



**INTEZER**

---

BUILDING YOUR **BULLET PROOF** INCIDENT  
RESPONSE PLAN

# BUILDING YOUR **BULLET** **PROOF** INCIDENT RESPONSE PLAN

Security teams at even the largest organizations are often overwhelmed by the volume of flagged incidents and unknown files that need to be investigated. Meanwhile, businesses' and customers' sensitive information is at risk of being compromised by the needle in the haystack: the major threat hiding in plain sight among false positives. A variety of malware could be lurking in their network. It's a dire scenario to be sure, but far from a hopeless one.

Accurately detecting and analyzing such malware is critical—although it has historically involved a very time-consuming process that required expert personnel. Even then, it continues to be very difficult for experienced professionals to **fully comprehend an existing threat within a short timeframe.**

But what if organizations had a tool in their arsenal that could accomplish all of this quickly as part of their incident response plan? How might it impact their security operations, and ultimately, their bottom line?

## The State of Corporate Cyber Security

In the world of business, cybersecurity is rife with challenges; chief among them today is incident response teams' varying ability to mitigate threats both efficiently and effectively. For the majority, detecting and understanding attacks as soon as they occur remains impossible.

Few organizations have the budget to support an in-house team with all the requisite skills (including highly experienced malware and security analysts) to properly

handle, categorize and classify thousands of incidents flagged by a series of tools, both SaaS and on premise, which are also, of course, managed by the same team. Business silo issues across departments and satellite offices can often complicate matters further.

Having all of these operations run smoothly represents a dream scenario in which CISOs could sleep soundly at night.

**Whether hobbyist hackers or state-sponsored threat actors are targeting organizations, internal security operations center (SOC) teams must proactively assemble a robust incident response plan in order to strategically manage and ultimately eradicate attacks.**

This plan should consist of logistical information, including a communications chain of key internal contacts in the case of a breach, as well as the operational flow of responsibilities from the prevention phase to an attack's eradication.

With a majority of organizations' SOCs at an immature or only now maturing ability to respond to events, it's clear that few are truly able to independently eliminate threats using existing tools.

In this document, the Intezer team has provided insights into how the technology behind Intezer Analyze™ offers security teams continuous and unmatched support along every step of the way, as the only cyber security tool to date applying code reuse detection.

Powered by Code Intelligence™ technology, Intezer Analyze™ is a malware analysis solution that was built by incident response professionals for incident response teams. It easily integrates processes and automations, saving time and simplifying operations, and most importantly, providing an accurate and definitive report on the nature and location of any current attacks on an organization. With nearly 70% of organizations reporting malware as the root cause of investigated incidents,[2] Intezer Analyze™ is poised to change the odds for security leaders.

## A Bullet-Proof Incident Response Plan: 4 Steps to Protect Against Today's Threats

While the following plan incorporates the NIST lifecycle, as suggested in its Computer Security Incident Handling Guide, it differs in how Intezer Analyze™ transforms the security team's experience and results within each phase.



### 1 Preparation

The initial phase, preparation, centers on assessing an organization's security. This requires a deep, comprehensive understanding of the pillars of a digital operation, starting with the code of any and all software programs running within an organization's network.

Using Intezer Analyze™, you can pre-index all of the existing code within an organization, creating a highly effective CODE whitelist, which then serves as a baseline for highly customized future code-comparison matching. Unlike other whitelisting

systems that frequently send false positives, Intezer Analyze™ highlights only unique files. Intezer offers a complementary tool that works for Linux and Windows; it examines all executable files within an organization and indexes them as part of Intezer's Code Genome database. Many types of endpoints can be indexed—from a developer endpoint up to a C-level endpoint. Through DNA mapping, any new, unknown malware is quickly identified and classified, as are variants of existing malware and any trusted software. As such, any file that appears without any matching genes will be immediately apparent to security teams.



### 2 Detection & Analysis


Cutting through the noise to find which threats require further mitigation has proven to be a challenge across industries. As previously mentioned, the majority of security teams are reporting a dwell time in which threats go undetected and unanalyzed for a period of 40 days or more—a large enough window in which hackers can do significant damage, gaining access to sensitive data or control of internal systems.

A variety of systems provide alerts to security events of varying levels; some are troubling enough to warrant immediate attention, while countless others could very well be false positives. In the meantime, genuine threats can go undetected. At this stage, categorization and prioritization is crucial, and time is of the essence.

Intezer understands the sense of urgency at this stage, and has made it a priority to enable teams to quickly classify security events. Its rapid, comprehensive categorization of any file via mapping its code DNA offers a deeper perspective than any security tool currently offers. Intezer Analyze™ dissects any binary into thousands of miniscule fragments, comparing it to the company's Code Genome Database. Within seconds, a full analysis of any file is available, denoting any code fragments stemming from known malware families. This includes source attribution to relevant attackers—empowering security teams to trace the origins of an attack, and understand who might be attempting to exploit their vulnerabilities.

## Incident Response Life Cycle



 **“This is the future of threat detection, Cyber attackers are constantly modifying their malicious files in order to evade detection, and security professionals need to ‘chase’ and sign these new files every minute. Since many malware code pieces are indexed in our Genome Database, Intezer changes the entire equation: now, attackers must adapt and rewrite code completely from scratch, which effectively makes attacking your enterprise a far less cost-effective endeavor.”**

Ari Eitan, VP of Research

### Near-Instantaneous Detection

Integrating existing endpoint protection with the Intezer Analyze™ API effectively adds another layer of defense to your cyber security plan. With its code reuse detection technique, Intezer Analyze™ has proven to detect sophisticated malware where other methods—even those involving modern machine-learning or anomaly detection—have failed. Intezer Analyze™ offers out-of-the-box integrations with many security products such as CrowdStrike, Carbon Black, and more.

### Reducing False Positives

One of hundreds (or even thousands) of alerts raised from security solutions may lead to a specific file that catch an organization’s attention. Intezer Analyze™ enables users to filter through such alerts and reduce false positives by integrating a SIEM or any other alert system with its API, automatically sending every file into Intezer Analyze™ in order to map its DNA. By doing so, security teams aren’t only able to filter all false positives; they are provided with robust data-driven insights on each alert to the extent that a Tier 1 SOC can have the same conclusions of an expert Tier 4 malware analyst, for example. Within seconds, security teams can know with confidence if the file in question is from a trusted or malicious source.

### Accurate and Comprehensive Analysis

If the file is flagged as malicious, security staff will have a clear advantage by gaining a quick understand the threat’s capabilities, the attacker’s goal, and their identity or known affiliations.

Intezer Analyze™ accelerates malware analysis by detecting and analyzing code reuse of known malware—leading to a deeper understanding of attackers’ intentions and potential behavior. For example, if malware possessing Mimikatz genes has been detected, it implies that this person will at some point attempt to undertake a lateral movement within a given network, seeking the ability to spread to other computers with greater permissions and access points.

Gaining a deeper understanding of the goals behind an attack based upon the approach used (ransomware, a Trojan Horse, etc.) is critical. This enables organizations to protect themselves against a variety of malicious pathways that a given attacker might use in order to accomplish the same goal in future, be it information theft, destroying data or compromising internal systems.

When the origins of their code is detailed in plain sight, it is difficult for hackers to remain unknown. With Intezer Analyze™, attributing an attack is now increasingly straightforward. In addition, alerts can be immediately prioritized since they are accurately classified by both the level of attacker sophistication (for example, code that is based upon a government’s known types of malware) as well as the malware type (such as an APT versus more generic malware).

## Sample threat scenario

A lead security analyst receives an alert from one of their systems. Whether it’s an AV hit, suspicious SIEM alert --he or she is able to send the file, either via Intezer’s web interface or automatically via API into Intezer Analyze™ for thorough investigation. From this, the analyst can instantly understand the type, goal and content of the potential threat.

Let’s take the 'Bad Rabbit' malware--one of the most infamous attacks of 2017--as a concrete example. Analyzing the sample with Intezer Analyze™, offers a number of immediate, critical conclusions:

1. The threat type is ransomware, since it shares more than 80 percent of its code with a known ransomware called NotPetya;
2. The authors of this malware are also the ones behind NotPetya, based on the genes and code reuse. Since NotPetya was one of the most infamous and damaging attacks, it is clear that this threat actor is highly sophisticated and therefore this alert should be prioritized above the rest;
3. Lastly, this threat has the ability to spread itself via network, based on its shared genes with Mimikatz, which is a well-known hacking tool used to steal passwords for lateral movement purposes. This serves as an immediately warning to rapidly contain this threat before it spreads throughout the network.

### Memory analysis and file-less threats

Another critical use for Intezer Analyze™ technology involves memory investigation. In this continually challenging area for industry, Intezer outperforms other solutions.

Investigating a full memory dump is similar to finding the proverbial needle in a haystack; moreover, until now, analysts had to know precisely what they were seeking in order to find it.

Intezer Analyze™ simplifies the entire process and conducts a more rigorous analysis. Now, a full memory dump can be analyzed within minutes. Security pros who rely on Intezer will receive a clear report containing all the executable regions in the computer's memory, along with full DNA mapping based on the genes within those regions—enabling them to immediately focus on those that share code with known threats or include unique, never-before-seen code. This kind of investigation isn't possible with most malware analysis tools available today, such as sandboxes, since these rely upon running samples which cannot be done using modules dumped from memory.

### Deep code analysis and reverse engineering

Deep malware analysis and reverse engineering are possible through a special plugin that Intezer has developed to IDA Pro, which generates a list of the unique genes worthy of security professionals' attention in their analysis, saving critical time during this stage and improving the speed with which they respond to any relevant threat. Security teams are able to zero in on actual threats during the investigation phase.

For example, upon analyzing a suspicious file using Intezer's system, 90% of code has previously appeared within a specific APT, but the remaining 10% is totally unique code. With Intezer's advanced plugin, security teams can focus IDA directly on only the unique code. This saves valuable staff time and energy by eliminating the need to investigate familiar code, not on any irrelevant portion. Organizations also stand to save a lot of money by only allocating internal resources toward the most appropriate areas.



## 3 Containment, Eradication, & Recovery

Once the scale and scope of the breach have been identified, teams must work quickly to address issues in the containment, eradication and recovery stage.

### Containment

Naturally, the priority is containing the attack: determining which systems have been affected and just how far attackers have penetrated into an organization. Once pinpointed, affected systems and devices are immediately disconnected to prevent further damage.

### Eradication

Once the incident's origins have been investigated and discovered, the team can address the root of the problem and remove all traces of malicious code.

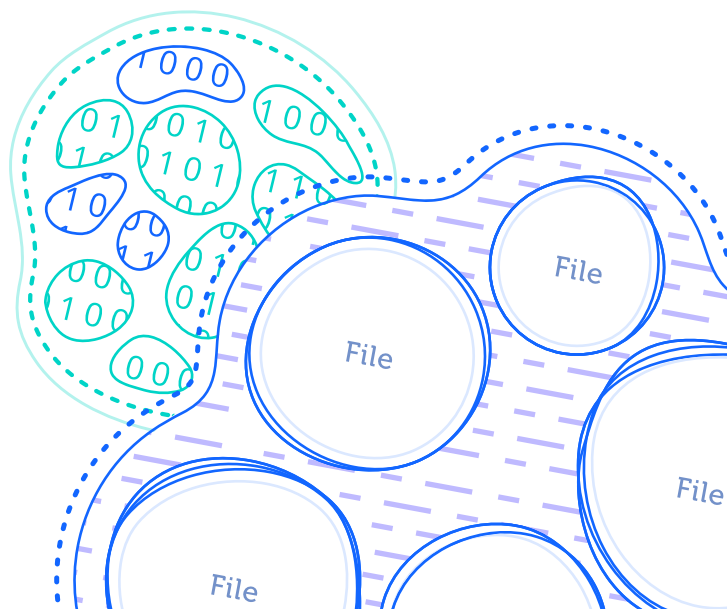
### Recovery

At this juncture, data and software can be restored from an organization's clean backup files, ensuring that no vulnerabilities remain. Systems are continuously monitored for any signs of weakness or recurrence.

The above steps may very well already comprise a routine part of an incident response plan, and with good reason. However, an augmented layer of protection is now possible. Intezer Analyze™ enables security teams to automatically create YARA signatures at the gene level, which improve the speed and accuracy with which a team can move through the containment, eradication and recovery stage. YARA formats are widely supported and allow for the swift removal of an attack.

The above steps may very well already comprise a routine part of an incident response plan, and with good reason. However, an augmented layer of protection is now possible. Intezer Analyze™ enables security teams to automatically create YARA signatures at the gene level, which improve the speed and accuracy with which a team can move through the containment, eradication and recovery stage. YARA formats are widely supported and allow for the swift removal of an attack.

The YARA signature is very effective, as it functions at the gene level—so the signing on of a specific code part automatically won't produce any false positive hits, and also it can detect other variants of the adversary within the network (most malware variants from the same attacker tend to share code with one another). Using this signature, security professionals are able to search their entire organization for specific files based on their genes, identifying infected computers that possess said genes, and even contain the threat by blocking relevant files and/or memory regions.





#### 4 Post-Attack

Following any security incident, security teams Analyze™ the nature of the attack itself, including its intended purposes, access points, malicious actions and possible sources. Additionally, leadership then evaluates team performance under pressure, noting that how the attack was handled may matter just as much as identifying what internal vulnerabilities they've been able to address as a result.

The recommendations that can be made at this stage to improve future response and prevent a recurrence of this threat will have a direct impact on an organization's future security. Those equipped with Intezer Analyze™ will have added advantages, including:

##### Repelling repeat offenders

If the malicious actor attempts to penetrate an organization again, it will directly be flagged as the malware will have already been indexed in our Code Genome Database, enabling the discovery of new variants as well as versions of their preferred coding method. This will cause major delays and require enormous amounts of resources for would-be attackers, who will ultimately be forced to completely rewrite their code from scratch—yet in this case, they'll ultimately be uncovered by Intezer Analyze™, as the system will recognize any new code as unique and lacking a connection to legitimate software.

##### Reporting with clarity

From the perspective of the management team, being able to view an organization's security through both a macro and micro perspective in real time is important for strategic decision making. Intezer Analyze™ provides enhanced reporting for management in an intuitive, easy-to-interpret format that provides clear answers about the nature of an organization's current threats. Today's common malware analysis systems currently don't offer security leaders a sophisticated high-level view, making it harder to extract meaningful conclusions from complex data.

##### Defending with specific diagnoses

The capability to attribute and categorize threats unique to an organization is invaluable. If a security team is aware of what it is up against—knowing that a specific category of malware is most frequent among its attacks—it can gain the upper hand by intelligently planning ahead versus simply attempting to protect systems against generic malware.

## The limitations of malware analysis

One of the most popular type of malware analysis systems, sandboxes, enable security professionals to scan files and receive reports based on runtime behavior analysis. They're able to view any modified registry values, API functions, created processes, and network activity.

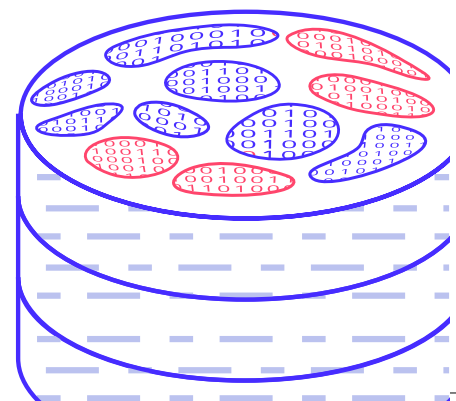
While these reports contain a litany of technical details, they're unfortunately presented as very complicated, protracted documents—leaving managers and even some security analysts struggling to interpret results and make meaningful business decisions.

In this situations, getting straightforward answers to the most important questions is paramount; sifting through technical minutiae is not. Managers seek to understand attackers' goals, intent, type of attack, and level of sophistication, and Intezer Analyze™ can provide this information immediately, without unnecessary details.



**With our technology, there is no need for security teams to run after the latest threats or update their signature database. Each day, hundreds of thousands of new threats appear, and we're tracking them all as code reuse is our area of focus. We know code is evolutionary; regardless of type, it's not wholly written from scratch every time. We're using this information to attack new threats, representing a novel concept in today's cybersecurity landscape.**

Ari Eitan, VP of Research, Intezer



## Securing an Organization Starts at the Gene Level

Existing cyber solutions only empower security professionals to examine issues at the file level through a sandbox scenario, for example. Intezer is transforming corporate cybersecurity by taking defense one step deeper, to thoroughly diagnose issues at the DNA level.

Organizational health doesn't begin with a single file, but rather, in the code it contains. Think of the human body-constantly under threats of one kind or another, be they viruses, bacteria or even cellular mutations. If a person could successfully treat a virulent disease through a remedy that bolsters his or her DNA, for instance, they'd take it because it provides the very best chance of eradicating the issue forever. Intezer makes that kind of immunity possible for organizations.

With Intezer Analyze™, entire security teams can attain reverse engineer-level conclusions; now, optimizing and accelerating an incident response plan while minimizing false positives is possible without requiring everyone to possess this highly specialized skill set. Intezer Analyze™ integrates easily with an

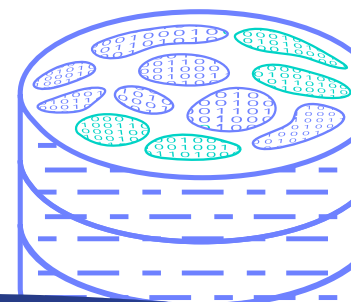
organization's internal processes, including automation and forensics tools such as IDA and endpoint security solutions like CrowdStrike and Carbon Black, SIEM systems, as well as security orchestration systems, among others.

Classification is now possible in the same breath, empowering teams to begin remediation efforts immediately. The most technical analysts will be supported with the deepest insights possible on every file present in a network, preventing them from losing valuable time in the fruitless and costly pursuit of removing false positives. Aspects of attacks and their potential to cause further damage will be immediately classifiable, offering critical information to management teams and CISOs with a clear, insightful report on the actual threat situation in real time.

In any organization, removing the massive distraction of false positives is only half the battle. The other lies in capitalizing on available time and staff attention to address attacks before they wreak havoc on businesses. Intezer Analyze™ equips security professionals to do all of this and more, bolstering defenses against future threats intelligently with immunity starting at the genetic level.

[1] FireEye C-level executive cyber security survey, 2017

[2] SANS 2017 incident response survey



Building your **bullet proof** Incident Response Plan



**INTEZER**



**INTEZER**

Malware Detection & Analysis  
it's our DNA