elastic

Search. Observe. Protect.

How a European police force hunts for digital threats with Elastic

Several years ago, this European national police agency of 22,000 officers and 1,000 IT personnel began a transformation journey, one that included consolidating the bureaucracy, modernizing its policing equipment, and digitally transforming its IT infrastructure.

A key element to that digital transformation project was securing the new, modernized enterprise which entails about 35,000 connected computers and 250 IT systems. Other elements to the modernization project included a new app store for police officers' smartphones, new drones with cameras, an upgraded command center, and specialized telecommunications to connect with embassies.

"All of these things need to be secure and they need to work every day, every night, all of the year," says the agency's security operations center manager.

The internal, external threat landscape

The threat landscape for a police department is similar to those confronted by most businesses. This European police agency says it's harnessing Elastic to defend against:

- Targeted cyber attacks from external actors who want to steal data
- External actors who want to destroy data and prevent police infrastructure from functioning
- Malicious insiders who want to steal information, sabotage data or prevent police infrastructure from operating

These threats, both internal and external, originate from email, the Internet, USB drives, and partner connections. In response, the agency has adopted a security strategy that relies on **Elastic Security,** to prevent, detect, and respond to these threats.

"We will not reach the level of security, the required level of security, unless all these three components work together," says the agency's senior cyber security specialist.

Enhancing threat hunting with machine learning

To increase visibility, reduce time from detection to response, and improve threat hunting capability, the agency built an Elasticsearch cluster with load balancing and message queueing layers. They are now able to search and visualize raw log data for threat hunting, build advanced detection rules, and apply machine learning to improve and hasten anomaly detection. Overall, the agency has increased by tenfold their capacity to receive events per second (EPS) from relevant security data streams.

The department's Elastic journey began in 2019, when they tested Elastic's free and open version to log endpoint data. A year later, they moved to a paid **Enterprise Subscription**, and began migrating data sources to Elastic's **SIEM** with a goal of dropping the agency's legacy SIEM.

"Basically, we're able to take in 10 times more data than in the previous SIEM. We have a totally different, much improved visibility on the operating system level. We are collecting log records from our 35,000 endpoints and network sensors," says the agency's senior cyber security specialist. "We're talking about several billion log records. All the data that we need in order to detect anomalies, we now have at our hands."

