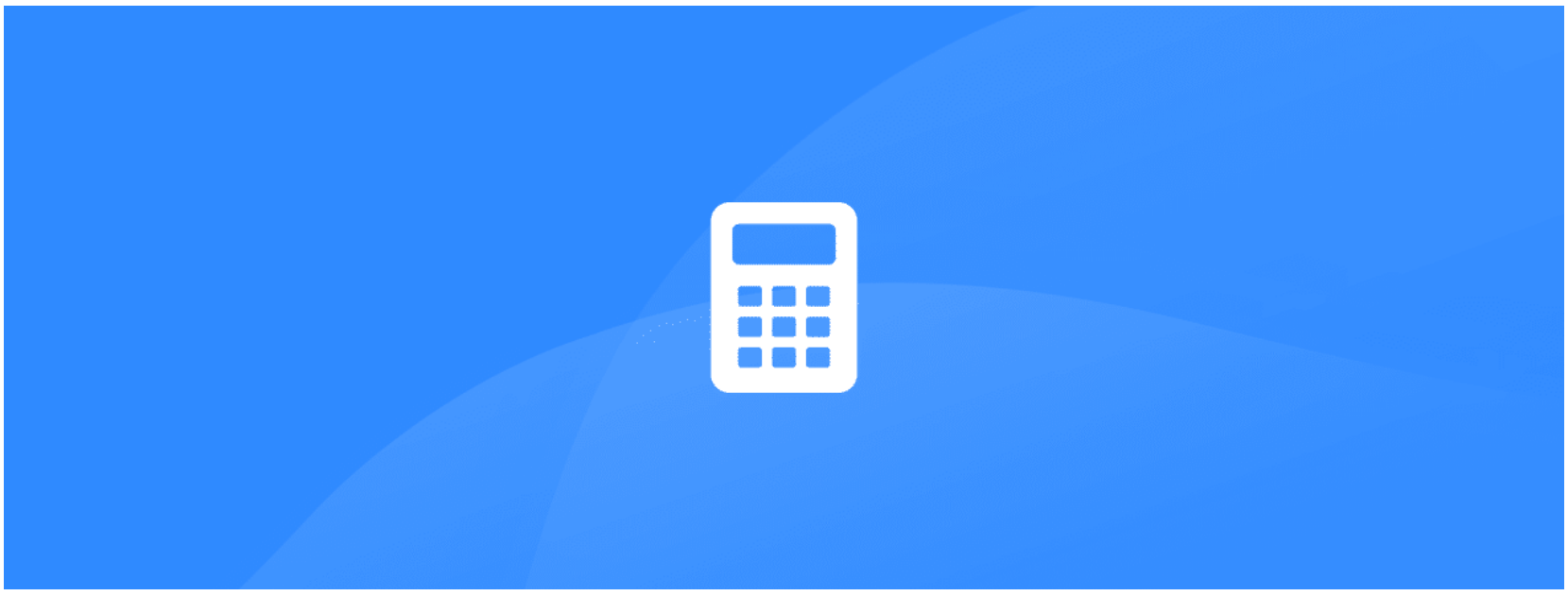
Security ROI: Time & Resource Savings for IR/SOC Teams

Written by Intezer - 31 March 2022



Automation can augment your security team to help you manage never-ending alerts, reduce skill gaps, respond faster, and leverage historic investigation data. Intezer can cut tasks that take hours into minutes.

The promise of automation is a strong draw, as more and more security teams look for ways to introduce automation into their workflows. With constant streams of alerts to triage and investigate, SOC and incident response teams are often overwhelmed. While cybersecurity tools have evolved, we have resource shortages in the industry, skill gaps, and knowledge lost to turnover. And many organizations still struggle with a steady volume of false positives and noise that lead to wasted time.

Leveraging automation to reduce the number of manual tasks required for alert triage, incident response, and threat hunting presents an important opportunity for teams feeling their time and resources stretched to the limit.

Our team calculates that more than 80% of the threats that teams deal with are mutations of something already seen. Intezer's technology can detect these mutations by identifying any reused code or techniques from previously seen threats, to help teams streamline the majority of their workload. By integrating automation into SOC and IR workflows, we can automatically classify threats in easy-to-understand reports that get archived for knowledge retention and connecting separate incidents.

This saves time and resources on tasks that bog down SOC and IR teams, allowing you to stay focused on critical issues and respond to novel threats. Not wasting time on false positives, noise, or previously seen threats. With more automation in your toolset, you can eliminate time wasted on low priority alerts, reduce pressures that lead to turnover, close skill gaps, and retain historical data.

4 Ways to Save Time and Resources for Your SOC/IR Team

1. Alert triage — Automatically analyze files, URLs, and machines to classify threats and threat actors. Intezer has a false positive rate of 0.2%, effectively eliminating false positives triggered by EDR or other detection systems to ensure your team can focus on real threats.
2. Incident Response — Teams can see an immediate improvement in Mean Time to Respond (MTTR), with automated extraction of IoCs and detection content. Teams using Intezer see alert triage time reduced by up to 90%.
3. Threat Hunting — With 10,124 mapped threat actors and malware families (and growing daily), Intezer allows your team to track threats of interest and leverage a feed of high-quality detection opportunities based on genetic code analysis.
4. Knowledge Retention — The cost of lost knowledge due to turnover is high, so teams need a way to preserve data over time. With access to a central source of knowledge for all micro-artifacts ever seen in the past, IR teams can easily make connections between separate incidents and even new analysts can provide deeper, historic context.

Collectively these time and resources savings from automation allow IR/SOC teams to manage an increasing volume of detection alerts while rapidly identifying critical threats. Intezer also provides the toolset for teams to take advantage of these time savings by proactively hunting for new, undetected threats.

"Getting Intezer was like adding two reverse engineers to our team for a much lower cost." Head of Security Operations

“Intezer contributes to our incident response and forensics investigations daily. Knowing what we are dealing with in the middle of an attack in less than 30 seconds directly impacts our clients’ risk mitigation and recovery time.”Head of Forensics and Incident Response Team

Key Points: Quantifying Time and Cost Savings on Incident Response

1. Time on False Positives: Today, security teams can waste up to 90% of their time investigating false positives. Meanwhile, teams using Intezer only spend on average 9% percent of that time on false positives.
2. Mean Time to Respond: MTTR decreases by 89% for teams using Intezer, compared to their previous MTTR before using Intezer.
3. Cost Savings of Potential Incident — Data breach costs hit $4.24 million on average in 2021, a record high. The same research noted that costs were significantly lower than that average for some organizations which had a more mature security posture, while organizations that lagged in security areas such as automation experienced higher costs. With automation from Intezer, security teams increase their capacity and can focus on real alerts, helping to prevent data breaches.

Automation for Deeper Insights Than Traditional Tools, Faster

Using a traditional toolset of paid or free tools takes an analyst at least 30-60 minutes to classify and identify each new alert or threat. Validating, investigating, identifying detection content, and creating detection rules for each threat could require a set of complex tools and unavailable skills, including virtual machines, behavioral analysis, and code analysis tools like disassemblers, debuggers, and memory forensics.

Percentage of Team Time Spent on Threat Analysis

Between 37-75% without Intezer

6% or less with Intezer

Intezer provides higher quality results in less time by utilizing automation to sift out false positives, while reducing the number of tools that analysts must switch between. Automation and consolidation of tools present the best options for addressing the rising volume of alerts and threats that SOC/IR teams face.

“Traditionally, an incident would have to go through an investigation process where we get the images and investigate each of the workstations. Typically, that means we’re going to have results in a couple of days. Being able to run Intezer allows us to speed up this investigation process to get immediate initial results.” Chris Stewart | Director of Security Operations | iSecurity

Automation for Quick Time-To-Value

Intezer’s cloud-based SaaS model and out-of-the-box integrations with most EDR and SOAR tools allow companies to start seeing immediate value on Day 1. Security teams don’t have time to spend on long implementation projects and waiting around for data ingestion. By allows your team to focus on unique threats, not repetitive alerts and noise.

Free your team from false positives, automate alert response, kickstart investigations with reverse engineer-level insights, and expand your threat hunting.

Talk with us.


Intezer

Track the latest malware variants and threat actors analyze.intezer.com

Alert Triage cybersecurity skill gaps false positives Incident Response MTTR soc teams Threat Hunting