Cracking the Upper Management Code

KEVIN GARVEY

MANAGER – INCIDENT RESPONSE AND THREAT MANAGEMENT

TIME WARNER CORPORATE

Background

- Cyber Security for four years and eight in IT

- SIEM administrator for four years as well as an administrator of other cyber security toolsets

- Worked with many different groups within IT to help develop better relationships with Cyber Security

- Metrics is just as important to my job as finding the adversary

Challenges

- Metrics are not clear cut for upper management.
- Cyber Security is very often a cost center.
- Amount of alerts may be a good or bad thing.
- What else do you quantify metrics on?

Audiences

- Built in SIEM reporting is almost always good for technologist, maybe up to mid level management. However, reports should be seen by a much larger audience.

- Reports should be going outside of the Cyber Security department
  - Are they? If not, how come?

- What does upper management really care about?
  - Return on Investment
  - Reasons to keep renewing the product or to invest in talent
  - Remember Upper Management most likely either does not have access into your product tools or does not log in daily to notice trends.

What is the Story?

- What story are you trying to tell?
  - Are you overwhelmed with alerts?
  - Are your devices reporting the way you would like them to?
  - Are there deficiencies in the product line?
  - Is one person on the team closing alerts without proper investigation?
  - Are your alerts and investigations being impeded by forces outsides your control?
  - Is it time to invest in additional labor?
  - Would this data help out anyone else?

Visibility Case Study

- Case study of an alert as part of the metrics
  - Start to finish discussion about how the alert was taken care of, including what was involved with getting other groups involved in your investigations.
    - Assume upper management has never gone over an alert before
  - Discuss any financial impact the alert may have had or caused.
    - Was their downtime?
    - How can that be quantified?
    - How many hours per worker were put onto this alert?
  - Discuss challenges you had getting the alert fully triaged.

Data

- Data that SIEM solutions collect can help other groups
  - Can you use that data for regulatory requirement request?
  - Can Internal Audit use this data to help with their questions?
  - Can HR use the data to look through violations?
  - Can Privacy offers utilize this data for
  - Can Marketing use the data to see where traffic is coming from?

- Do other groups know this data is even being collected?

- Help make yourself indispensable my showing off the data collection or creating another repository for other groups.
  - This can be done through simple methods such as a spreadsheet or through deeper API connections.

Evangelize

- Upper Management is not limited to just IT upper management
  - What would other CxO positions like to see?
  - Remember, this is a very tight knit community at the top levels. Use it to your advantage.

- The more you communicate your successes and challenges, the more your toolsets and most importantly you and the team will be known and highly regarded throughout the company.

Teamwork Across the Company

“ Unity is strength… when there is teamwork and collaboration, wonder things can be achieved.
– Mattie Stepanek