



Red Piranha

# SECURITY INVESTIGATION

DIGITAL FORENSICS & INCIDENT RESPONSE (DFIR)

AUTOMATED  
RESPONSE

## FIND OUT WHAT HAPPENED

You need a competent partner to contact when there's a security breach;

- It's time to get the experts in.

## BE PREPARED AND RESPOND QUICKLY

A comprehensive incident response plan helps eliminate surprises and allows rapid response;

- It's time to get your plan in place and up to date.

## IF YOU FAIL TO PLAN, YOU PLAN TO FAIL

Too many organisations don't have a documented incident response plan;

- It's critical to have a clear plan for when things go wrong.

Red Piranha's Digital Forensics & Incident Response services help answer these key questions following a security incident:

- What happened? (understand the attack vector)
- Who was it? (attribute the attack)
- Where is my data? (did data exfiltration occur?)
- Can I recover my data? (What to do about the ransom demands)

### Services

We offer the following Security Investigation services:



Incident Response



Digital Forensics

### Incident Response

Most teams struggle to identify incidents accurately because of the sheer volume of traffic and events on the network, which leads to information overload and false positives.

Coordinating an organisation-wide response when a serious incident occurs can also be difficult, with people unsure of what action to take, which can lead to additional issues arising.

Implementing a tried and tested incident response plan means you can respond swiftly and effectively when things go wrong.

### Working Together

During the forensic investigation, Red Piranha works hand-in-hand with your IT team to mitigate risk, allowing proper containment of incidents. We study the information and work with your team to understand where the security system failed and to improve the handling of the event by looking at the existing security handling plans and make recommendations for improvement.



Red Piranha's experienced team of certified security experts deliver comprehensive Security Investigation services to help you plan for and manage a security breach.

Crystal Eye customers also benefit from automating a range of investigation activities to be better prepared.

## BENEFITS

Be prepared for the worst



Reduce time to respond



Find out what went wrong



Contain the spread

 **Red Piranha**  
Automated Cybersecurity

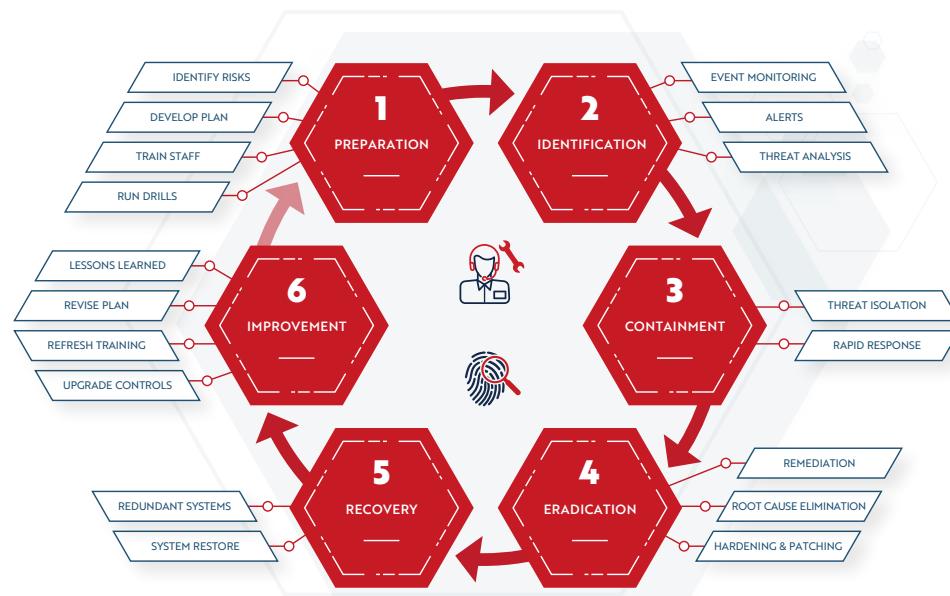
We're helping protect the world from cybersecurity threats by providing automated security solutions for every business; large and small.



Certificate No. 781489  
Crystal Eye Security operations



# SECURITY INVESTIGATION



## Digital Forensics

Digital forensics uses scientific methodologies to collect, analyse and present data relating to digital systems, networks, wireless communications and devices. Data that if needed, is admissible as evidence in a court of law. Forensics deals primarily with the recovery and analysis of latent evidence. It's critical to ensure a chain of evidence is maintained, and it's easy to get this process wrong, rendering the evidence inadmissible if you don't know what you're doing.

Usage of computers, mobile devices and the internet for everyday tasks is ever-increasing, and these activities see us often unknowingly storing personal and work-related data on these devices throughout the day. These changes have seen a vast increase in cybercrime, civil litigation cases and cybersecurity incidents that exploit data found on these devices.

The demand for digital forensic professionals to analyse these devices, particularly in the event of a data breach, has increased exponentially, due to the sheer number of cases that organisations now face.

Cases relating to corporations being breached like Toll, BlueScope and Landmark White tend to attract media attention due to their size; however, attacks against small and medium businesses such as data breaches, fund transfers and intellectual property theft are increasingly common, costing organisations millions of dollars. Digital forensic investigators must be able to effectively respond, investigate and ultimately answer the difficult questions that arise in these cases.

## Forensic Compliance

To ensure compliance requirements are met, organisations must have had a complete, forensic examination conducted with a comprehensive report produced and kept on file; this report must also detail that a proper incident response plan has been assembled.

A breach could result in your company's data being exposed to hackers, potentially crippling operations in the short term and impacting your financial and reputational position in the long term.

Failing to conduct a proper investigation and take corrective action could see the company and its directors open to litigation if sensitive information is stolen and exploited.

## PRICING

Security investigation services are priced for each client based on your specific requirements.

## NEXT STEPS

1. Get in touch
2. Get a proposal
3. Get started

+61 8 6365 0450  
[redpiranha.net](http://redpiranha.net)  
[sales@redpiranha.net](mailto:sales@redpiranha.net)

## Red Piranha Services



AUTOMATED  
PROTECTION

AUTOMATED  
DETECTION

AUTOMATED  
RESPONSE