

# Malware / Ransomware Prevention Assessment

How resilient is your organisation when faced with a potential **Malware / Ransomware** attack?

# Malware / Ransomware, a potential Achilles heel

Malware / Ransomware attacks by nature, have proven to be a growing concern of organisations in general, given their increased frequency, technological / methodological sophistication and taking into account the different dimensions of impact.

In addition to the direct financial impacts that are estimated in billions of euros annually, there is also the impact on the image of the corporation and its operational regulation, among other different vectors.

One of the reasons that makes the defensive approach to this type of attack difficult, is the fact that malware / ransomware is the end result of a successful exploitation of an entry point into the organisation, which can have different natures, requiring a structured coordination of technology, processes and people.



# How should organisations **proceed?**

A structured and quick action plan is imperative to minimize windows of opportunity.

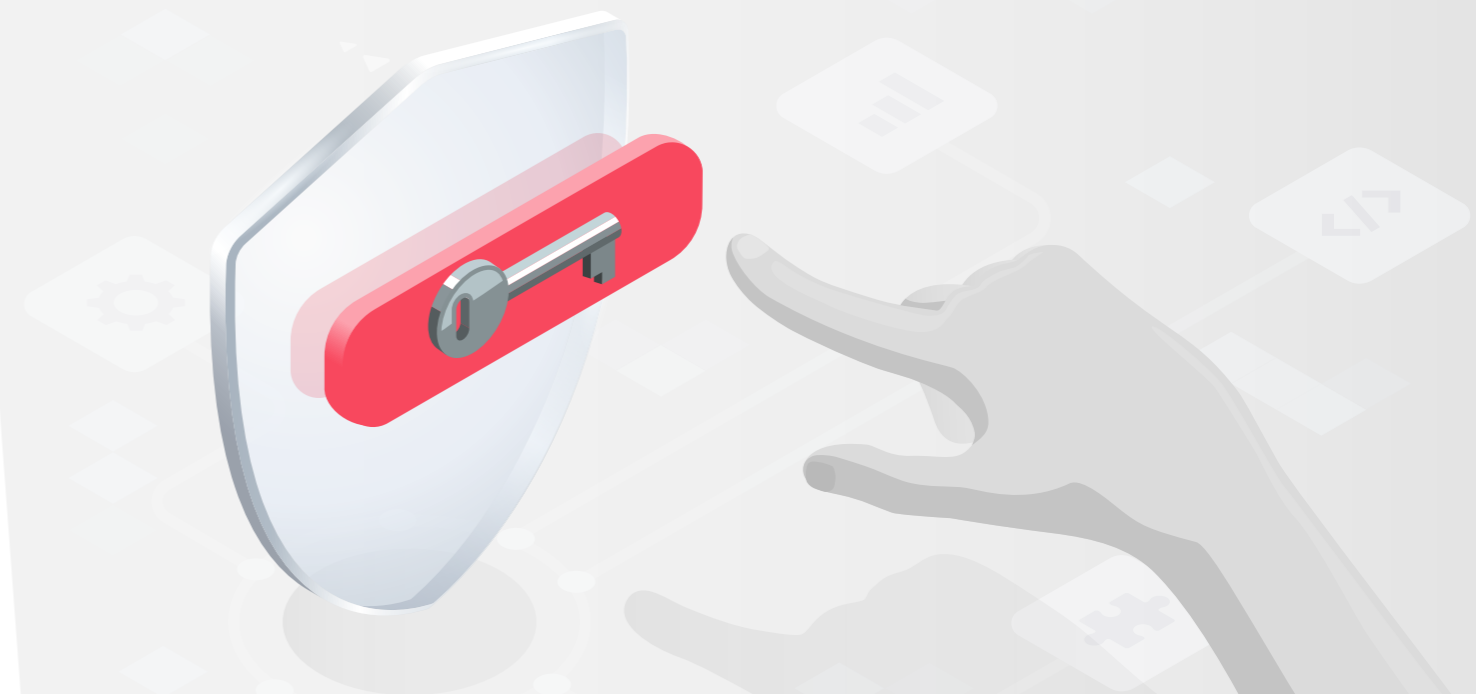
According to the relevance that this subject poses, it is imperative that organisations assess their resilience capacity and readiness in terms of prevention, detection and response to the threat.

Organisations should **assess new potential risks** to their business and information **as soon as possible** and adapt to this new threat in order to improve their resiliency.

Organisations shouldn't limit their risk assessment to technology, there is a need for a broader approach in terms of existing processes and employee's level of awareness.

**Risk assessment is an essential factor in information security in terms of identifying risks in a proactively manner, according to the threats, vulnerabilities and its' potential impact resulting from a successful exploitation.**

**Addressing risks as soon as possible will allow organisation to minimize windows of opportunity and will mitigate any potential weaknesses before resulting in serious incidents.**



## Why a risk assessment with **Devoteam Cyber Trust?**

We are a recognized company specialized in Cybersecurity services, making us the right partner to help your organization to quickly ensure and design a mitigation plan for this scenario.

This service leverages our experienced Consulting and Pen-testing teams, in combination with the Assessments Module (IntegrityGRC), to provide fast and accurate results.

The evaluation process will be conducted in order to assess the maturity and level of applicability of the organisation in each of the controls of the seven evaluation domains.

As a result of this assessment, organisations will be able to know the risks identified, their levels of severity and the recommendations, having an action plan to implement.

Organisations will also be able to efficiently manage their mitigation plans, extract reports and manage risks on our IntegrityGRC platform, already included in this service and without any additional costs for that purpose.

Be aware of your risks.  
**Be Smart. Be Secure.**



# Who

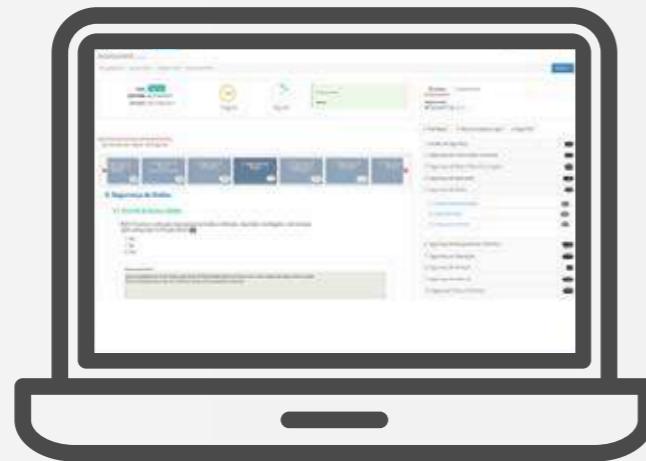
Technology

---

Processes

---

People



The service takes advantage of IntegrityGRC platform in the organisation's assessment processes.

# Assessment Domains

**Network**

**Systems**

**Perimeter**

**Remote Work**

**End-Point**


**User Awareness**

**Incident Response**




# What are your **benefits?**

**We take advantage of our 15 YEARS EXPERIENCE** on CyberSecurity Services to outline a very effective and ready to deliver service to help organisations to quickly assess their risks under this context.



**ENVIRONMENT SPECIFIC BUT VENDOR AGNOSTIC**

As a vendor independent provider for Cyber Security services, we focus on your needs and bring in our practices combined with adequate tools, people and methodologies.



Utilizing our ready to deliver service you benefit from our broad research and real experience from dozens of risk assessment processes that we have delivered over the course of last years.

**SAVE TIME AND EFFORT & REDUCE RISK**

**Devoteam Cyber Trust** is the right partner to support your organisation in this intense and evolving threat landscape, with best-in-class Offensive Security Services.

This is why dozens of medium-large clients from over 20 countries worldwide trust our services.

We are happy to share **our experience** and help you improve your **cybersecurity practice**.

**Balanced risk management requires a solid strategy.**

**Talk to us.**

## Contact us



✉ [info@integrity.pt](mailto:info@integrity.pt)

Present in **18 countries in the EMEA region**

[www.integrity.pt](http://www.integrity.pt)





[www.integrity.pt](http://www.integrity.pt)

[www.devoteam.com/expertise/cyber-trust](http://www.devoteam.com/expertise/cyber-trust)

**Devoteam Cyber Trust is the Cybersecurity specialist arm of the Devoteam Group. With our 800+ experts located across EMEA, we aim to establish cybersecurity as an enabler of business success rather than a gatekeeper. We leverage an end-to-end approach to Cyber Resilience, Applied Security, and Managed Security services to secure the tech journey of large and medium-sized companies from all sectors and industries.**

Since 2009, previously known as INTEGRITY, our team based in Portugal is specialised in providing cutting-edge Managed Security Services that combine its expertise and proprietary technology to consistently and effectively reduce the cyber risk of our clients. The comprehensive service range includes Persistent intrusion Testing, ISO 27001, PCI-DSS, GRC Consulting and Solutions, and Third-Party Risk Management, ISO 27001 (Information Security), ISO 27701 (Privacy Information Management) and ISO 9001 (Quality) certified, PCI-QSA, and member of CREST and CIS - Centre for Internet Security, we provide services to a considerable number of clients, operating in more than 20 countries.



[www.devoteam.com](http://www.devoteam.com)

Devoteam is a leading consulting firm focused on digital strategy, tech platforms and cybersecurity.

By combining creativity, tech and data insights, we empower our customers to transform their business and unlock the future.

With 25 years' experience and 10,000 employees across Europe, the Middle East and Africa, Devoteam promotes responsible tech for people and works to create better change.

Creative tech for Better Change