RSA Conference 2019

BETTER.

LEARNING LABS

Bad Intelligence: Or How I Learned to Stop Buying and Love the Basics

Session ID: LAB2-T08

Heather Gantt-Evans, Heather.Gantt@ey.com

Brett Rogers, Brett.Rogers@ey.com

Larry Lipsey, Larry.Lipsey@ey.com

EY

Table of Contents

Session Summary

The purpose of this learning lab session was to introduce a business-based approach to building or refreshing a cyber threat intelligence program. This approach is designed to address many of the challenges we see in threat intelligence programs today, including: difficulty showing value, over-budget, over-scoped, and over-reliance on venders. By building a threat intelligence program in the same way we approach building a new company, many of these challenges are addressed through the normal steps of market research, customer and product validation, etc. Session participants were guided through applying this model and provided with artifacts to reproduce successful results.

Agenda

- The Current State of Threat Intelligence
- Our Solution, Build like a Startup
- First Step: Market Research & Group Participation Exercise I
- Second Step: Customer Validation & Group Participation Exercise II
- Third Step: Product Validation & Group Participation Exercise III
- Take Aways

Key Insights and Considerations

The Current State of Threat Intelligence

- Staffing struggles and high turnover rates
- Programs lack strong understanding of the operational environment “internal intelligence”
- Difficult to show value, often have small return on investment/effort
- Over budget, over scoped with data overload and heavy vendor reliance
- Failure to integrate with the rest of the business
- Based on a military model dropped into a civilian world

Our Solution, Build like a Startup

- Build your solution the way all successful businesses are built, a startup
- Key Tenants include:
    - Understand your threat (competitors) priorities
    - Understand and scope your customer base
    - Collect actionable feedback
    - Build a manual minimal viable product (MVP) first, before iterating to scale
- Work your way through the startup cycle and continue to grow your program in ways that show value to your leadership (investors)

First Step: Market Research & Group Participation Exercise I

Covered how to conduct initial market research on competitors (threats) by leveraging business data and security data to identify and prioritize market needs (threat scenarios).

Second Step: Customer Validation & Group Participation Exercise II

Covered how to identify, enable and prioritize, customers for a threat intelligence program. Specifically keeping in mind that intelligence resources are finite, participants made decisions on which customers to support based on what defensive capabilities those customers could provide to the business network.

Third Step: Product Validation & Group Participation Exercise III

Covered how to combine market research and customer validation in order to develop a collection plan. Exercise participants utilized the threat scenarios identified in exercise 1, and the enabled defensive capabilities/customer groups from exercise 2, in order to granularly break down threat scenarios into collection tasks that support prioritized customers.

Take Aways

- Discovered an end-to-end framework developed for cost-effective, custom integration of intelligence
- Learned how to implement custom workflows for the most valuable threat intelligence integration
- Walked away with real analytical artifacts and became confident in application to the business

Instructor Contact Details

Heather Gantt-Evans, EY

Heather.Gantt@ey.com

https://www.linkedin.com/in/heather-gantt-evans-m-s-cissp-a2b09299/

Brett Rogers, EY

Brett.Rogers@EY.com

https://www.linkedin.com/in/brett-rogers-cissp-08368216b/

Larry Lipsey, EY

Larry.Lipsey@ey.com

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