Introducing the PEAK Threat Hunting Framework

Cybersecurity is an ever-evolving game of cat and mouse. As security experts come up with new ways to protect valuable digital assets, cybercriminals develop craftier techniques to bypass these defenses.

Enter threat hunting — the proactive practice of ferreting out those sneaky cyber-rodents. Or, if you insist on a more formal definition, "any manual or machine-assisted process intended to find security incidents missed by an organization's automated detection systems." Either way, hunting is a great way to drive improvement in automated detection and help you stay ahead of the attackers.

Of course, we want our threat hunting operations to be a well-oiled machine, something documented and repeatable so we're not continually making things up as we go. That's where the PEAK Threat Hunting Framework, brought to you by SURGe by Splunk, comes into play.

In this article, we'll introduce you to PEAK, a cutting-edge approach to threat hunting, designed to adapt and thrive in today's dynamic cybersecurity landscape. Over seven articles, we've described in detail how to hunt with PEAK:

What's a Threat Hunting Framework?

Before we dive into the world of PEAK, though, let's take a step back and talk about threat hunting frameworks in general.

A hunting framework is a system of repeatable processes designed to make your hunting expeditions both more reliable and more efficient. They help you understand:

- What types of hunts exist
- Which type might be most appropriate for your specific hunt
- How to perform each type of hunt
- What the outputs could or should be
- How to measure success

With a trusty framework by your side, you're armed with a clear set of guidelines that can be tailored to your specific needs for each hunt. In essence, a framework provides repeatable processes and improves both the efficiency of your operations and the quality of your outputs.

While there are already a few frameworks out there — like the Sqrrl Threat Hunting Reference Model (which I helped create and was first published in 2015) and TaHiTI, created by the Dutch Payments Association in 2018 — they're starting to show their age. As our hunting programs continue to evolve, we need a framework that incorporates the additional experience and lessons we've learned in the last several years.

And that brings us to PEAK.

The PEAK Framework: Threat Hunting, Modernized

PEAK, an acronym for "Prepare, Execute, and Act with Knowledge," brings a fresh perspective to threat hunting. It incorporates three distinct types of hunts:

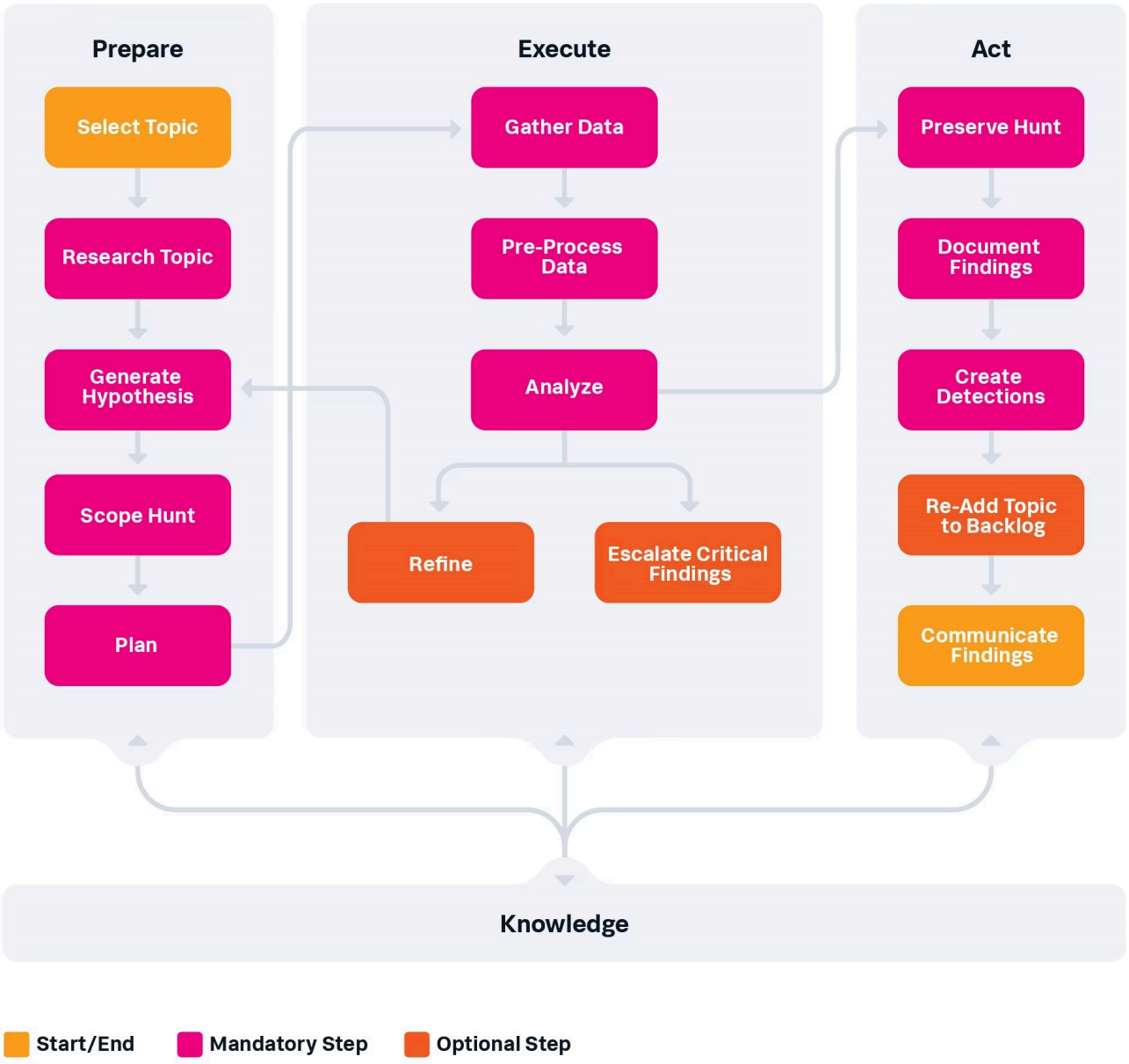
Each PEAK hunt follows a three-stage process: *Prepare*, *Execute*, and *Act*. In the *Prepare* phase, hunters select topics, conduct research, and generally plan out their hunt. The *Execute* phase involves diving deep into data and analysis, while the *Act* phase focuses on documentation, automation, and communication. Crucially, each phase integrates *Knowledge,* which could be in the form of organizational or business expertise, threat intelligence, prior experience of the hunter(s), or of course, the findings from the current hunt.

Oh, and did we mention that PEAK is flexible like a cybersecurity ninja? We include detailed process diagrams and descriptions that show how most hunts of each type work to guide you while constructing your specific hunt. Hunters can skip, reorder, or add steps to each phase, tailoring their approach to suit the situation at hand.

Hypothesis-Driven Hunts

This is the classic approach, where hunters form a supposition about potential threats and their activities that may be present on the organization's network, then use data and analysis to confirm or deny their suspicions.

Hypothesis-Driven Hunting Process in the PEAK Framework

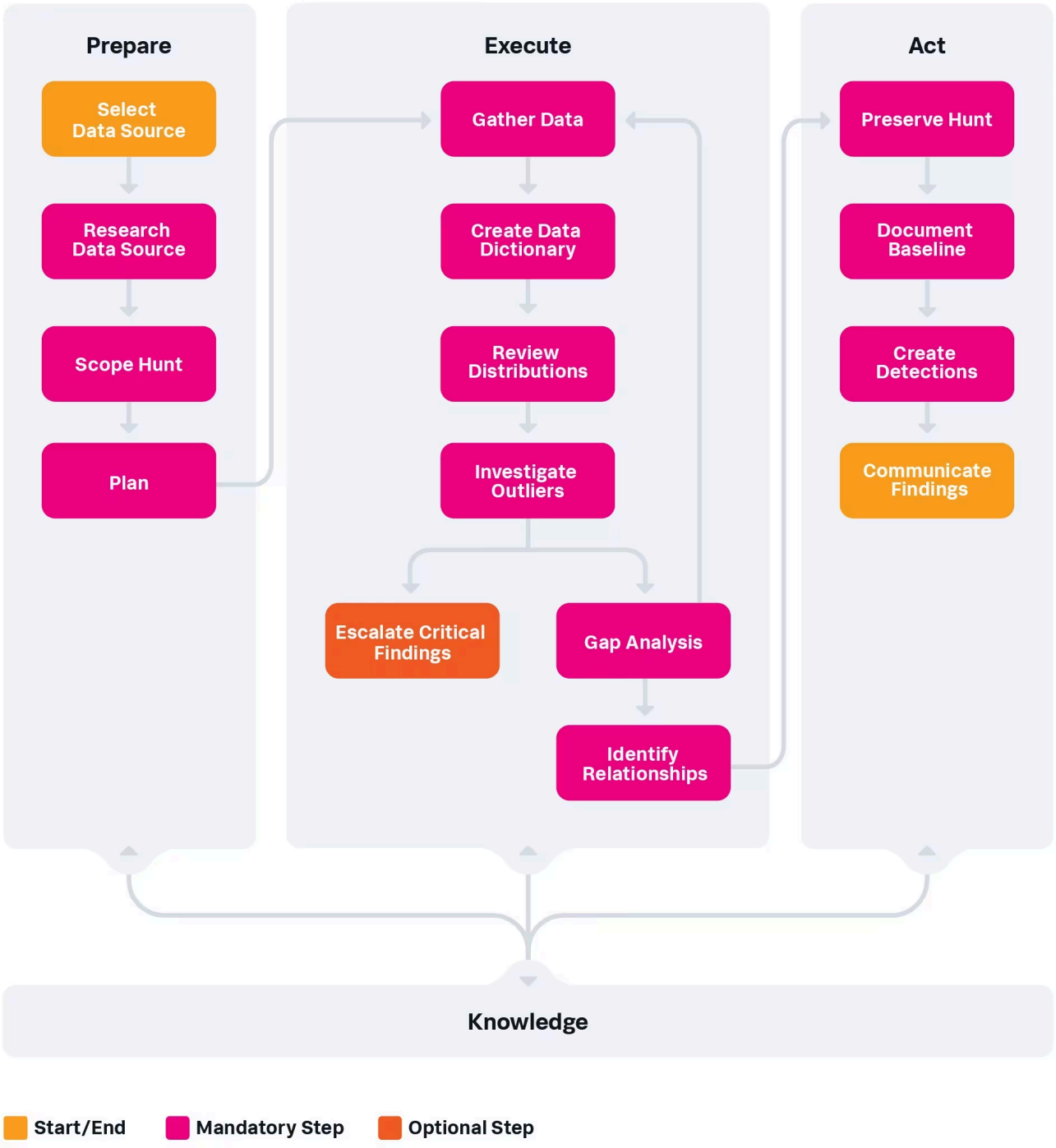


➡️ Read our in-depth explainer of hypothesis-driven hunts in PEAK.

Baseline Hunts

In this type of hunt, hunters establish a baseline of "normal" behavior and then search for deviations that could signal malicious activity.

The Baseline Hunting Process in PEAK

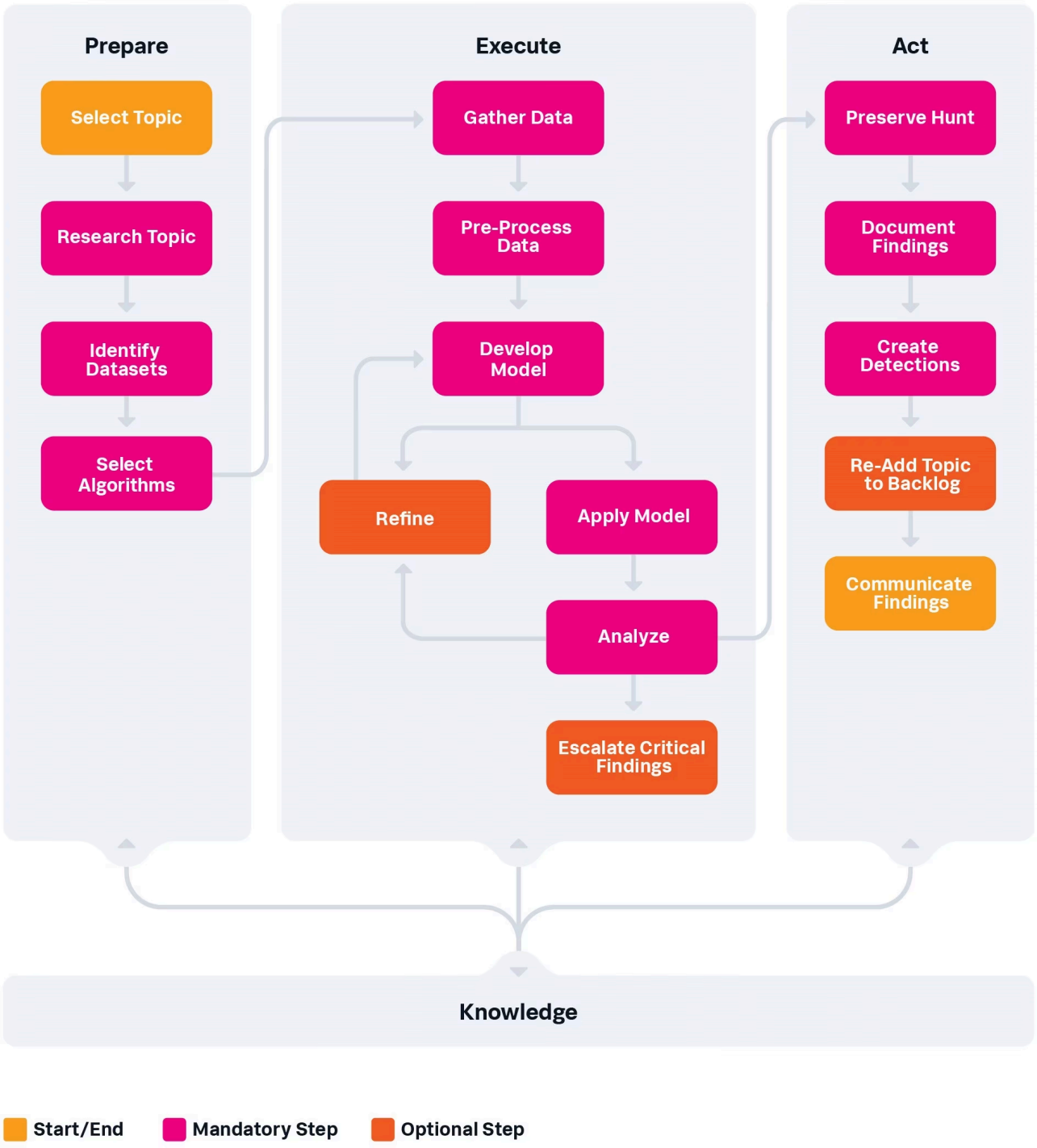


➡️ Learn the who, what, where and why for baseline hunting with PEAK.

Model-Assisted Threat Hunts (M-ATH)

M-ATH hunts could be accurately described as "Sherlock Holmes meets artificial intelligence." Hunters use machine learning (ML) techniques to create models of known good or known malicious behavior and look for activity that deviates from or aligns with these models. Think of this as almost like a hybrid of the hypothesis-driven and baseline types, but with substantial automation from the ML.

Model-Assisted Threat Hunting (M-ATH) Process in PEAK



➡️ Get all the details on M-ATH in this dedicated tutorial.

PEAK Highlights

Now that you're acquainted with PEAK, you might be wondering what sets it apart from the crowd. Well, here are a few of its standout features:

- **Modernized hunt processes**: PEAK incorporates experience gained and lessons learned from conducting real-world hunts over the past several years and is fully up-to-date with the latest threat-hunting trends and approaches.
- **Standardized and integrated content:** PEAK brings together the best hunting methodology, terminology, and concepts from across the Internet – all in a consistent format, with examples!
- **Comprehensive and adaptable approach**: PEAK offers versatile, customizable processes for hunting down cyber threats while making it easy for security teams to adapt those processes to meet the needs of specific hunts.
- **A blend of manual analysis and machine learning**: With the M-ATH hunt type, PEAK combines the best of human intuition and practical machine learning to create a formidable threat detection methodology.
- **Improved efficiency and effectiveness**: By offering repeatable processes, embracing a range of hunting techniques, and adapting to different situations, PEAK allows security teams to hunt with greater precision and speed.

Conclusion

In the ever-changing world of cybersecurity, staying ahead of the curve is crucial. The PEAK framework, with its unique blend of Hypothesis-Driven, Baseline, and Model-Assisted hunt types, provides a repeatable, flexible, and modern approach to threat hunting. As a result, organizations can defend against evolving threats more effectively than ever before.

So, there you have it — a preview of PEAK (you might even call it a “sneak PEAK”). Want to know more? Excellent, because we're just getting started! Explore the supporting articles, papers and other media diving deeper into the PEAK framework and threat hunting in general.

As always, security at Splunk is a family business. Credit to authors and collaborators: David Bianco, Ryan Fetterman