Incident Response PRO

The question is not if your organization will be hit by a cyber incident - the question is when. This means it is wise to prepare for the worst. We can help you with this. An Incident Response PRO subscription guarantees you help in case of an incident and helps your organization prepare. Let us help you.

Incident Response PRO allows you to:

Solve cyber incidents

You will know what to do and who to call when a cyber incident hits your organization.

Find out what happened

You receive help in finding out what exactly happened after an incident.

Comply with regulation

You comply with the incident response requirements of regulation like NIS2 and DORA.

Why choose Incident Response PRO?

The chances that your organization will suffer a cyber attack are growing. That is why more and more cybersecurity regulations, such as NIS2 or DORA, require implementation of a complete cyber incident response cycle. This involves **preparing for incidents, responding adequately to an attack, and knowing what to do afterwards**. You can compare this to the way fire safety has evolved. Of course, putting out fires is still important. But modern fire brigades also take preventive action and evaluate how a fire started in the first place. The same goes for cybersecurity incidents. We can help you prepare for and handle cyber incidents. Incident Response PRO also guarantees you expert support in case of an emergency, because attackers don't keep to office hours. Let us help you prepare for and handle major cyber incidents.

How Incident Response PRO works

An Incident Response PRO subscription has 2 main parts:

Incident Response Retainer

Forensic and Incident Readiness Assessment

1. Incident Response Retainer

You've been hacked - your important systems are down. Now it is important to limit the damage and get back to business as soon as possible. You need immediate support to take quick action. This retainer buys you our guaranteed availability in case of a cyber incident. It also gives you:

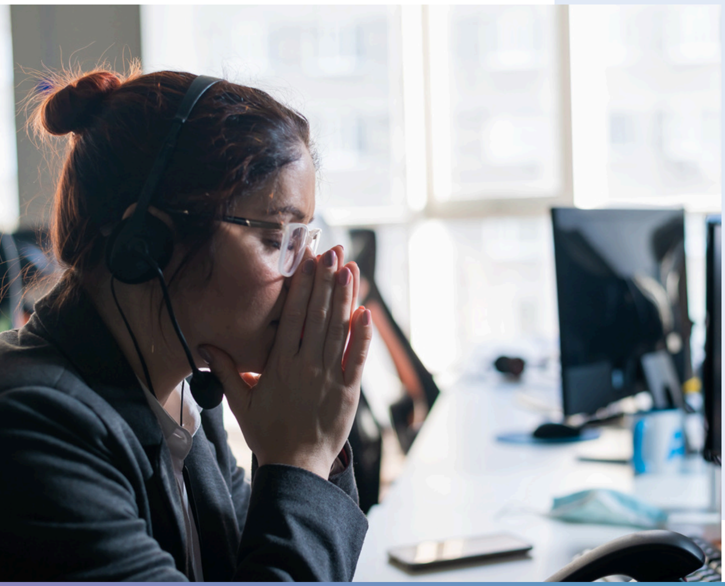
- Guaranteed response times
- On-site support within 12 hours
- Discounted incident response fees

2. Forensic and Incident Readiness Assessment

The last thing you want to find out during an incident, is that your crisis team has no idea what to do or that your organization has never preserved the correct digital evidence.

That is why we help you prepare for the worst, with a **Forensic and Incident Response Assessment (FIRA)**. We conduct a review of your organization's current incident response capabilities, policies, procedures, and technical controls and logging policies.

We identify gaps in your incident response process. Also, you receive recommendations for improvement, based on probability and impact. This assessment results in a written report, and is the perfect 'intake' for the Incident Response PRO service.



Help in case of an incident

Have you suffered an incident? We can we can help you solve it. We can also help you find out what exactly happened - to prevent it from happening again, or because you might be initiating legal proceedings. We can perform so-called post-mortems on systems and equipment.

Because we are registered as a **Private Investigation Bureau** with the Dutch Ministry of Justice and Security, you can use our reports and documents in legal proceedings.

Secura
A BUREAU VERITAS COMPANY

Handling a cyber incident

During a cyber incident we follow steps to minimize the impact to your organization. These steps are based on the NIST framework.

1. Triage

What happened? You need clarity on the what, when, how and where. This is why our experts first conduct a triage. The outcome determines the response and the urgency.

2. Containment

Most cyber incidents are caused by malware - more specifically: ransomware. During an incident, we want to prevent malware from spreading, for instance by disconnecting or blocking access to the affected systems.

3. Mitigation

As an incident evolves, we might discover new entry points that attackers can use or may have used. It is important to close these gaps. That's why we often repair vulnerabilities, install patches, reconfigure systems and change passwords.

4. Eradication

We can then remove any malicious software, remote access tools, or code that caused the incident.

5. Recovery

It is important to restore business operations as soon as possible. Steps we might take to this include restoring back-ups, reconfiguring affected systems and testing if they work properly.

Attackers don't keep to office hours. This service guarantees you that our Incident Response experts are available to help when you need them.

☎ **EMERGENCY? CALL +31 (0)88-8883107**

What our customers say

"The communication was to the point"

"We were impressed with Secura's fast response during our unexpected cyber incident. Their communication was to the point. What we also appreciated was how the experts thought along to make sure this doesn't happen again."

Related Services

SIEM/SOC Assessment

An incident often means that your detection did not work as it should. We can assess if your SIEM or SOC solution works correctly.

External Attack Surface Assessment

How did attackers gain initial access? Is there information about your organization available on the dark web that you don't know about? The External Attack Surface Assessment helps you find out.

Cyber Crisis Exercises

Practice makes perfect: learn how to deal with a cyber security incident through interactive workshops and simulated scenarios.

SAFE Awareness and Behavior Program

To prevent an incident it is important that your employees are aware of cybersecurity. We can help you raise their awareness with the SAFE Awareness and Behavior Program.

Secura
A BUREAU VERITAS COMPANY

About Secura / Bureau Veritas

Secura is a leading cybersecurity company. We help customers all over Europe to raise their cyber resilience. Our customers range from government and healthcare to finance and industry. We offer technical services, such as vulnerability assessments, penetration testing and red teaming, but also provide audits, forensic services and awareness training.

Secura is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80.000 employees and is active in 140 countries.

Example case | Incident Response PRO

Which problem did the customer have?

Several customers reached out to us when a new critical vulnerability was discovered in Citrix appliances. These customers suspected that attackers had carried out potential malicious activities due to this vulnerability.

Result

We were able to quickly scale up investigations and used indicators of compromise from several cases in addition to public sources. This threat intelligence showed activities carried out by malicious attackers. We were able to help the customers take measures to solve the issues and minimize the damage.

BUREAU VERITAS 1828

Interested?

Contact us today to start raising your cyber resilience.

✉ info@secura.com

☎ +31 (0) 88 888 3100

secura.com