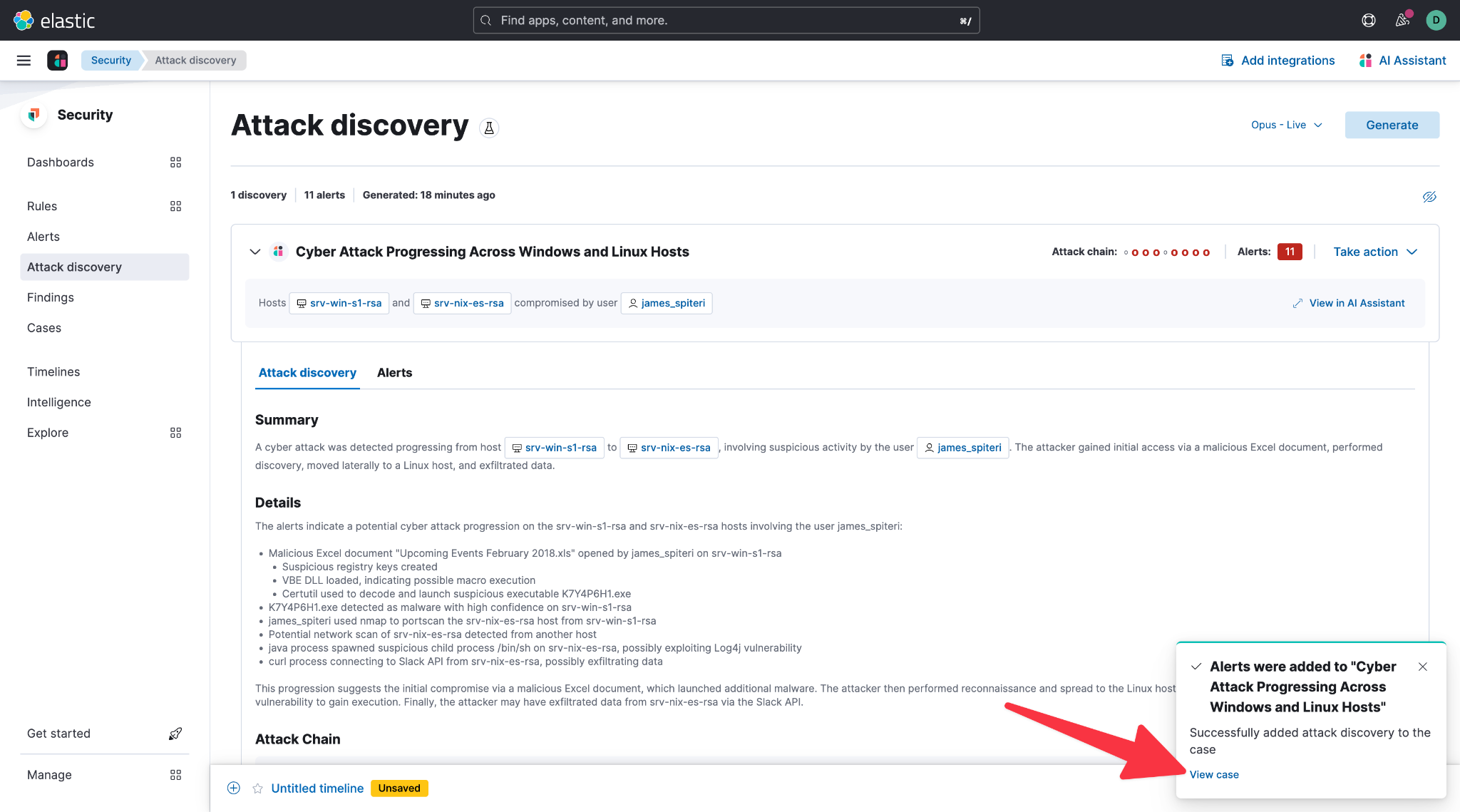
# Attack Discovery Demo Talk Track

## Introduction

Today, I’m thrilled to introduce our latest addition to Elastic Security: Attack Discovery.  
  
Attack Discovery is designed to help security operations teams of all sizes triage and investigate alerts quickly using generative AI. Let’s dive right in and see how it works!

## Exploring the Alerts View

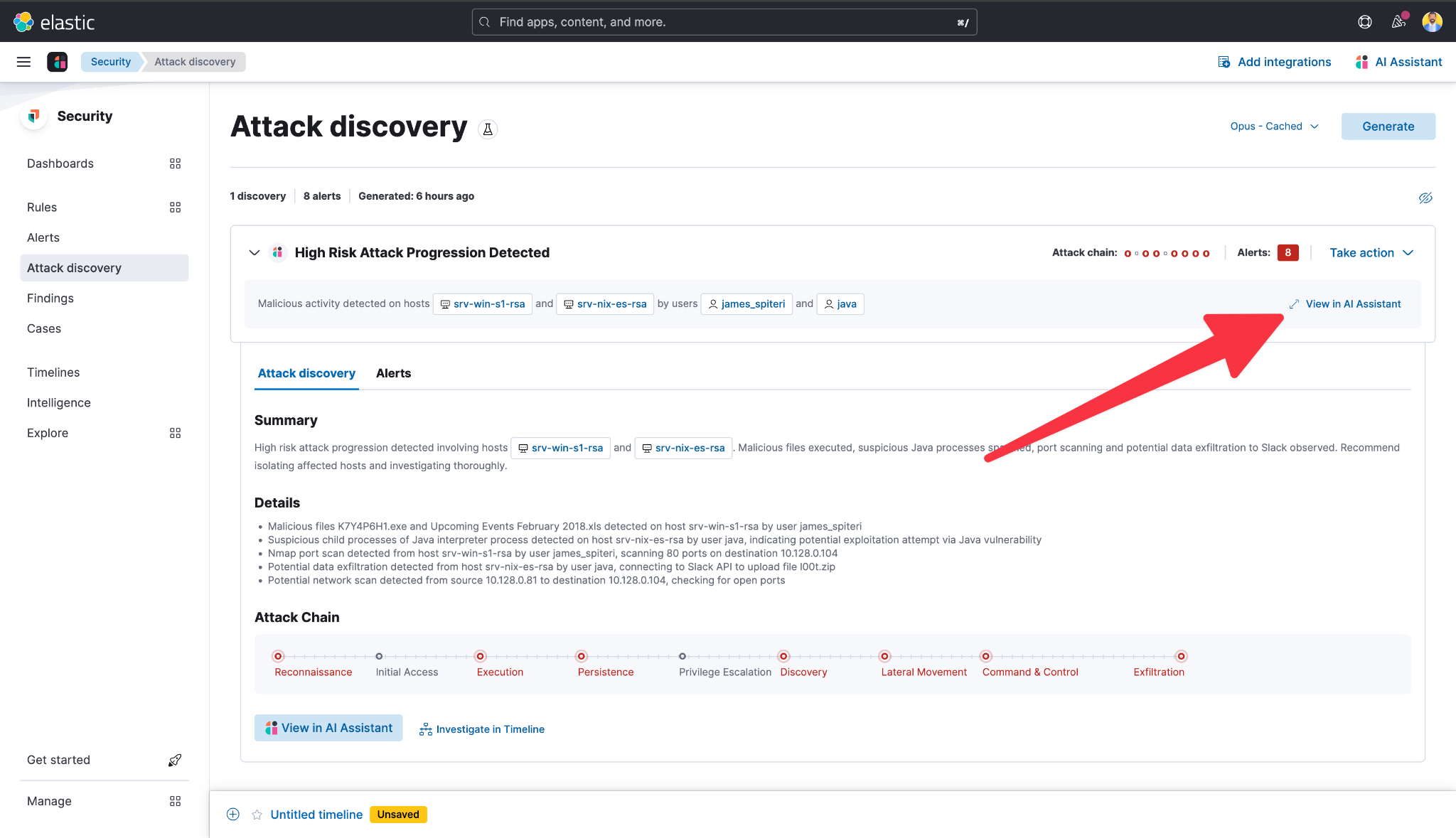
What you see on my screen right now is the Alerts View in Elastic Security.



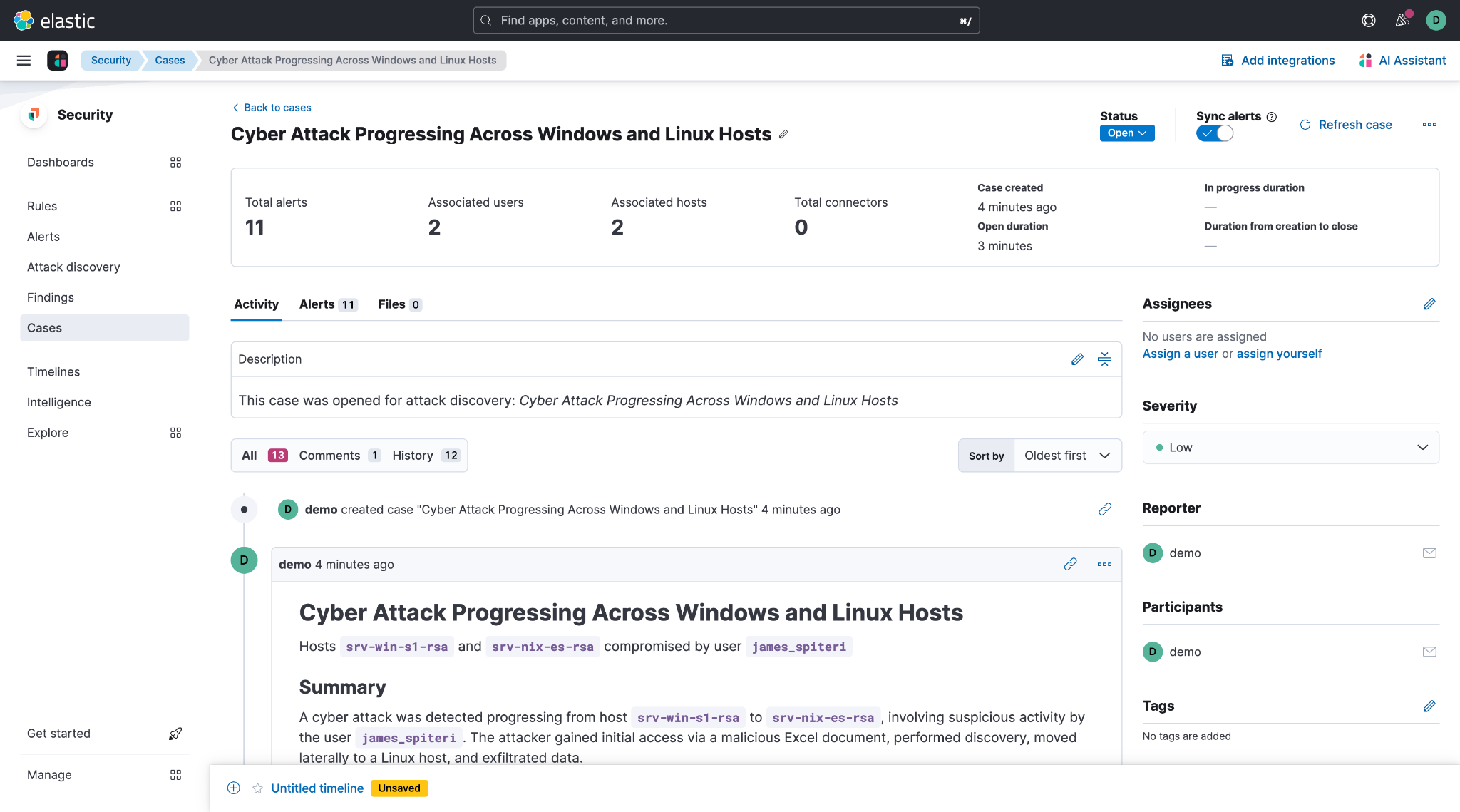
This is where security analysts typically begin their daily operations, reviewing alerts triggered within their environment.  
  
These alerts come from two main sources:  
- Elastic Security’s built-in detection rules powered by our Security Labs team.  
- Custom rules that you or your team have created.  
  
So, If you notice on the Alerts page, I have 108 alerts to analyze. While that’s not an overwhelming number, it still presents the common challenge security teams face daily: Where do I start?  
  
This is where Attack Discovery comes in.

## Introducing Attack Discovery

Instead of manually sifting through all these alerts, I can pivot to the Attack Discovery tab.

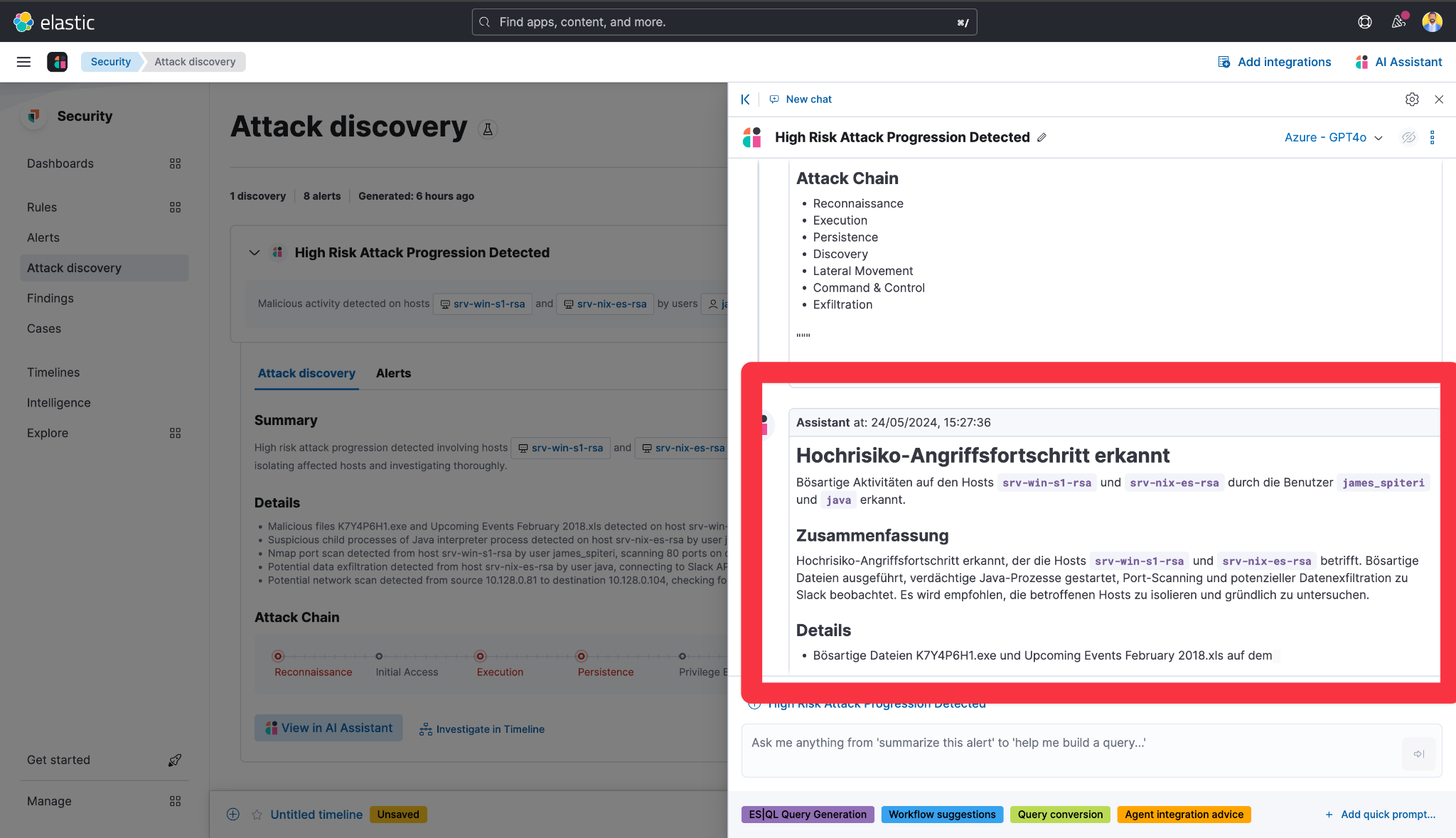


Here, we’ve designed a simple and intuitive interface that makes it easy to analyze alerts using generative AI. So In this case, it will process all of the 108 alerts at once.  
  
A key advantage of Elastic is that we allow you to integrate any large language model (LLM) of your choice. You can see here that I’ve selected my preferred model, and Elastic’s powerful search and AI capabilities will ensure accurate and actionable results.  
  
Once I’ve selected my model, all I need to do is click 'Generate' to begin the analysis.



## Reviewing Attack Discovery Results

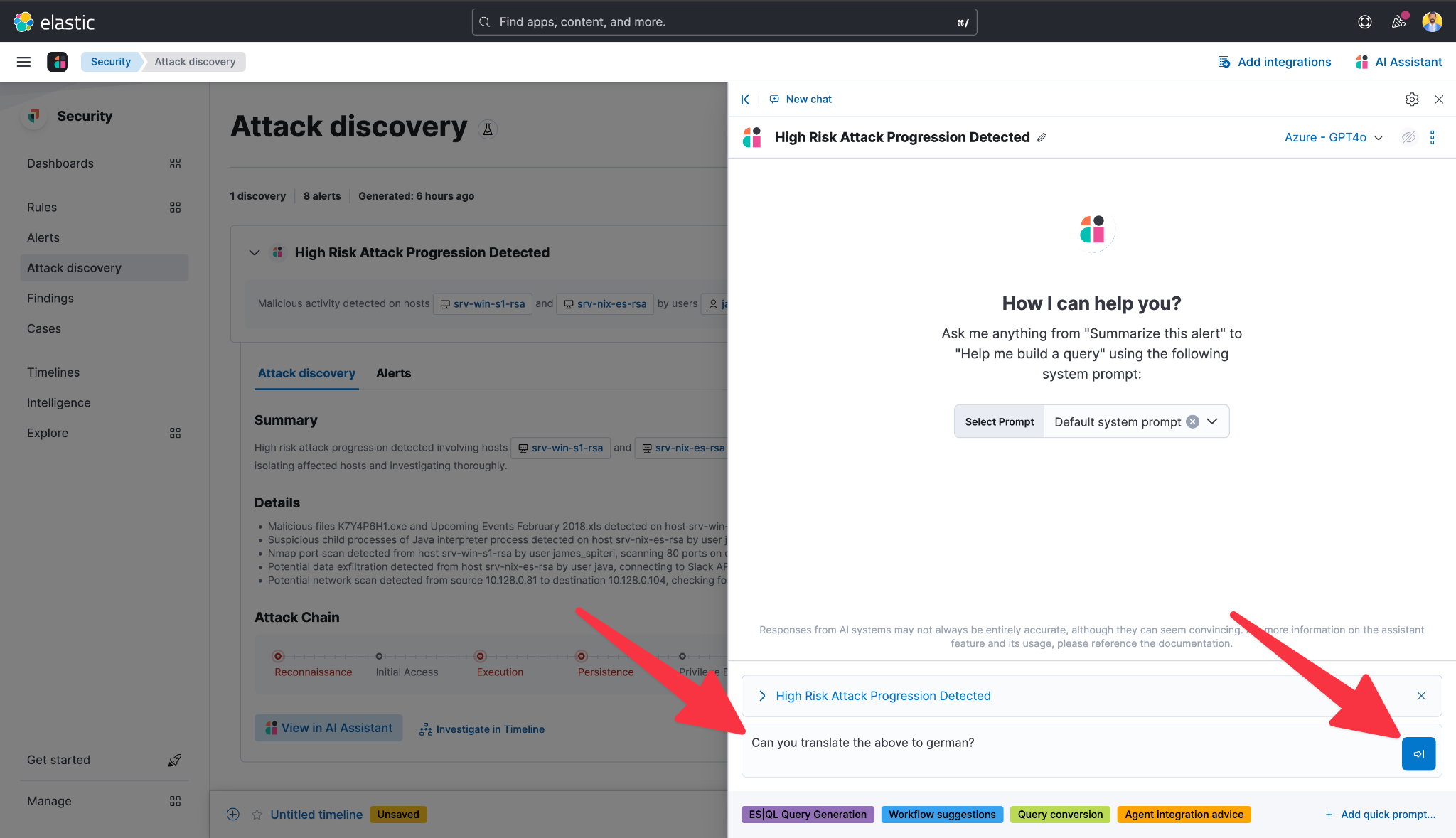
Now that the results are in, let’s take a look.



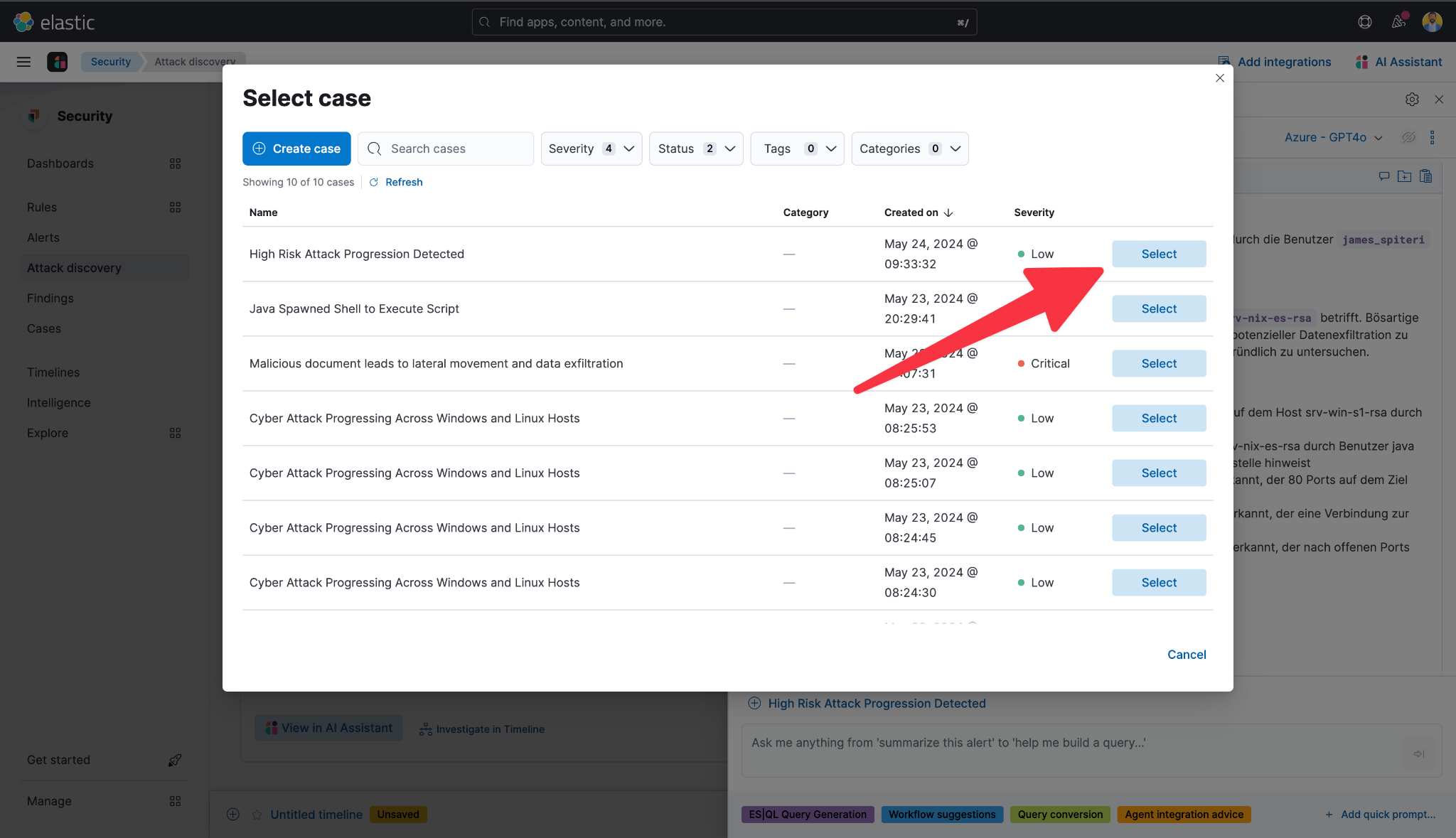
At the top, we get a high-level summary of what happened:  
- The alerts have now been grouped into key discoveries, which represent the active security incidents within my environment that require further investigation.  
  
Each discovery has a clear and descriptive title, making it easy to understand the nature of the threats at a glance. For example:  
- Malware attack on macOS  
- Ransomware attack  
- Malicious Office document attack  
  
Let’s dive into one of these discoveries.

## Deep Dive into a Discovery

Attack Discovery has automatically correlated alerts and provides a structured summary for quick analysis.



Key Findings:  
- Entities involved: Affected host and user details  
- Suspicious behavior detected:  
 - Execution of untrusted code  
 - Credential phishing attempts  
 - Failed code signature validation  
- MITRE ATT&CK mapping for contextual threat intelligence  
  
This summary gives me instant situational awareness, allowing me to quickly assess the severity and impact of the attack.  
  
If I need to investigate further, I can pivot directly to the Alert View, where I’ll see the original alerts that contributed to this discovery.

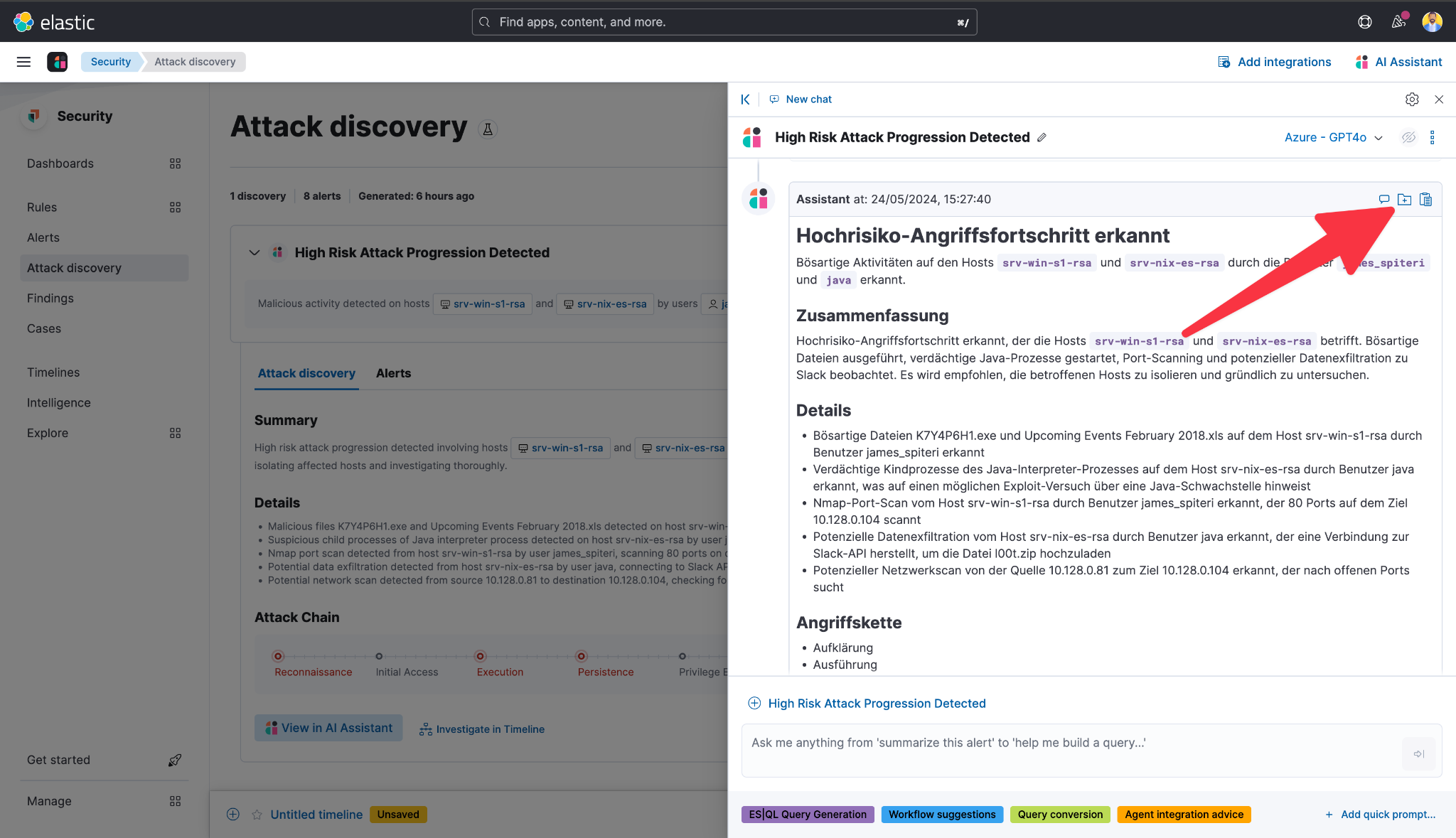


## Streamlining Incident Response

Investigating an attack is only half the battle—acting on it is just as critical. Elastic Security makes that process seamless.

### Creating a Case

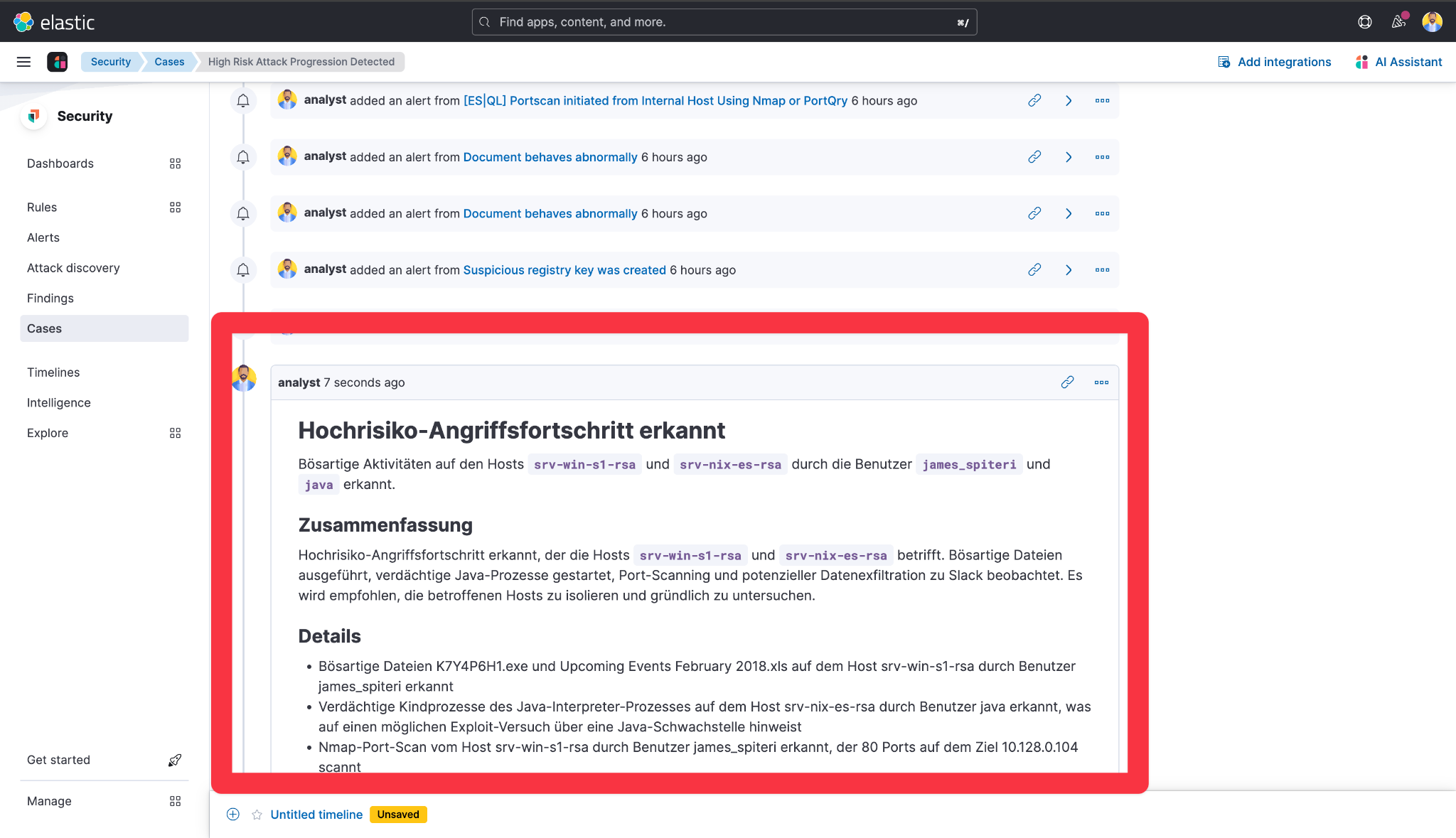
With just a few clicks, I can create a new case from this discovery.



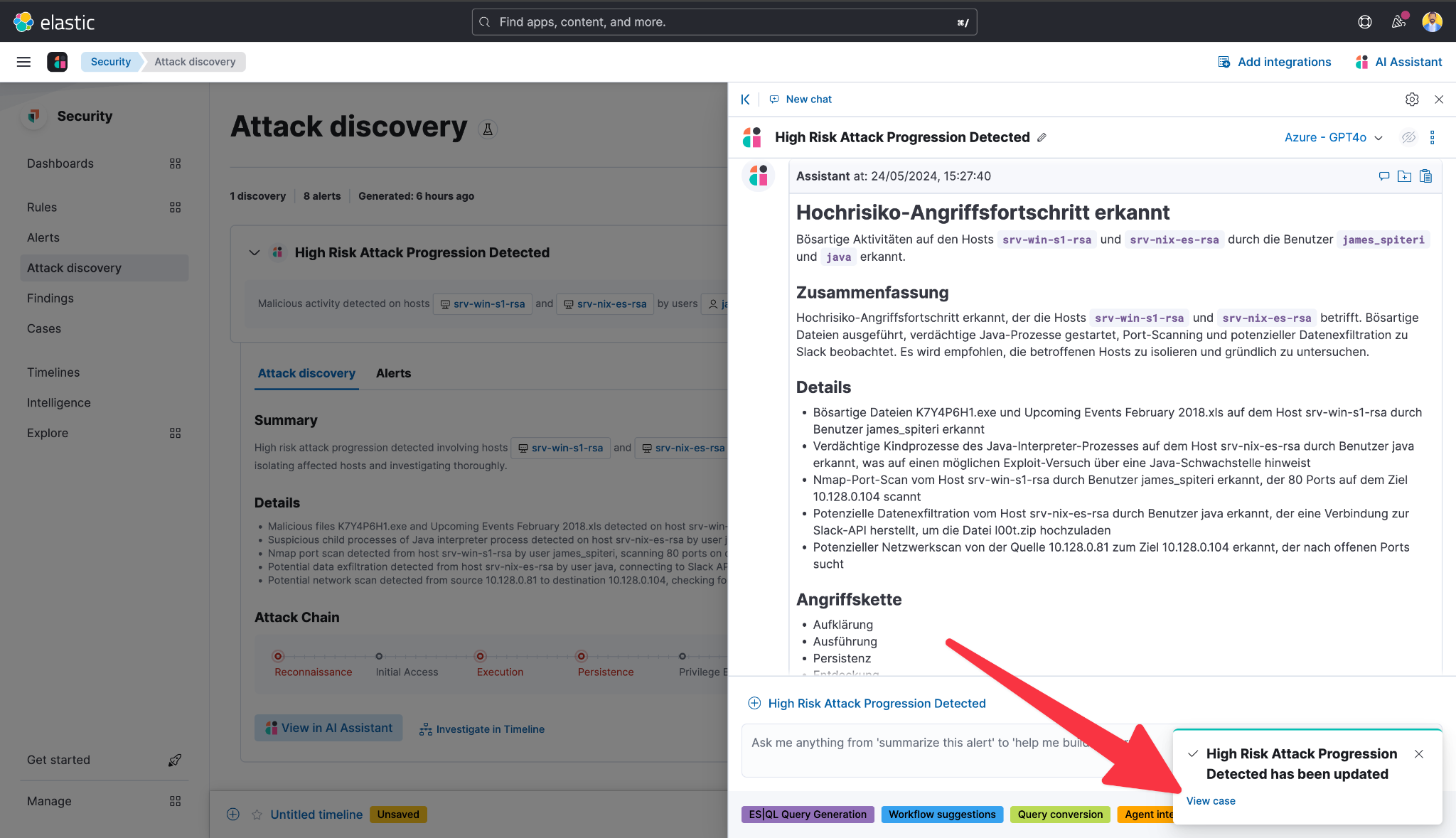
Elastic automatically populates:  
- The case title  
- A detailed description of the attack  
- All associated alerts  
  
This makes it easy for me to collaborate with my team and track incident resolution efficiently.

### Leveraging AI for Remediation

In addition to investigation, Attack Discovery also helps with remediation.



If I’m unsure about the next steps, I can send this discovery to the AI Assistant and ask: 'How do I remediate this attack?'  
  
The AI Assistant will generate step-by-step remediation guidance, which I can then add to my case for reference.



## Conclusion

We’re incredibly excited about Attack Discovery and the efficiency it brings to Elastic Security users. This is just the beginning, and we’re committed to enhancing security operations with AI-driven insights.  
  
To learn more, visit our website or start a free cloud trial today.  
  
Thank you for your time, and I look forward to seeing you in the next session!