elastic

How modern is your SIEM, really?

You may already have a security information and event management (SIEM) solution.

But is it adapted to take on today's demands of flexibility, scale, and openness?

Nearly half (44%) of organizations want to augment or replace their SIEM[1]

SIEM will be one of the top investment areas in cybersecurity over the next two years (2023-24)[1]

89%

of companies have been damaged before responding to a detected attack[2].

Why? Because traditional SIEMs lack the ability to quickly automate workflows.

The needs of SIEM have changed. Here are the...

Key requirements for the modern SIEM

Effective detection & triage

A modern SIEM should ship with a robust library of security expert created and maintained detections, while providing context like entity alert risk and threat intel to efficiently triage those alerts.

Easy investigation

A SIEM should provide a strong, built-in case management function that facilitates collaborative investigation and centralizes associated alerts, data, and notes.

Fast response

Enable rapid remediation across your environment. Look for a SIEM that bolsters analyst efficacy with prebuilt playbooks and streamlines workflows with automated response actions like processes suspension and host isolation.

There's a lot to consider when purchasing a SIEM.

Explore our SIEM Buyer's Guide

Get started

1 | ThoughtLab study: Cybersecurity solutions for a riskier world

2 | New ESG Research Reveals 89% of Companies Negatively Impacted by Cloud Cyber-Attacks Prior to Full Investigation

elastic