Introduction to the EASY Framework

Student Guide

Revision 2020.10.13

Table of Contents

Introduction and Background

Hello everyone, Thank you for enrolling in the Introduction to EASY framework course. This course serves a holistic frame of reference when building out threat intelligence programs.

My name is Chris Cochran. I've spent pretty much my entire career building out threat intelligence capabilities, starting in the government as a United States Marine and have also built Threat intelligence programs in Silicon Valley and all over the country. And I've combined all of this expertise and experience into what we're presenting to you today

My name is Ronald Eddings, I've spent my career architecting and building automation for cybersecurity programs. I am constantly a utility for translating business requirements into technical implementation.

The beautiful thing about the EASY framework is that it not only helps analysts that are building threat intelligence programs, but also those that need to make readjustment to get back on track. Both Ron and I have looked at threat intelligence from two different areas, and this is why we're bringing you the EASY framework today.

So why are we here? We're here because cybersecurity practitioners are constantly innovating as the threat is constantly evolving. While we adopt new tools and practices, organizations and cybersecurity programs begin to get stretched thin and experience inconsistencies with requirements and implementation. We're certain that any analyst viewing this content that has assisted or fully built a cybersecurity program has questioned

- Why are we doing this?
- Who is this for?
- What impact will it make?

As we take new roles or team membership changes, we'll have to continually answer these questions. Sometimes we'll run directly to google and attempt to implement the first security modeling framework we find - which may serve our purpose. The EASY framework can help your team identify which security framework works best given your team's needs and is comprehensible enough to be used alone.

The EASY Framework

It all began when I moved to Silicon Valley and became a Threat Intel Lead at an organization that was at the forefront of technology. Everything from the perspective of company culture to technology was so different. I had to realign myself as the person that was building out threat intelligence for this organization in order to fit this new dichotomy of technology. When I first arrived, I struggled and didn't know how I was going to make an impact because this organization didn’t have, and in some cases, didn’t need traditional security tools. I went home and I really sat and I focused on what do I need to do to make an impact?

While working at this organization, a very notable comedian joined us for a Q&A, Jerry Seinfeld. Someone asked Mr. Seinfeld, “what are you focused on now?” He said that now he is focused on mentorship and hopes to mentor the young up and coming comedians in efforts to give back to the community that he loves. This is our way of giving back to our community which has given so much to us.

When the EASY framework was created, the goal was to distill Threat Intelligence advice that I had for myself and others into something that could be understood and implemented effortlessly. The goal was to also create a touchstone for practitioners that are looking to build or correct threat intelligence programs.

The EASY Framework can enable you to resolve the difference of opinions between stakeholders and generate impactful requirements. More specifically, the framework can bring you back to base as a touchstone for threat intelligence practitioners and leaders that are aiming to either operationalize their threat intelligence or get their threat intelligence programs back on track.

- Elicit Requirements
- Assess Collection Plan
- Strive for Impact
- Yield to Feedback

Elicit Requirements

This is a step when building a threat intelligence program that is often overlooked or skipped. Eliciting requirements starts with identifying stakeholders and who would benefit from threat intelligence.

So many times I've seen it. I've done it. I've come into an organization where I brought in my prior requirements from another organization and immediately applied them to the organization that I was building the program for. This is not the best way to use threat intelligence.

During this step of the EASY Framework, the goal is to understand the business, people, processes, and technology. While enhancing threat intelligence capabilities you're likely supporting multiple teams or organizations. Work to establish a close working relationship with each team and its stakeholders. (Think Customer Success)

Fact-Finding

While working with multiple teams, it's going to be vital to understand the business and technical language of each team.

- What do they mean when they say vulnerability?
- How do they track critical events?
- What does a critical event mean to each team?

Also, a great question to ask is, who would be surprised by the result in threat intelligence?

- Which threat intelligence gaps are your stakeholders aware of?
- Which threat intelligence gaps were previously difficult to resolve?

There's also a possibility that your stakeholders have been burned by threat intelligence in the past and believe that threat intelligence is not something that the team needs. Socratic questioning can help identify threat intelligence pain points and team history

- Getting stakeholders to clarify their thinking and explore the origin of their thinking
  - ie) Why is APT X a threat? Could you explain further?
- Challenging stakeholders about assumptions
  - ie) Is this always the case? What details do we have?
- Providing evidence as a basis for arguments
  - Has there been reasons to doubt this evidence?
- Discovering alternative viewpoints and perspectives and conflicts between contentions
  - ie) Can/did anyone see this another way?
- Exploring implications and consequences
  - ie) But if...happened, what else would result? How does...affect...?
- Questioning the question
  - ie) Why do you think that I asked that question? Why was that question important? Which of your questions turned out to be the most useful?

Asking insightful questions and understanding the pain points of your stakeholders will enable you to make a greater impact. After you've met with teams and defined requirements, it's time to marry the requirements with the question of what information is needed.

Getting to Know The Team

- What is threat intelligence to you?
- When was the last time you needed information, but you didn't have it?
- When was the last time a piece of information would have saved you time, money, or resources?

Setting Expectations

- Previous attacks on the organization
- Are any teams using a threat modeling strategy?
  - Where are the areas where threat intelligence can help?
- What are your expectations with threat intelligence?
  - Any expected outcomes?
- If you're not able to hit this specific requirement that your stakeholder provided you, what's the worst-case scenario.

Avoid Non-Impactful Requirements

Some threat intelligence analysts have sent out weekly threat intel reports to internal teams just to find out that no one reads the report. While this may be a good way to show that you're attempting to be productive, there's no impact made from a report unless it is consumed by people or technology. All of the intelligence you provide should be impactful

Assess Collection Plan

Now it's time to figure out how to get the information that can satisfy your stakeholder's requirements. During this step, the goal is to identify internal and external data sources that can help produce threat intelligence. Assembling disparate data points could help formulate your hypotheses, analysis, and assessments.

More is not always merrier with threat intelligence data sources. There are always risks when trying to boil the ocean. For example, if we're inundating ourselves and other teams with threat intel feeds that internal tools can't consume then we are missing the point. Surveying industry peers while discovering internal and external data sources could be key to getting a headstart and avoiding pitfalls.

The point is to be surgical about your intelligence collection. You only want to collect what you can use, both internal to your network and external to the company. More specifically, looking for data that can help you make better decisions.

Internal Data Sources

- Network logs
- Application logs
- SIEM
- Incident Management / Case Management

External Data Sources

- Free and premium threat feeds
- Information Sharing and Analysis Center (ISAC) groups
- Threat reports
- Security news
- Social Media (ie. Twitter)
- Industry Peers

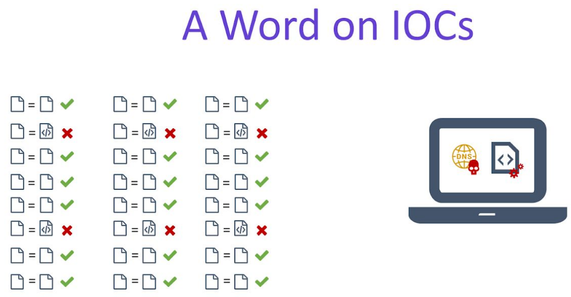
External data sources are helpful for staying informed about the threat and attacks. However, intelligence from external data sources can quickly become stale and due to volume can be hard to manage. Justify each external data source:

- How impactful is my threat feed(s)?
- Does my ISAC group help satisfy my requirements?
- Is anyone reading the security news and reports that I'm sharing?
- Do the tools and teams have the capabilities to ingest my threat intelligence?

Information sharing with industry peers and ISAC groups assists with developing a professional reputation and building relationships with other practitioners. Having the ability to ask questions, compare ideas, and stay informed leads to more opportunity to continually improve your threat intelligence capabilities.

Atomic and Computed IOCs

Threat intelligence is constantly evolving - years ago, teams relied on indicators of compromise (IOCs) for detection and response. For a time, this was helpful and still can be but fast-forward to today, there are millions of IOCs and no combination of threat intel sources that will protect against all threats.



Behavioral IOCs

In addition to atomic and computed IOCs, an important type of IOCs for threat intelligence analysts to track is behaviors. With behaviors, we're looking at the behavior of a network artifact or the behavior of an application.

As mentioned, Twitter is a great source for staying current with the latest threats and gaining insight from industry leaders. When assessing your collection plan, review what others in a similar industry have implemented and stay current on the latest news about threats affecting your industry.

Metrics

How is threat intelligence helping your organization? Gathering metrics can answer that exact question.

You can actually look at your sources and see how valuable those sources are based on metrics. How many reports did you receive from your premium threat feed? Premium threat feeds can be very expensive, but really understanding how many of those reports actually produced an incident or produced an action that someone had to take on an endpoint or an action that needed to be fixed at the firewall.

Automation

Threat Intel analysts often fall into the trap of too much data, time-consuming investigations, and manual repetitive actions. Automation can scale and enhance the capabilities of a threat intelligence team. Security products and services are becoming API centric, making it easier to integrate. All teams can benefit from taking a well-documented process and translating analyst logic into automation

- Use automation to collect, store, and help curate threat data feeds.
- Collecting metrics
- Repeating previous threat hunts
- Notifying stakeholders when threat actor activity is observed.

Identify Gaps

If you're on a small team, there's a good chance your analysts are not scouring the dark web to find sensitive information on your organization. Based on the requirements collected with stakeholders, identify the requirements that cannot be met. For example

- Technology gaps
- Process gaps
- Skill gaps

Strive For Impact

Strive for impact is one of the most important aspects of the EASY Framework. We've all been down the route of producing threat intelligence for the sake of seeming productive but our goal should be to really make an impact. More specifically, your intelligence should be saving your organization time, money, and resources.

Your requirements and collection plan are your roadmap for implementation and impact. During this part of the EASY Framework, you should know clearly whether or not your team has the ability to fulfill the requirements that were collected. If so, it's time to begin prioritizing the work that needs to be completed. It's a good idea to review which aspects of your program need resources from other teams and create a plan for completion. The last thing that you want is to find out that other team resources are busy and coming up short on deadlines

Whether you are a one-person threat Intel shop or a team of multiple analysts there are limits to the number of requirements that your team can support. You may need to leverage the relationship built with your stakeholders and revise the original plan. Regularly review which requirement is the most important and what is the team's current focus. Confirm that priorities are set for the organization and addressing top threat intelligence opportunities.

Impact Levels

- Is your threat Intel capability saving your organization time?
- Are you adding a capability that is valuable to your organization?

If a requirement was identified as - Creating the capability to perform threat hunting in your environment and your team focused on adding threat feeds with existing feeds, time and reputation could be lost by not addressing the requirement completely.

When we talk about prioritization and we talk about saving time, it’s important to look at what are the metrics that we can use to help measure how impactful our team is being for the bigger organization.

The Intelligence I sent to you…

- Were you able to do anything with it?
- How many times did someone make a decision?
- How many times were actions taken when your team provided intelligence?
- Were you able to use it?

Planning for Success

There are so many times where analysts are putting out products that no one was reading. You're spending so much time doing things that no one's going to actually use. There was a time where I was with an organization and we spent the better part of a year developing a single report that was hundreds of pages long. Unfortunately, I found out later that no one read it.

Another way to create an impact after you’ve gathered requirements and assessed your collection plan is creating a draft and inviting your customers or stakeholders. to review More specifically, team members that can give you valuable feedback. Maybe it's a security analyst or a security engineer that you can leverage to vet your threat intelligence product. Creating drafts, or using a dev environment is a great way to constantly create opportunities for proactive feedback. Before your final product is complete.

Cybersecurity programs were previously the department of NO

- No, you cannot download this
- No, we cannot use this application
- No, we cannot use this infrastructure.

But really that's not what that really, that's not what cybersecurity is anymore.

So really thinking about what, from an impact perspective, can you do to provide that security program with the information that it needs to be as efficient and effective as possible and push that organization to its limits and innovation and the enterprise.

Yield To Feedback

Feedback is a process that leads to continual impact. Find opportunities to constantly retrieve feedback for your threat intelligence program. As relationships are established with your stakeholders, their review is going to be essential to further development.

Feedback Forms

Create a web form (ie Google Forms) to collect feedback from threat intel consumers. Chris built a Google Form that contained inputs that his stakeholders would fill out which helped to measure impact and relevance. The form took about 45 seconds to fill out and had 100% participation from the team. The form to collect feedback was sent via Instant Message - opening a channel for more communication if needed. The form contained two questions:

1. Relevant was the intelligence provided? (1-5)
2. How impactful is this for your team? (1-5)

Measuring relevance can help identify if you're giving threat intelligence to the right teams - and is it helping them. If you measure for relevancy often, you can quickly find if your intelligence program is improving. Also, metrics can help you set goals. For example, as you introduce new capabilities you can measure the change of relevancy as new features are added.

Feedback might also be an indicator for team growth, as metrics and feedback are collected - if the program is thriving and having growing pains, it may justify adding additional team members. To gain more insight about a strength or weakness, add more questions to your feedback form.

IMMEDIATE IMPACT ACTION:

Invite stakeholders or customers to review and provide feedback on your requirements and collection plan.

When looking at the impact that you made, there are always opportunities to grow. There's always going to be something that you can do to enhance your threat intelligence capability or program. Providing your team's feedback to stakeholders may invoke more opportunities to add capabilities and better requirements.

You should also assess your threat intel program as an analyst. Self-directed feedback can also be a form of documentation that can highlight the challenges and successes of the team. Some feedback points to comment on for your program:

- What could you do to improve results immediately?
- What problematic points of the requirement?

One of the key components of threat intelligence is communication. There have been many times when I'm working with a stakeholder and maybe we're missing the mark, but it's difficult to fix things with rigid communication. Feedback can be viewed as a suggestion for adjustment. With communication being a component of threat intelligence, relationships need to be constantly built and maintained.

The Future For Analysts

I believe that threat intelligence, practitioners, and leaders have a unique perspective within cybersecurity. They touch so many different functions within and outside of an organization. Threat intel analysts are interfacing with Engineering, Marketing, and C-suite. And so they have a unique perspective for how everything works together. Our belief is Intelligence experts and practitioners will consistently grow to acquire positions as head of security and ultimately obtain the title of CSOs.

The CSO of the future is going to be the nexus between risk and innovation. Threat Intel analysts often have to survey the entire landscape of an organization. They need to be able to answer security-related questions for all teams to help protect data, users, and assets.

Conclusion

- Eliciting requirements from your stakeholders - Avoid creating your program in an echo chamber of previous experience - Focus on the needs of your organization and stakeholders.
- Assessing the collection plan - having a plan and a strategy for how you're going to get the information that you need to support your organization.
- Striving for that impact - moving the needle forward for the threat intelligence program and staying flexible to adjust as needed
- Yield for Feedback - Measure the impact of the threat intel programs and develop ongoing relationships with the organization.

The challenge will remain evolving as quickly as the threat landscape - our solution is to always have our frame of reference is to look at and implement the easy framework and build the best threat intelligence programs that we can.

And with that, we hope you enjoyed this course. Be sure you take the assessment. Remember everything that we've talked about in this course, and we hope you build the best threat intelligence capability that you can.