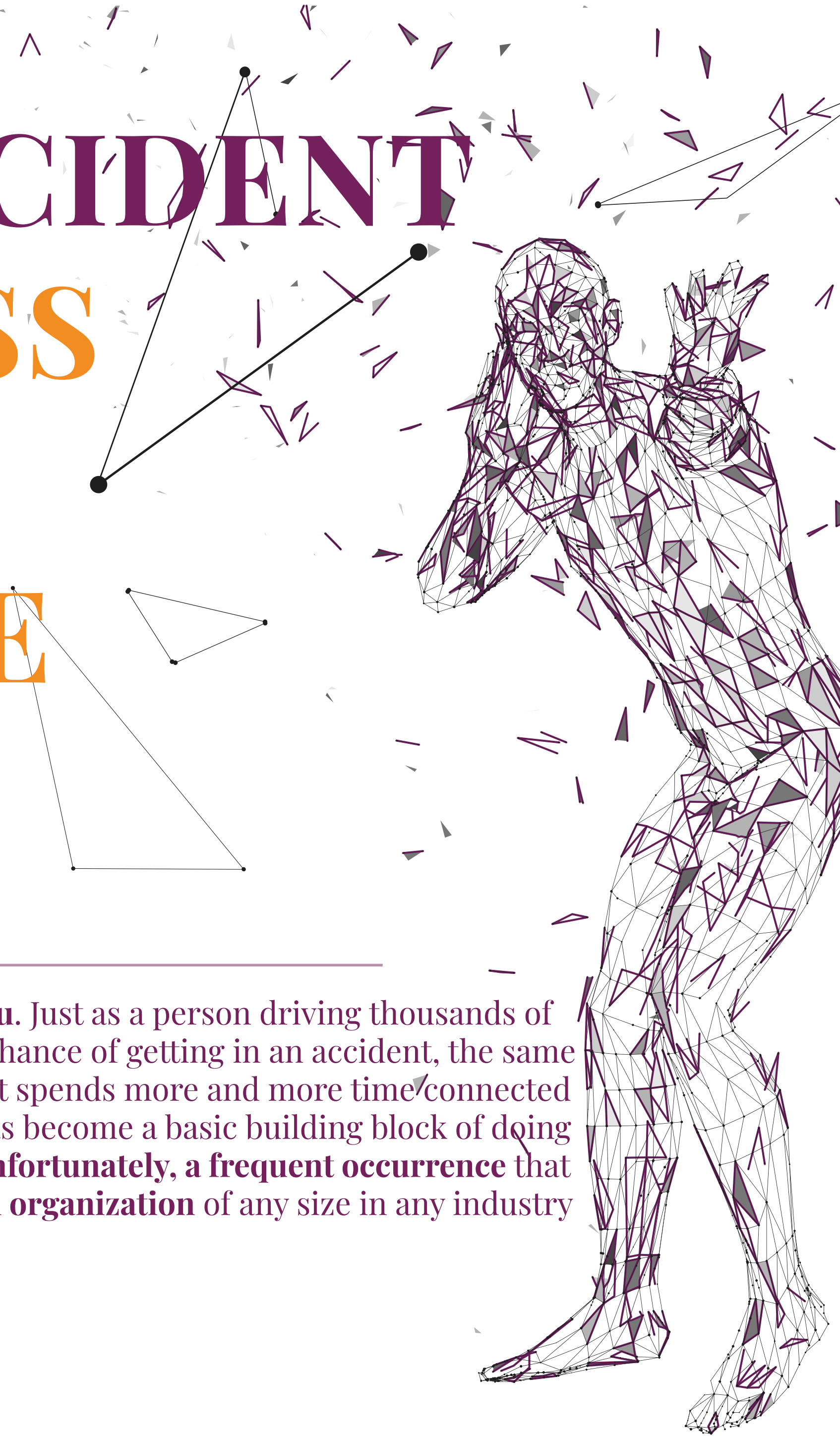
Infigo

Cyber Incident Readiness and Response

Good preparation, quick reaction time, and successful cyber incident resolution for a cost averse organizations

CYBER INCIDENT READINESS AND RESPONSE



Statistics are **always against you**. Just as a person driving thousands of kilometers per day has a higher chance of getting in an accident, the same is true about an organization that spends more and more time connected to the Internet. Since Internet has become a basic building block of doing business, **cyber incidents are, unfortunately, a frequent occurrence** that can **have a massive impact on an organization** of any size in any industry

Three phases of a successful cyber incident management

Preparation

In the preparation phase, Infigo assesses current organizational cyber security incident response capabilities – this is important as it provides a baseline, identifies key stakeholders, resources (from documentation to key application and ICT services), and all that comes into play when the cyber incident happens. It is performed on the annual basis.

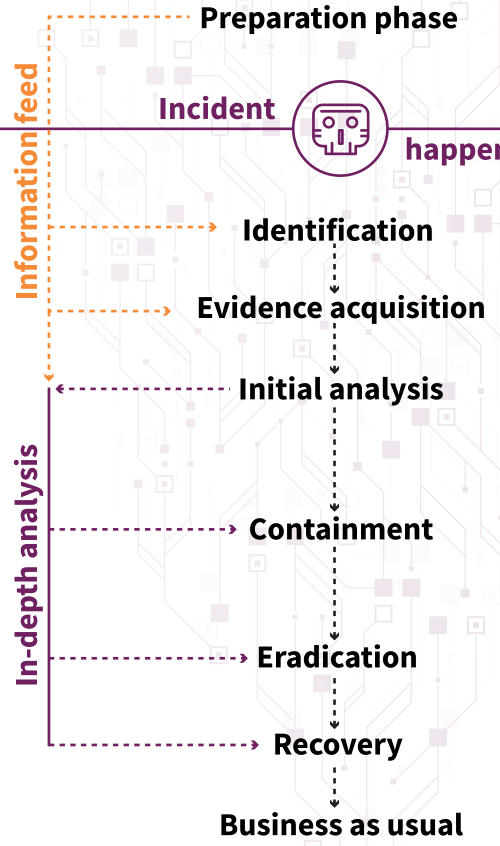
Response

The response phase is when a cyber incident happens – it is the time when every minute counts and good preparation will keep everything running smoothly even in the most hectic situations. Infigo will go through a couple of subphases such as identification, initial analysis, in-depth analysis, containment, and support in the eradication process done by internal IT department.

Recovery

Although Infigo is involved in the recovery phase, it is mostly done by the organization's internal IT department. Infigo will produce an executive summary of the incident, an incident report, and an incident wrap-up workshop – all that will be tied with lessons learned, a critical step that increases a long-term organizational security posture, boosting cyber resilience in general.

With Infigo Cyber Incident Readiness and Response



Preparation phase

Incident happens

Identification

Evidence acquisition

Initial analysis

Containment

Eradication

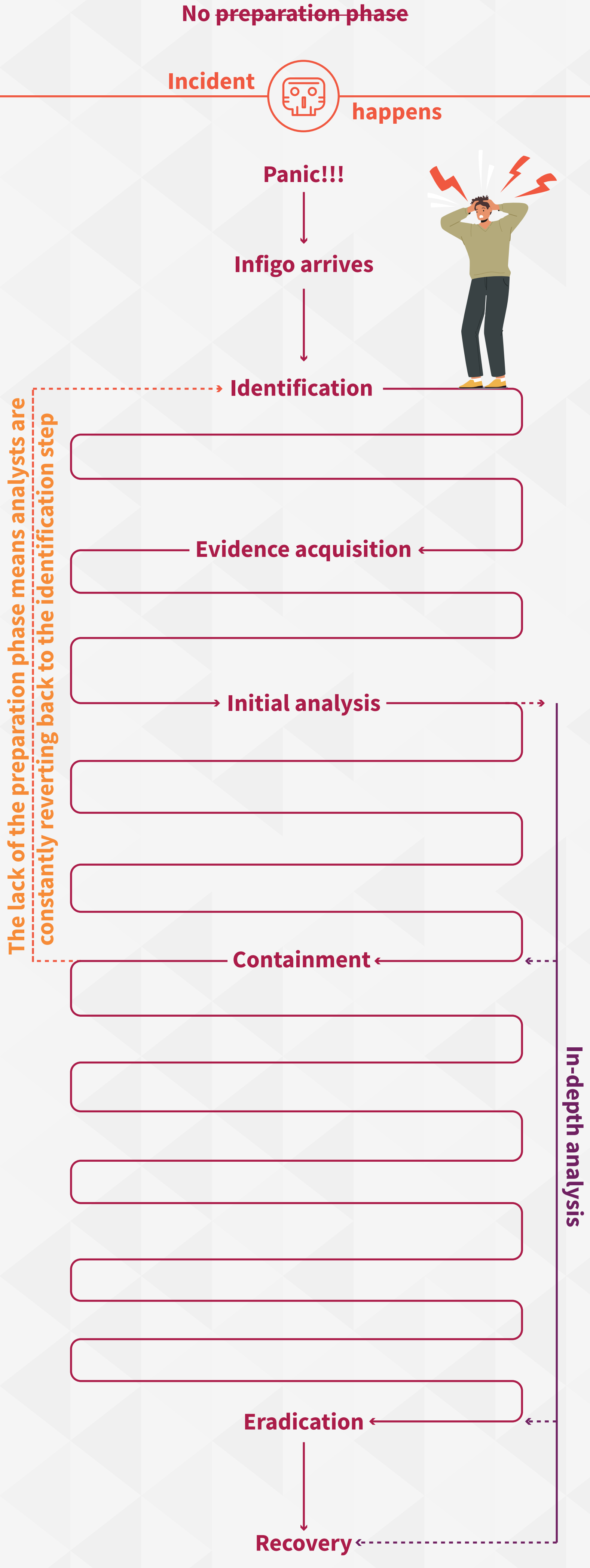
Recovery

Business as usual

Information feed

In-depth analysis

Without Infigo Cyber Incident Readiness and Response



No ~~preparation phase~~

Incident happens

Panic!!!

Infigo arrives

Identification

Evidence acquisition

Initial analysis

Containment

Eradication

Recovery

The lack of the preparation phase means analysts are constantly reverting back to the identification step

In-depth analysis

Key Features

The preparation phase (before an incident happens), drastically increases the speed of resolution, the chance of a successful resolution and shortens recovery time

With the service, the organization gets a trusted partner who is ready to help with a security incident of any size within a very short SLA (Service Level Agreement)

This great value service provides the organization with an additional level of reliability when solving security incidents, without requiring drastic investments in products/processes/people or long-term implementations

How does a typical cyber incident response look like?

Although Infigo considers **all three phases of cyber incident management as equally important**, organizations are curious about the response phase when something happens. Good preparation is crucial to a good response, but that has to be done before an incident happens - **without the preparation phase, the whole process takes much longer**. Not only do security specialists go in blind, but it means that at any step of the response phase can revert to the beginning with newfound information.

When it, unfortunately, happens, the first step is to establish the **impact, urgency, and severity of the incident**. Get a clear understanding of what systems and/or users are affected, and what actions were performed by the threat actor.

An initial brief with the organization and evidence acquisition will answer some of the questions, but the initial analysis will set a best-effort incident hypothesis as quickly as possible. Evidence acquisition and initial analysis are conducted in parallel as evidence acquisition can take a long time (depending on the size and complexity of the organization).

It is important to stress that:

- all actions are aligned to ensure operational security of the organization is maintained at all times
- **no evidence is analyzed using public resources**, uploaded, or shared in any capacity (e.g. a suspicious binary hash may be searched in VirusTotal, but a malicious file extracted from the organization will never be uploaded to VirusTotal)
- all tools used are exclusively deployed in Infigo's internal network
- all data pertaining to the incident is completely **removed from Infigo's systems upon the incident closure**; additionally, **the data is encrypted at-rest**

An in-depth analysis is done to reinforce or adjust the incident hypothesis established in the initial analysis. As typical in-depth analysis takes time, it may be conducted in parallel with multiple other phases (containment, eradication, and recovery).

The containment phase seeks to limit the damage and prevent further damage by the threat actor with the primary input being the short-term containment plan created in the identification phase. Infigo can, depending on the existing capabilities and tools present in the organization's environment, deploy additional tools to assist in effective containment.

Eradication is the last step in the response phase – it is the complete removal of the threat actor's capability to interface with compromised systems and their restoration into a last known good configuration.

Why is Infigo so good at this?

Infigo IS was founded in 2005. as an information security company and that has never changed. Every department is dedicated to security, employees cover different aspects of security and all that **positions Infigo as a one-stop security shop** rivaled by none.

By being able to look at information security from every angle – consulting, implementation, development, attack, defense – Infigo's security specialists have a unique view that most others lack. Every organization is different and Infigo's vast experience guarantees it can find a solution for myriad problems that can occur in live and complex business systems; of course, a good preparation phase ensures that Infigo's security specialists can do their jobs effectively, bringing organizations back from any kind of cyber security incident, big or small.

With a long list of satisfied clients of every size, **we have saved organizations from financial, operational, and reputational damages** – we leverage all that experience, processes, and procedures to help organizations around the world.

According to IBM, it takes an organization up to 69 days to contain a security breach. With Infigo's help, organizations can do that in a fraction of that time.

What happens next is up to you - let us make your life easier

www.infigo.is

INFIGO IS d.o.o.

Karlovačka 24a
10020 Zagreb
Croatia
+385 1 4662 700
info@infigo.is

INFIGO IS d.o.o.

Hasana Brkića 2
71000 Sarajevo
Bosnia and Herzegovina
+387 33 821 245
info@infigo.ba

INFIGO Software Design LLC

2902, Level 29, Marina Plaza
Dubai Marina, Dubai
PO Box 5000307
United Arab Emirates
+ 971 4 512 4081
info@infigo.ae

INFIGO IS d.o.o.

Tivolska cesta 50
1000 Ljubljana
Slovenia
+386 1 777 89 00
info@infigo.si

INFIGO IS d.o.o.

Ul. Metodija Shatorov Sharlo br. 30/2-17
1000 Skopje
North Macedonia
+389 (0)2 3151 203
info@infigo.mk