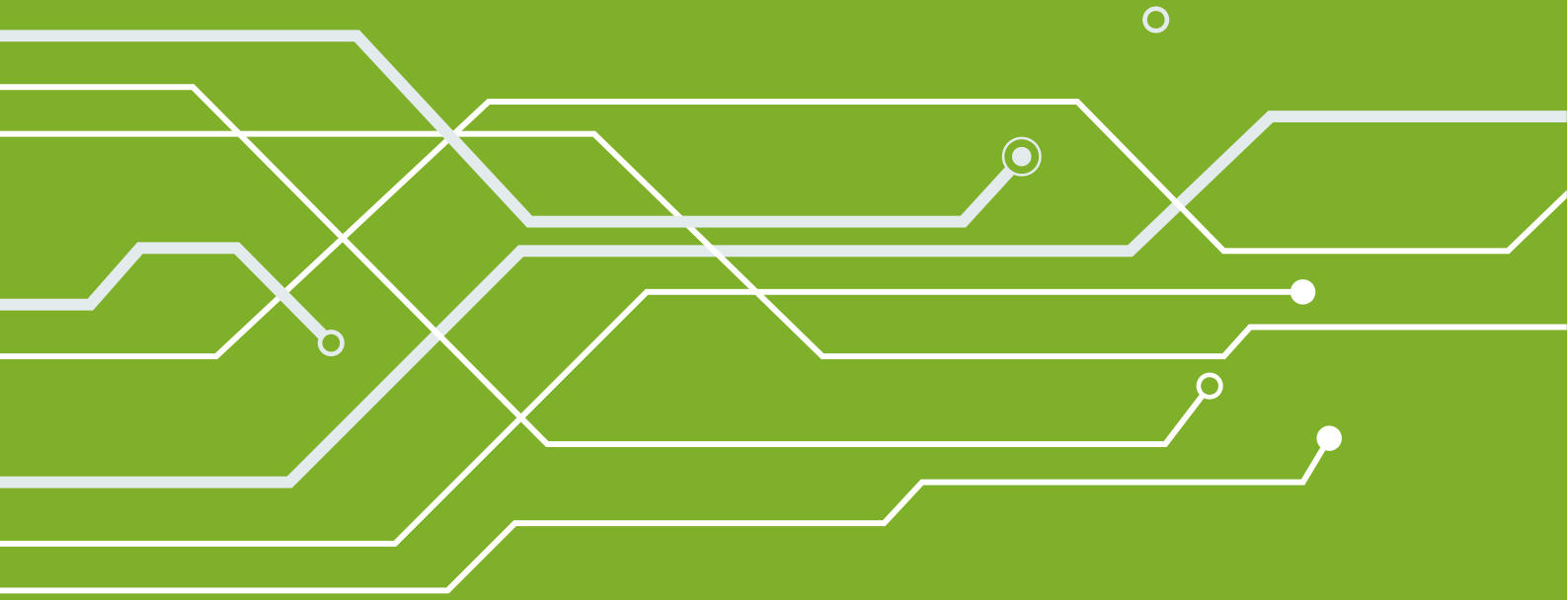
diverto

YOUR INFORMATION
SECURITY EXPERTS



Diverto is a company that provides a high level of information security to companies, institutions and other organisations in an information-centric world. We protect our clients against security threats that can cause data breaches, financial loss and damaged credibility.

Founded in 2007, we are considered one of the pioneers of cybersecurity in this part of the world and have only continued to grow in strategic and technical expertise.

Contact us: **info@diverto.hr**
Our website: **www.diverto.hr**

Information security in your organisation

If you're wondering whether your organisation needs information security, the answer is yes. We're here to find the security solutions that keep you safe while maximising price-performance ratio.

How do I choose the right information security partner?

Information security is not a quick fix, but a continuous process, and your information security company is truly a strategic partner in protecting and fortifying your business.
Look for a reliable partner whose skills and expertise you can trust, and who has the credentials to prove it. Someone driven to eliminate every threat and defend your business, but who also understands the imperative of confidentiality.

As any other business partner, besides being highly capable and specialised, your information security partner should also have its finger on the latest developments, trends and threats in the field of information security.

CHIEF INFORMATION SECURITY OFFICER AS A SERVICE

Many organisations entrust their CISO function externally, primarily because of cost reduction, advanced technologies and skills that a third party can offer, as well as 24/7 support and flexibility.

We have built-up work mechanisms and ways of collecting knowledge and information. We also have access to experiences from the environment, which is one of the foundations for security management. We bring that knowledge and information into your business.

Should I approach information security as a strategic initiative or an operational task for IT?

The first step is acknowledging that information security is not an add-on, but a necessity for operating your business. With cybercrime on the rise, it is crucial to know right where you stand when it comes to your organisation's information security. If you tackle information security as just one of IT operations tasks, you will never achieve more than a basic level of information security in your company.

STRATEGIC PLANNING

We can provide you with information security experts who will influence your business, help with building organisational capabilities and power up your knowledge while making sure your business assets are safe and secure.

Our approach is designed to help you intelligently prioritise tasks based on real risks and develop a cost-effective strategy for dealing with information security threats and attacks.

Get our support while:

- Aligning information security with the strategic direction of the company
- Establishing ISMS as a governing policy
- Conducting risk assessments and GAP analysis
- Establishing standard operation procedures - SOP
- Assessing third parties
- Implementing SOP (physical, environmental, operational, communication security)
- Building your Business Continuity Management capabilities

How do I align my information security with best practices or relevant regulations?

Figuring out security compliance requirements and keeping track of ever-changing regulations can be a strain on your time and resources. Our experts are here to help you implement methodologies and processes that will bring you in compliance with those practices and regulations that address your business or are relevant to it.

COMPLIANCE

To understand how legal and regulatory obligations affect your organisation, and more specifically, if your current security controls are adequate for achieving compliance, we perform a thorough impact assessment.

Being compliant is all about risk management, therefore, we apply a risk-based approach when assessing the impact that results with a business-compliance model and the complete roadmap for aligning your business functions, processes and controls.

While we are at it, we will use our experience and advise you on how to improve overall operations, save you some money and make your company more competitive.

Basically, we help you understand which compliance requirements are relevant to you, how they are related to your business needs and how to ensure that you are compliant.

Our compliance team performs:

How do I determine if our current approach is good enough to protect us?

Because every organisation is unique, your information security road should start with an evaluation of your organisation's security posture. Being audited by a third party gives you a complete picture of your current state of information security and capabilities. Also, we give you feedback with specific recommendations that will help you reach your desired level of security.

As a result, you will have an overview of all standard information security areas and recommendations based on best practices and standards.

INFORMATION SECURITY ASSESSMENTS

The best way to assess and understand the level of your organisation's information security is to execute a comprehensive security review. However, if you would just like to assess certain solutions, applications or business models against security standards, we are here for you as well.

Our methodology is based on proven industry-accepted frameworks.

We conduct customised interviews with key staff members to identify the information protection requirements, review the current risk management practices and collect other relevant data to understand the current security processes implemented in your organisation. And you can be sure that we will be right there with you during the information gathering process.

Our goal is to understand your approach towards information security, how it is or can be governed, configured and managed.

The result is a detailed report with prioritised recommendations on how

$21,155	31%	21%
average cost of a data breach per day	of organisations have experienced attacks on operational technology infrastructure	of all files are not protected in any way

How do I determine which level of my organisation is exposed to information security breaches or attacks?

A breach or attack can cause major consequences for an organisation's business. Losing valuable data or intellectual property can lead to reputational damage, great financial losses and fines. To prevent this from happening, it's important to thoroughly test and identify the pain points of every level of your organisation's system.

VULNERABILITY ASSESSMENT & PENETRATION TESTING

In order to get a grasp of potential weaknesses and vulnerabilities in your organisation and start checking off that list, it's best to have a complete analysis. Most organisations make the mistake of assessing their organisation's information security measures from a defensive standpoint when they should be tackling it from an attacker's perspective, who will exploit the weak spots the organisation was not aware of.

By adopting the offensive role, we test and probe your organisation's internal and external systems to pinpoint its vulnerabilities and weaknesses.

600%	56%	24,000
increase in attacks on IoT devices in the last year	increase in mobile malware variants in the last year	malicious mobile apps are blocked every day

We perform targeted tests to evaluate your information security posture and detect cracks in your information technology, but also your employees. Phishing testing and education can help employees recognise attacks and prevent further damage to the organisation.

Examples of services we provide:

Social engineering testing

Internal and external vulnerability testing

Industrial control systems testing

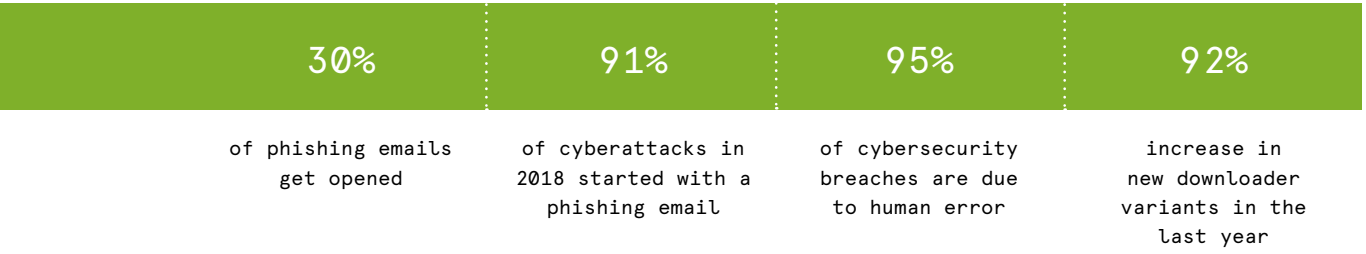
Internal and external penetration testing

Application testing

Product testing

Why should I educate my employees on the importance of information security?

You can (almost) always fix hardware, but you can't do the same with people, as they are the weakest link in any system. A simple convincing phone call to your organisation's call center can lead to loss of information, money and reputation. Because people are most vulnerable to deceit and various scammings, the only way for them to recognise and avoid potential threats is to know more on information security.



EDUCATION AND TRAININGS

We offer various education courses and seminars — from general security awareness for specific departments and employee roles, to specialised trainings aimed to educate software developers.

Based on your field of operation and parts of organisation, we assess the methodologies being used within sessions in order to achieve the needed level of awareness. We also assess our sessions and upgrade them towards your needs.

These are some of the most requested trainings, but we have experience in tailoring any security-related education to our clients' requirements:

Information security awareness session

Social engineering awareness session

System security from an offensive perspective

Secure development techniques training

Security training for system administrators

Security training for network administrators

What if an information security breach has already happened?

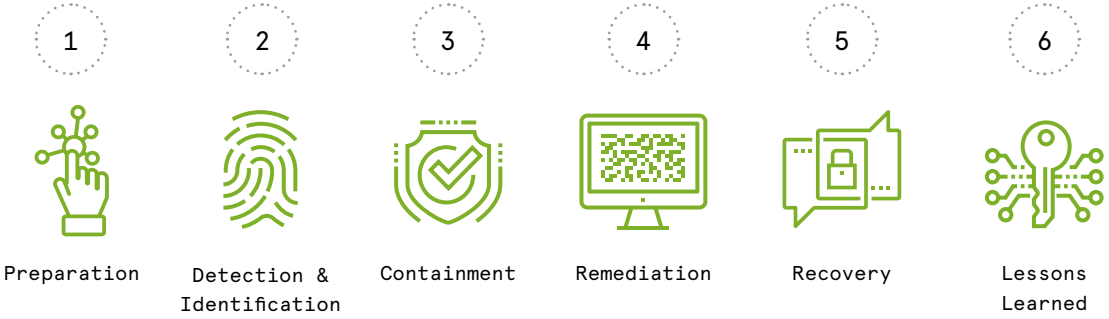
Unfortunately, sometimes it takes an incident to happen for organisations to realise that their systems are not in line with information security standards and protocols. In this case, it's important to seek help immediately, because a quick reaction can help prevent further losses.

INCIDENT RESPONSE AND FORENSICS

Our experts coordinate and perform complex forensic services, assist you in preservation of data and help you manage the consequences of security breaks or attacks.

We perform analyses of security incidents ranging from desktop compromises, mobile and IoT devices to system-wide issues such as industrial control systems and assist in the preservation of lost or compromised data. Our experts are experienced in managing the consequences of security breaches or attacks and can offer guidance in just about everything — from preparing evidence for potential court proceedings to how to communicate a breach to the public.

We provide services in every step of the incident response six-step process:



How do I defend my organisation against a hacker attack?

From the information security standpoint, cyberattacks are a part of an alarming trend.
Their goals are mostly to steal, expose, alter or destroy information, and disable the functioning of an organisation — which can all lead to disastrous losses. Protecting your organisation from threats is a continuous process, but it all starts with a change in mindset.

DEFENSE SERVICES

Thinking like an attacker is often the best defense, that's why we believe in balancing both the defensive and offensive approach. By identifying attackers' objectives, potential targets and ways they could carry out an attack, we assist you in raising the bar for potential attackers. We fine-tune your perimeter, making your network more resilient to attacks and making incidents more visible after a breach has occurred.

frequency of hacker attacks

of cyberattacks target small businesses

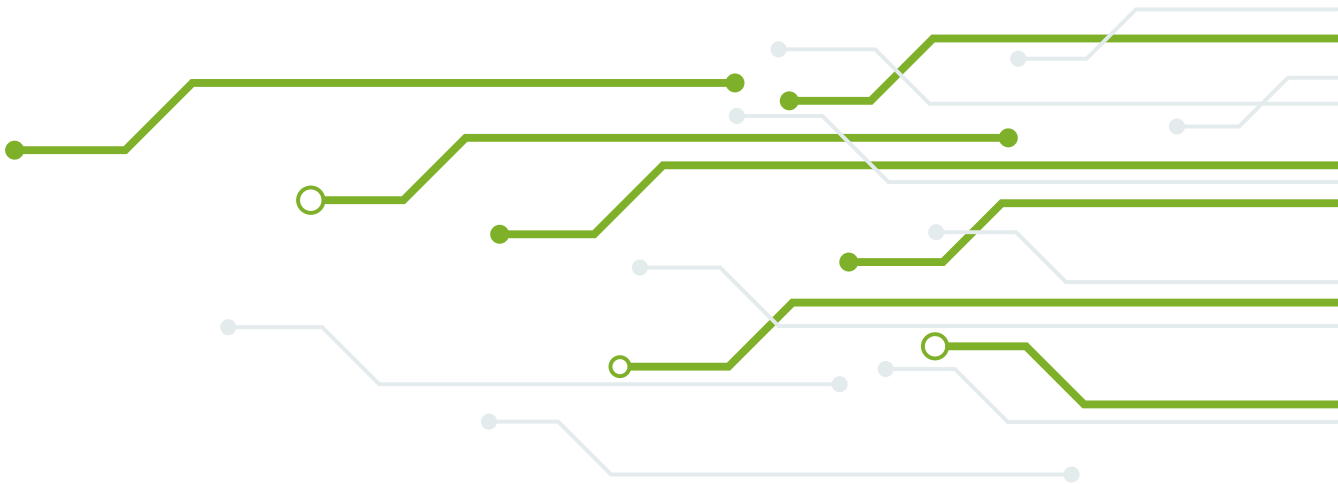
of data security breaches are caused by malicious intent

of businesses suspend activity within 6 months of a cyberattack

How do I catch another cyber incident in time?

Every organisation has something it needs to protect — intellectual property or employee, financial, client or other confidential data. So why would you even risk another incident?

12%	101 days	100%
of companies believe they are prepared for a cyberattack	the average time it takes to identify a malicious attack	of all incidents in 2018 have involved login data theft



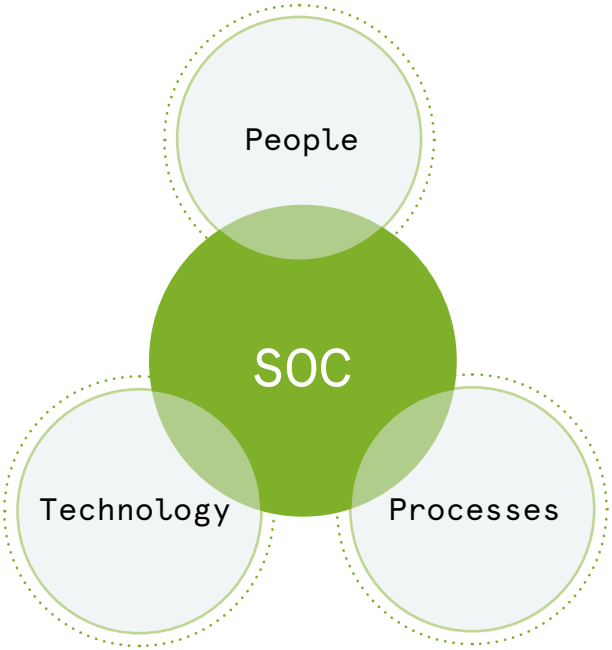
SECURITY OPERATIONS CENTER

SOC is a centralised solution in charge of continuous monitoring, evaluating and protecting organisations by guarding their information, infrastructure and business against attacks. With SOC, you can react fast and save valuable time, money and reputation.

Our managed SOC solution acts as a watchdog on your network 24/7. We cover all three aspects that you will ever need to ensure information security of your organisation: we implement the technology, develop security processes and have a team that monitors daily operations. This allows for timely detection of external and internal threats, improved incident detection and incident response, improved forensic investigation possibilities and overall prevention of incidents.

Whether your organisation needs to comply with certain security regulations or wants to act proactively concerning its information security, the best way to coordinate security operations for maximum effect is to centralise your security efforts.

But building a Security Operations Center (SOC) is quite a challenge for most organisations, since it takes time, expertise and money.
That's why we developed our managed SOC solution that saves you time and money and is adaptable to every organisation, regardless of its size and complexity.



Benefits of Diverto SOC

- Adaptable to every organisation
- Flexible and cost-effective integration models
- Real-time monitoring and intelligence-based threat detection
- Compliance with regulatory requirements
- Expertise in all SOC tiers
- Fast detection and incident response
- Proactive hunting of threats
- Advanced reporting capabilities

info@diverto.hr
www.diverto.hr