INTEZER

Time and Resource Savings with Intezer

Key Benefits
- Decrease false positives by 90%
- Decrease MTTR by 89%
- Reduce chances of a breach

Boost your team with the power to manage never-ending alerts, reduce skill gaps, and leverage historic investigation data. Cut tasks that take hours into minutes.

Intezer reduces the time and resource pressures on SOC and IR teams, by automatically classifying threats in easy-to-understand reports that get archived for knowledge retention and connecting separate incidents. With more automation in your toolset, you can eliminate time wasted on false positives, reduce staff turnover, close skill gaps, and retain historical data.

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

Alert triage

Automatically analyze files, URLs, and machines to classify and prioritize threats. 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.

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%**.

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.

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 before 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 allows IR/SOC teams to manage the increasing volume of detection alerts while rapidly identifying the critical threats. Intezer also provides the toolset for teams to leverage 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.[1] With automation from Intezer, security teams increase their capacity and can focus on real alerts, helping to prevent data breaches.

Get 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 and creating detection content 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 and eliminating 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.

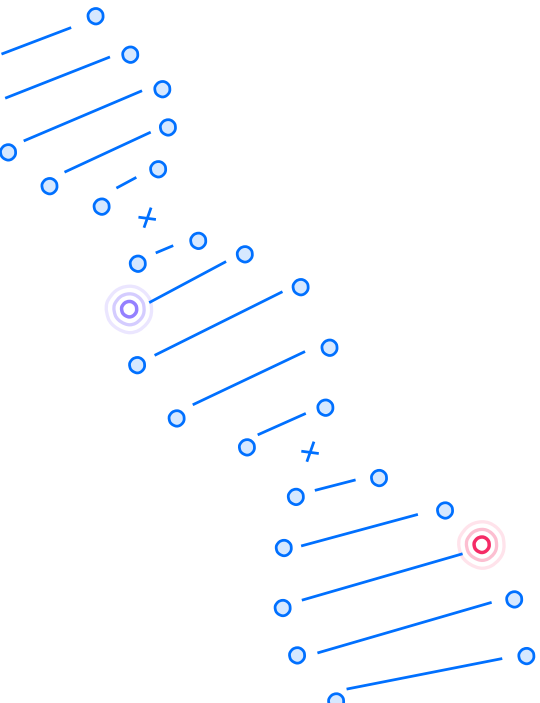
[1] Cost of a Data Breach Report 2021 from IBM Security. https://www.ibm.com/downloads/cas/OJDVQGRY

> 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**.
>
> Director of Security Operations

Quick Time-To-Value

Intezer's cloud-based model (SaaS) and out-of-the-box integrations with most EDR and SOAR tools allows customers to start seeing immediate value on Day 1.

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



INTEZER