ELASTIC SECURITY

SIEM powers investigation and response

Upon detecting a threat within an enterprise's perimeter, the SOC must investigate and respond fast enough to stem the attack before damage grows. But complications abound:

- Experienced security practitioners are difficult to hire, train, and retain
- SOCs often struggle to implement standard operating procedures and adapt them to keep pace with the breakneck evolution in how companies operate
- Many SIEMs from an earlier era don't come close to providing the speed, scalability, or versatility needed to definitively address a detected threat

Due to these and other challenges, typical mean time-to-respond (MTTR) intervals extend an adversary's unwelcome stay by days, weeks, or even months. It's no surprise, then, that 89% of organizations report having endured damage from an already-detected attack.

How does fast access to data expedite investigation?	To stop attacks at scale, practitioners need command of comprehensive environmental activity. Embedding insights and context (i.e. threat intelligence) informs decisions without swiveling between screens. Putting observability data within easy reach enables the efficient resolution of an even broader set of issues.
How does standardizing processes contribute to team success?	To thwart attacks before damage occurs, organizations must standardize and streamline processes. Case management establishes fundamental workflows and third-party integrations power collaboration beyond the SOC. Embedded guidance routinizes key investigation and response steps, improving analyst efficacy.
How does automation enhance SOC efficiency?	Automation reduces MTTR and supports the sustainable operation of the SOC by reducing the burden of repetitive tasks, thereby enabling analysts to focus on work requiring intuition and skill.

> "We used to take days to find a problem. Now we're doing it in minutes. This reduction in mean time to resolution was something we couldn't do with our legacy solutions."
>
> **Ali Rey, Vice President of Cloud and Data Platforms, Emirates NBD**

|

Why Elastic for investigation and incident response?

Enable full and fast analysis

Elastic Security enables the SOC to retain years of rapidly searchable forensic data to reconstruct an attack, determine its cause and scope, and direct remediation efforts. Providing immediate access to this wealth of information is the first step to predictably reducing MTTR.

Investigate rapidly

Elastic Security accelerates investigation with intuitive analyst workflows and expert-written guidance. Practitioners can analyze diverse data and correlate it in an intuitive manner with a unified timeline. From this same UI, they can scrutinize individual users and hosts and access an array of insights and internal and external context.

Respond decisively

Built-in case management helps security teams coordinate efforts, while integrations with third-party ticketing and security orchestration platforms align efforts with organization-wide processes. When time matters most, easily inspect host and cloud workloads and remediate threats with a robust automation framework and the power to take action across distributed endpoints.

Migrate to a modern SIEM for security investigation and incident response

To achieve investigation and incident response for your security operations program, choose a massively scalable platform with a powerful data schema and prebuilt data integrations supporting the most innovative technologies in your enterprise stack.

Adopting a modern SIEM isn't a trivial undertaking and you'll have a lot of decisions to make along the way. But rest assured, the Elastic team and our partners have walked this road countless times, and we'd be glad to share what we've learned.

Get started by considering the most important attributes of the right SIEM solution for your organization with our SIEM Buyer's Guide.

Start your SIEM journey