Today, I’m excited to introduce **Attack Discovery**, the latest feature in Elastic Security.

**Attack Discovery** is designed to help security operations teams of all sizes quickly **triage and investigate alerts** using **generative AI**. So, let’s see how it works.

**Exploring the Alerts View**

What you see on my screen is the **Alerts View** in Elastic Security. This is where security analysts typically start their daily operations, reviewing alerts triggered within their environment.

These alerts come from:

* **Elastic Security’s built-in detection rules**, powered by our **Security Labs team**.
* **Custom rules** created by users.

Even on a slow day like today, I have **30 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.

We designed **Attack Discovery** to be **simple and intuitive**. It analyzes all **30 alerts at once** using **generative AI**.

A key advantage of Elastic is that we allow you to **integrate any large language model (LLM) of your choice**. Once I select my preferred model, Elastic’s powerful AI and search capabilities ensure **accurate and actionable results**.

I simply click **“Generate”** to start the analysis. Since this involves deep data correlation, it may take a few moments. I’ll pause here and return once the results are ready.

**Reviewing Attack Discovery Results**

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

At the top, we see a **high-level summary** of what happened:

* The **30 alerts** have been grouped into **four key discoveries**.
* These represent **four active security threats** in 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. Examples include:

* **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 **automatically correlates alerts** and provides a **structured summary** for quick analysis. Let’s examine a **macOS malware attack**.

**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 **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 allows 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 need guidance, I can send this discovery to the **AI Assistant** and ask:  
*“How do I remediate this attack?”*

The **AI Assistant** generates **step-by-step remediation guidance**, which I can **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!