --- | --- |
| Goal | Key Messaging | Stakeholders | Aligned Metrics |
| Highlight how the threat hunt team is becoming more efficient by identify threat hunts which can be automated and how automated detections from the threat hunt team provide the SOC with high quality alerts. Further buy into threat hunting team creating automated detections can be used for increase funding for data sources. | Threat hunting helps the SOC by creating actionable detections  Threat hunt team is continuing to scale by automating threat hunts through detections | CSO, CISO, SOC Manager | Number of threat hunts migrated to automated detections past 30 days  False positive reductions past 30 days |
| Goal 2 | Key Messaging 2 | Stakeholders 2 | Metrics 2 |
| Goal 3 | Key Messaging 3 | Stakeholders 3 | Metrics 3 |

With the communication strategy built, communications become easier to do and more importantly more effective. It is worth the time, to build out a Goal, Key Messaging, Stakeholders, and Metrics mapping for each of the metrics that you are tracking within your threat hunting program.