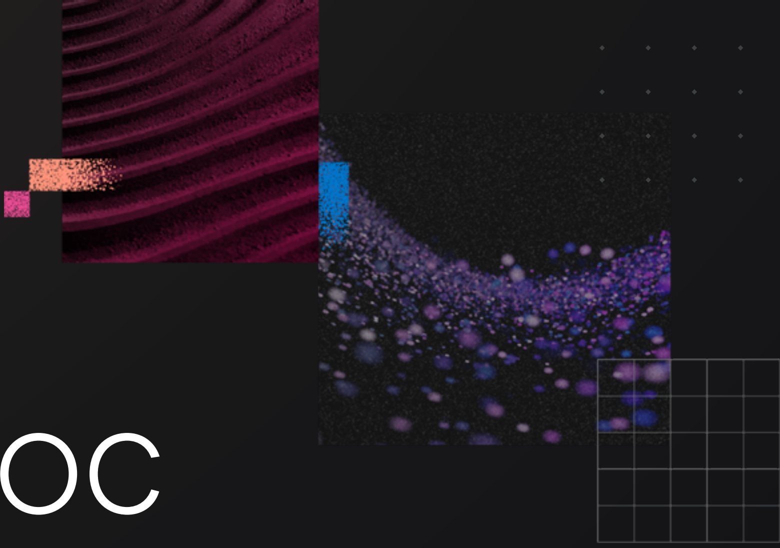
elastic security labs



2024

Elastic Global Threat Report

Threat trends SOC leaders should know

Built to provide actionable insights for security teams and CISOs alike, the 2024 Elastic Global Threat Report surfaces top findings from months of analysis on more than 1 billion data points, courtesy of both public and Elastic specific telemetry. These takeaways have been organized into insights from the data and suggested actions for your organization.

Top insights

01 Cloud environments are being misconfigured by enterprises

Our new section on cloud security posture management (CSPM) compared environments to Center for Internet Security (CIS) benchmarks and found that on average, ~50% of environments failed checks regardless of cloud service provider (CSP).

02 Defense Evasion remains the most frequently seen endpoint tactic

Defense Evasion accounted for 38% of endpoint behaviors, suggesting that adversaries are comfortable navigating security systems. Notably, this number has decreased 6% from last year, highlighting that defender tools are working effectively.

03 Credential Access alerts continue to increase, especially within the cloud

Within cloud environments, Credential Access accounted for 23% of activity. Furthermore, endpoint environments revealed a 3% increase in these techniques year over year. These can be traced to the growing prevalence of information stealers and credential brokers, as well the fact that security tools are growing in visibility.

04 Adversaries are abusing defender tools to enter systems efficiently

53% of observed malicious files were identified as offensive security tools — leveraged by enterprises to discover weaknesses and abused by adversaries exploiting them. These OSTs have large R&D teams to create new capabilities like Process Injection — a form of Defense Evasion which accounted for 53% of Windows alert events this year.

05 Generative AI did not increase the amount or impact of attacks we observed

Security teams have been concerned about an upcoming onslaught of GenAI attacks. While we saw a minor increase in threat volume, GenAI has largely bolstered defender technologies with capabilities like alert summarization and task automation.

Key suggestions

01 Audit your environment often

Adversaries are relying on permissive or misconfigured security controls to infiltrate environments, and once they're inside they're focused on tampering with sensors and data. Benchmarking and risk assessments can help you identify whether you're utilizing best practices and industry standards to effectively control access within your enterprise.

02 Prepare for generative AI by tuning your security controls

The increase in GenAI will result in an uptick in social engineering attempts. While training your user base to identify these attempts and more is always a good idea, security teams should also verify their controls and permissions to ensure that a successful phishing attempt won't cause long-standing damage.

03 Implement interactive endpoint agents to neutralize Defense Evasion attacks

Defense Evasion attacks have been the main tactic for a few years. While it's decreasing, adversaries are still utilizing these methods to infiltrate and navigate environments. Endpoint technologies like Elastic Agent provide visibility and capability while reducing the amount of tools you need.

04 Create a robust response plan for exposed credentials

We observed techniques like Brute Force and Access to Browser Credentials from Suspicious Memory being utilized regularly. Rotating exposed credentials and organizing quick workflows for breach response will make a large difference. Security teams should mandate multi-factor authentication if they haven't already.

05 Compare your cloud environment to the CIS benchmarks

The CIS benchmarks are an industry standard and will help you quickly identify what areas need attention. Your team should develop a plan to monitor and raise your score, which will improve threat detection and reduce risk in the long run.

Master the threat landscape

Prepare for the evolution of these threats and more. Get all of our suggestions and see the full breakout of today's threat landscape in the 2024 Elastic Global Threat Report. You can also follow our experts @ElasticSecLabs.

See how Elastic Security can modernize your security operations.