Snipesec

CYBER SECURITY AGENCY

DETECT DEFEND SECURE

www.snipesec.com

www.**snipesec**.com

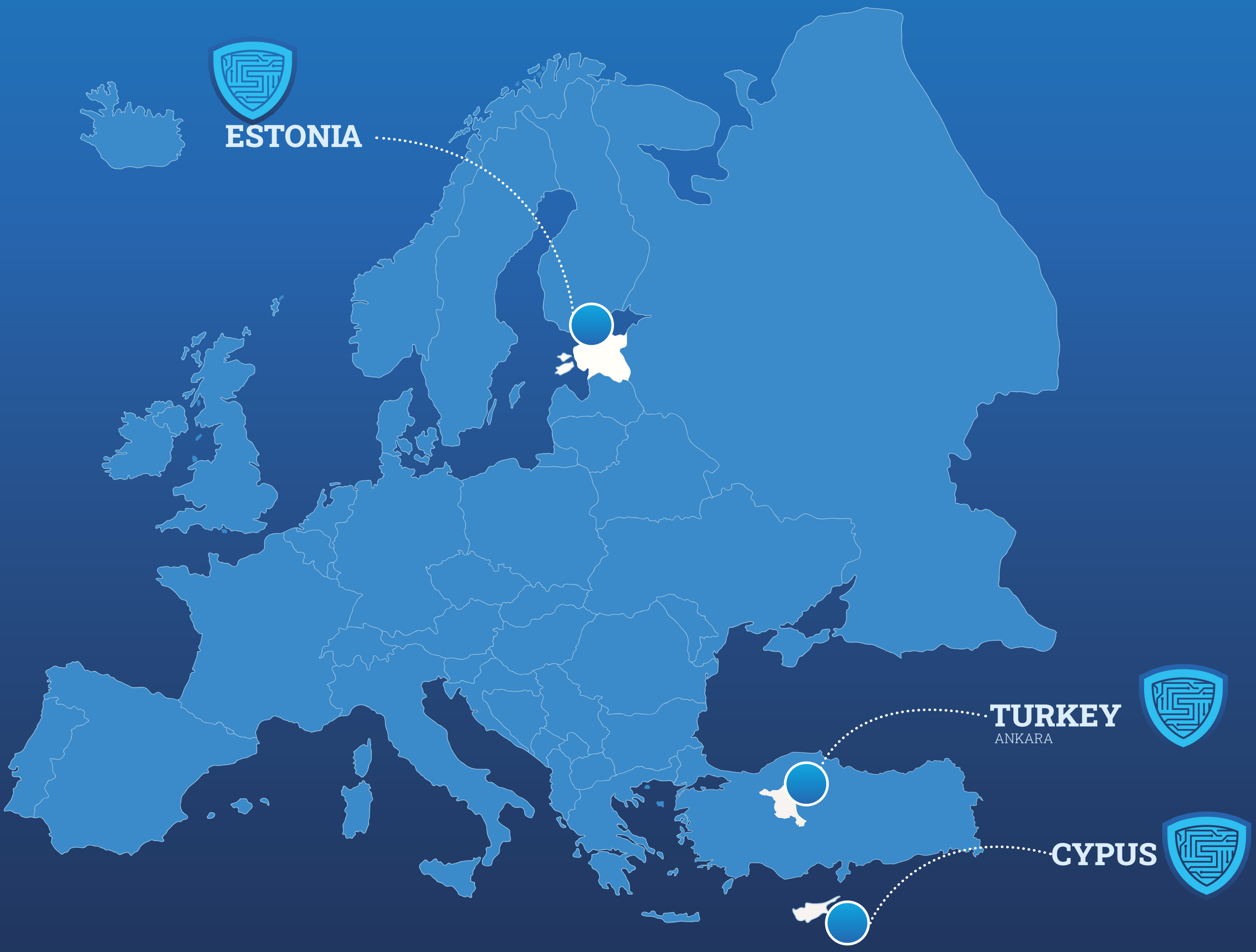
Snipesec
CYBER SECURITY AGENCY

INDEX

ABOUT SNIPESEC

Our key task: Secure your enterprise in cyberspace

Snipesec IT & Cybersecurity, Training and Consultancy Ltd., and SnipeNet Bilişim Hizmetleri Ltd. are organizations owned by SARIZADE Group of Companies that uses Snipesec brand which operates in the field of Information and Cybersecurity inTurkey and Cyprus.



Snipesec is an international cybersecurity solutions partner with operations extending from Turkey to Cyprus and Estonia, providing its clients with superior service quality.

It has over 10 years of experience in the IT sector and holds ISO 9001:2015 (Quality Management System Standards), ISO 27001:2013 (Information Security Management System Standards), and General Data Protection Regulation (GDPR) accreditations. This demonstrates that the company meets all quality standards.

Additionally, Snipesec has launched its new Remote Desktop Service, “Neptune.” This innovative solution helps startups, businesses, and other organizations work remotely as if they were in the same office, making it one of the most forward-thinking services in the market.

WHY
CYBERSECURITY
IS IMPORTANT?

Cybersecurity is important to every organization, no matter how big or small it is.

There are roughly **4000 cyber** attacks every day.

Cybercrime continues to increase is because it is

CHEAP > FAST > HIGHLY PROFITABLE

Cybercrime can cost businesses millions of dollars in damages. But it's not just about financial costs, it can also damage their reputations, and their ability to do business, and sometimes even compromise the physical safety and health of employees, patients, customers, and others.

Cybersecurity builds trust. Cybersecurity affects trust with customers and employees. When people don‘t feel that their information is being properly secured and kept private they begin to lose trust in the brand, the product, and the services.

HACKERS ARE GETTING ADVANCED EVERYDAY

A successful business can develop only when it is safe and protected

Our expert team specializes in securing your data from unauthorized access and malicious a attacks

Hackers are no longer simply driven by curiosity

Cybersecurity saves your company millions, reduces stress, and saves time through competent detection and high-quality defense.

And that's what our team takes on!

OUR SERVICES

Penetration Testing

?

Are you sure that your company's security policies are genuinely effective?

How much does your organization depend on IT infrastructure?

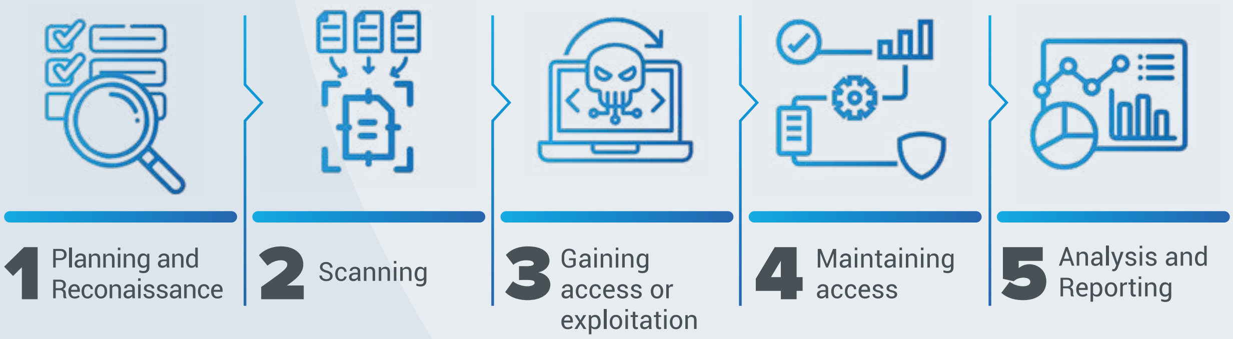
How much would it cost if that IT infrastructure is disrupted for a day?

By answering these questions you will find out the importance of security in cyberspace.

Most organizations are not aware of the risks and their impact on them. They cannot imagine the diverse ways in which their system can be hacked. When you know the risk, you take precautions so you can minimize or prevent the threat. That is what we can help you with.

We hack your system.

We perform an authorized simulated attack just like a hacker would, examine your system, and discover security vulnerabilities in order to prevent malicious attacks.



1 Planning and Reconaissance

2 Scanning

3 Gaining access or exploitation

4 Maintaining access

5 Analysis and Reporting

First, we define a goal and analyze the system. Then, we scan the vulnerabilities in order to see if they are exploitable or not. Next, the attack is performed once the exploitable vulnerability is found. After gaining access it is important to maintain it so there is always a back door that you can use to come back. At the end of the pentest, the client gets a report about the vulnerabilities of his system and the ways of fixing them.

Incident Response CYBER AMBULANCE

If you face any difficulties with your system we are one call away from you.

Your employees come to work and all of a sudden there is an unknown virus that doesn‘t let computers perform? Or there is a hardware issue that makes your network stop functioning? When you face this kind of situation and you need instant help, you can call SnipeSec 24/7. We immediately arrive and solve the issue that your business has faced. There are different cyber threats, including data leakage, service interruption, disaster recovery, and attacks on backup resources.

In the event of a cyber-incident that your company may encounter, if the incident response is done too late or in panic by people who are not experts, the response given may cause serious damage to your company.

As SnipeSec, our incident response teams (CSIRT), which we have formed from experts and people with specialized skills, provide Incident Response service in order to protect the continuity and security of your corporate operations in any cyber incident that your company is exposed to.

We take all necessary precautions against a possible data leakage within your company resulting in your critical customer information, financial information, or various plans/ projects being leaked.

Our emergency response service operates 24/7/365.

OUR SERVICES

Security Operation Center Service

24/7/365 surveillance of your system

Do you want to be sure that your network is monitored 24/7/365 so that in case of any incident actions are taken immediately?

That is why we are providing a SOC service. You have a remote IT team that is handling all your technical side of the business. Moreover, with SOC you are paying only for the service. You do not have to worry about additional employees in your company, about the equipment, additional office, etc.

Small and Medium-sized companies can benefit from the Security Operations Center Service (SOCaaS) quickly and efficiently, with a simple monthly invoicing model based on infrastructure size and the number of people.

The Security Operations Center (SOC) is an in-house central structure established for the purpose of detecting, analyzing, preventing, and responding to all internal or external cyber security incidents against your company and helps you to continuously monitor your security status and make improvements where necessary.

SOC as a service is an excellent solution for both mature and start-up companies, who wants to improve their security.

During SOC service our consultants will:

- **Report on the current state of vulnerabilities and security**
- **Suggest the optimal cybersecurity architecture and strategies for cost optimization**
- **Implement and customize the necessary security toolkit and establish supporting processes**
- **Take over all the SOC responsibilities based on the package**
- **Report regularly on new findings and further improvement ideas**

We're here to maximize your company's security!

Security Operation Center Service

BENEFITS

- Suited for companies at any level
- Security levels and protection is customized to your company
- Access to in-demand cybersecurity talent and domain expertise
- Customizable levels of security and support coverage
- High service levels with all the corresponding metrics
- Technology investment consultancy and assistance with meeting compliance requirements
- Support of custom SOC use cases for scenarios that are out of the ordinary
- Continuous security improvements and advisory

CHALLENGES

- **IT infrastructure visibility is required.**
  Prior to setting up a SOC, it is essential to conduct an infrastructure audit to achieve an end-to-end view of its components. Security experts underline the importance of providing them with a comprehensive assets inventory and data classification to enable efficient SOC performance.

- **Establishing effective communication.**
  Having delegated SOC to a chosen security provider, one should provide a single point of contact to enable effective cooperation. Choosing one contact can boost the efficiency of the SOC team

OUR SERVICES

Security Operation Center Service

Do I need SOCaaS service?

You have questions about whether you need this service or not? Let's first ask you some questions then.

- If an unknown person got into your network and gained access to sensitive information about your company would you know/when would you know about it?
- If your current employee changes or upgrades his privileges in order to gain access to unauthorized information how would you notice it?
- What if all of your databases don‘t function anymore and you lost all of the data which is critical for your business? How fast would you realize this situation and how would you solve it?
- Would like to know if there is just an attempt to hack your system? Who is it? Is it one of your competitors who want to learn your plans or steal your customers?
- If the information flow through your company‘s web applications began to be stolen, would you know about this/when would you know about it?
- A type of malicious software (virus/Trojan/ransomware (ransomware) etc.) has started to spread within your company by infecting your employees' computers/computers. When would you notice this? How long can you afford to wait to intervene?

Snipesec

CYBER SECURITY AGENCY

OUR SERVICES

IT infrastructure service

We build your infrastructure.

If your company's IT infrastructure is not properly implemented, businesses can face connectivity, productivity, and security issues—like system disruptions and breaches. If your Customer Service Department will not be able to properly communicate with the Marketing and Sales Department, or if Human Resources will access the data that should be available for only Accounting Office you can imagine the chaos which will appear in your organization.

A 60-person team.
All about;
SECURITY.

We install hardware and software components in your company's IT infrastructure and ensure that the security and recording systems of your company are properly configured.

After installation, we provide support to enhance your company's business operations, and we immediately intervene in any software or hardware failures that may occur in your information systems.

You will get a detailed report about the installation, periodic maintenance, and license renewals of all hardware and software.

IT infrastructure service

Setup

We perform the installation of hardware and software components in your company's IT infrastructure.

Configuration

We ensure that the security and recording systems of your company are properly configured.

Operating

Our expert staff provides support to your system infrastructure to enhance your company's business operations.

Troubleshooting

For the continuity of your company's operation, we immediately intervene in any software or hardware failures that may occur in your information systems.

Reporting

We can provide detailed reports regarding installations, maintenance/repairs, operations, or problem/fault removal processes within your company for you.

Update

Our team can apply the necessary updates to the hardware and software of your company's information systems.

Training

We provide you with the manager and user-level training and training material according to the information systems you currently have in your company.

OUR SERVICES

Digital Transformation and Consulting

We assist you in modernizing your business

Did you know that companies with a higher level of digital maturity enjoy the higher sales growth and resilience than their peers? A digitally mature organization is one that is making the best use of digital technology and its associated culture and networks in everything it does. Digital maturity is being fit for the world as it exists today, and for the people in it. Digital Transformation can improve your existing processes by automating them, thus increasing the profit significantly. But before implementing Digital Transformation, there is a need for Digital Maturity Assessment in order to know where your company is right now and to what extent it needs to be improved.

Alongside this service, we also ensure that your company keeps up with technology and move your business boundaries beyond the borders of the country.

In the consultancy process that starts with the creation of your company profile and SWOT analysis, we create all the necessary strategies that will add value to your company by determining all aspects of your company and planning your digital transformation processes.

We provide you with consultancy services in all technological matters (purchase-sale, investment, project design, profit-loss analysis, etc.), and we support you in all your investments that you plan to make with your company in the field of technology, within the scope of our international connections.

Dijital Maturity Assessment

Investing in
your digital maturity
is investing in
your success.

There's almost nothing technology can't improve these days, so it's worth investing the time and effort to do a digital maturity assessment and find ways that technology can solve your business' biggest hiccups and keep your employees challenged, engaged and motivated. With an open mind and an eye on the future, your business can overcome what's holding it back so your
success is full speed ahead.

After investigating digital maturity you will get guidance and advice about measuring and improving your digital maturity, or help using your digital maturity insights to build a digital strategy.

If your organization does not constantly transform with time and technology- it's life expectancy will decrease

OUR SERVICES

Malware analysis

CHECK MALICIOUS FILES

Nowadays there are more than 20 types of malware that can disrupt the performance of your business. They all have one thing in common - all of them make companies lose millions. Hackers around the world tremendous amount of profit by targeting small, medium-scale, and large enterprises. Back in the day, people could steal from your store directly, that is why every building has surveillance cameras to protect from thieves or to punish them by finding out their identity. However, stealing through a digital network requires less effort, it is cheaper and more profitable than stealing some items from the store.

That is why there are thousands of hackers around the world who invent various kinds of sophisticated malware. They target everyone because the internet nowadays is not bounded by country, language, or other characteristics. Organizations might not even be aware of the fact that their network is infected. And at the moment when they least expect, it strikes taking down everything valuable for the organization and pausing its performance.

With the Malware Analysis service, in-depth analysis and cleaning services are provided for malicious software derivatives (malware, ransomware, dropper, spyware, etc.) that have infected your company or your entire computing infrastructure and provide protection for your company's systems.

We ensure that all necessary measures are taken for you to recover all your data, which is critical for your business operations and in the infrastructure of your company that has been victimized by malicious software, and to prevent the recurrence of these attacks.

Malware analysis

Types of Malware

RANSOMWARE

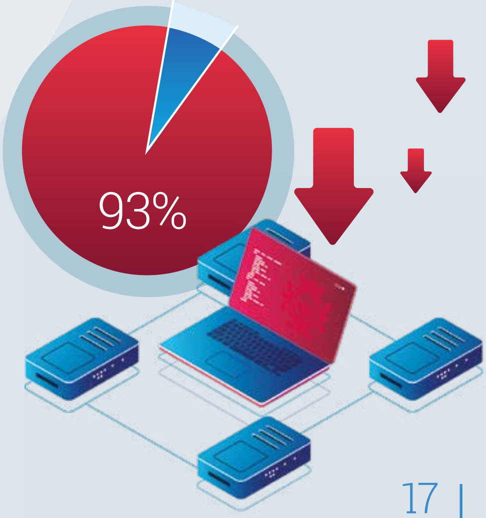
How much does your business depend on computers and the data that is in them? What if all the networks that you have will stop functioning for a day? How much money will your business lose in a day?

What about weeks? This is what hackers are calculating right now. After calculations, they break into your system, encrypt your files or change your password or do something else to hold your system until you pay up. So one day you walk into your office, open your computer and you see something like this, “Your computer has been locked. You have to pay a fine of $10,000 and be able to pay it through Bitcoin using this link if you want to get access back. If you pay me, then I'll give you the secret unlock code and then you can put that in the little white box and hit okay “. And oftentimes, even if you pay up, they won't give you access back to the key. In the best case, they do. In the worst case, they've now taken your money and you've got nothing to show for it.

Ransomware can be very painful. The attackers make businesses poorer. There is big money, hundreds of millions of dollars, maybe even billions of dollars per year in ransom attacks, and hackers get much much richer. The best cybercriminals in the world like some of the young guys in St. Petersburg or in other cities around the world they're making a million dollars a month. And they target all kinds of businesses from small to big.

Cybercriminals can penetrate 93 % of company networks.

In 93 percent of cases, an external attacker can breach an organization' s network perimeter and gain access to local network resources.



Malware analysis

Types of Malware

VIRUSES

Viruses may run on computers without your knowledge. Maybe you've gone to download a new program from a website that you need for your work. And when you download that installation file inside of it there may have been some malicious code. When you run the program to install it, you're allowing the code to be installed in your machine and that virus now can take hold. At this point, the virus is going to want to reproduce and spread and it does this because you have taken a user action. In this example, you installed the program and that allowed the code to be run and the virus to start doing its nefarious things (crash apps and programs). This allows it to begin to replicate and spread across your network. There are various types of viruses with different levels of complexity. Our antivirus providers are getting better and better all the time at understanding viruses and how they work and how to stop them. However, there are encrypted viruses that are making it harder for virus makers to find these types of viruses. And so again, this is one of those things of the good guys get better so the bad guys get better.

Malware analysis

Types of Malware

TROJAN HORSE

Before we can dive into this piece of malware, let me give you a quick history lesson.

Going back a couple of thousand years ago, Greece and Troy were at war. This lasted for about 10 years, with no end in sight. After a long siege, the Greeks started getting restless, and they decided that they were going to go try something different, so they went out and constructed a large wooden horse. And they were going to give it to the city of Troy as a peace offering. This seemingly harmless gift was actually filled with Greek soldiers, and once it was wheeled inside the city, the day turned to night, and the soldiers from within came out of the horse. They opened up the walled city's gates and let the invading Greek army into the city, and they laid waste to it. This was the first example of a Trojan horse.

Now, in computers, Trojan horses work very similarly. Basically, a Trojan says, I'm going to perform this function for you. And it will perform that desired function, but it will also perform a malicious one, too.

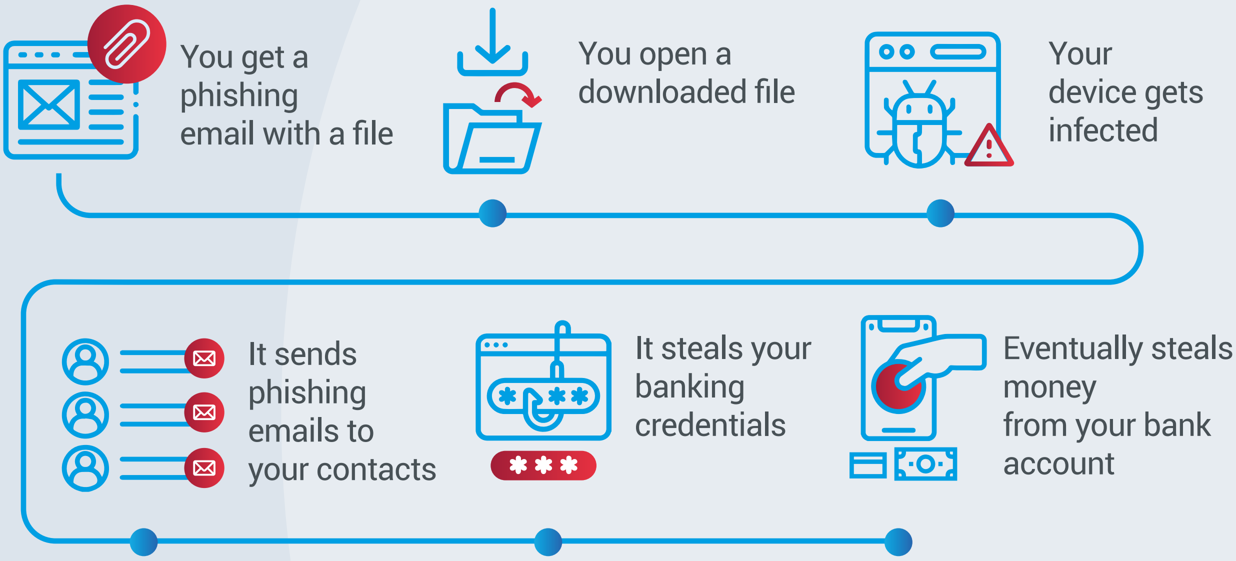
Now, back when we were kids, there was this new game that came out called Tetris, and it was all the rage. It was an extremely popular game and everybody wanted to get a copy of it. And so, a lot of times, your friends would give you a disc and say, hey, go ahead and install this, and you can play Tetris. Well, one person was really smart, and they decided to use a copy of Tetris and embedded a Trojan horse inside of it. So you'd take the disc and you'd put it in your computer, you'd turn on the game, and it would play just like normal. But what was actually happening behind the scenes was that it opened up a connection between your system and their system, allowing your friend to have remote control over your machine which can lead to stealing critical data and sending it elsewhere, deleting or modifying files, or otherwise disrupting the regular use of your IT infrastructure.

We ensure your secrecy to enhance security which leads to victory

Malware analysis

Types of Malware

MALSPAM



You get a phishing email with a file

You open a downloaded file

Your device gets infected

It sends phishing emails to your contacts

It steals your banking credentials

Eventually steals money from your bank account

Emotet is an attack that is primarily spread through email spam (malspam). You can get an email that is disguised as a legitimate email from Amazon, from your bank or a note from someone you know which tells you to click a link or download an attachment. You, thinking that this is a legitimate email, will not hesitate to do so. Especially, if this email is coming from someone you know. This is how the initial infection is made.

It will then try to spread onto connected systems in three main ways. First, now this time it will access your contacts and send a phishing email that appears to be from you. Next, it will try to use known software vulnerabilities to spread itself to other systems on your network, which can be other computers in the house or in your organization. Finally, it will try to get all the information by hacking the password.

At its peak, Emotet infected 1.5 million computers around the world and caused an estimated US $2.5 billion in damages before it was brought offline.

Malware analysis

Types of Malware

BOTNET

Do you know that your phone or your laptop can be part of the botnet right now? A botnet is when hackers make bots out of your device and perform attacks through them. You will not be aware even if your device is infected. Often times cybercriminals will seek to infect and control thousands, tens of thousands, or even millions of computers. So they can act as a master of a large zombie network or bot network.

The consequences of being a part of a botnet can be very serious. Some risks include:

- High Interent Bills
- Slow and Unstable Computer Performance
- Stolen Personal Data

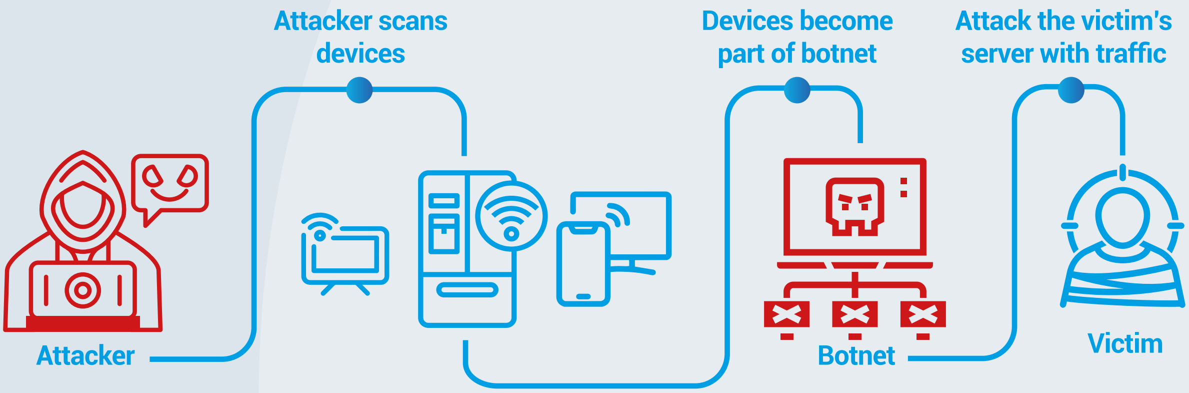
It is easy to become a part of a botnet by downloading something from an unknown website for free or filesharing. Even social media sites or apps can turn your computer into a bot.

One of the most successful pieces of the botnet is called Zeus. It afflicted millions of devices. Moreover, the virus continues to generate new variants, spawning on new hosts, and expanding its reach. Once the Zeus virus installs itself onto your device it can perform two serious actions. Firstly, it forms part of a botnet. The botnet allows the owner to collect massive amounts of information and execute large-scale attacks. Secondly, the malware can act as a financial services Trojan that steals banking credentials through website monitoring in Keylog The Zeus virus recognizes when a user is on a banking website and steals the keystrokes used for logging in. Eventually stealing money in your bank accounts.

Malware analysis

Types of Malware

BOTNET


Attacker scans devices
Devices become part of botnet
Attack the victim's server with traffic
Attacker
Botnet
Victim

Another example of botnet malware is called Mirai. It is also referred to as a worm. Mirai targets the smart devices within your home network which include all the smart devices you have such as smart TVs, toys, smart fridges, smart door locks, sensors, etc. This malware has been used in some of the largest cyberattacks ever recorded.

In 2016 hackers managed to infect thousands and thousands of household devices like printers, baby monitors, cameras, and smart refrigerators just like those you may have around your home. They took control o smart devices and used them to flood the servers, and have an important internet infrastructure company with malicious traffic appearing to come from millions of Internet locations. Many major websites became unavailable to users in Europe and North America. A big example of this attack is a cyberattack on the Dyn website, which is a DNS provider to Europe and North America. The Internet consists of domains and when your domain provider doesn't work, it means that your website doesn't work and customers can't reach it. That is why after the attack Dyn lost around 8% of its customers. As well as major US websites like Twitter, Spotify, and PayPal being affected, numerous other companies worldwide also suffered connectivity issues, such as HSBC, BankWest, and Ticketmaster. It affected the customer relationship and resulted in a big loss for the company.

Malware analysis

Types of Malware

SPYWARE

You' ve probably heard the term spyware before, but what exactly is it?
Your competitors would be happy to use this against you. Normally, this will be installed from a website or some third-party software that you've installed on your system. What it does is it starts looking through all of your files, your emails, your instant messages, your calendar invites, and whatever other information you might have on your system, and it gathers that all up and builds a profile on you, that's the best case.

In the worst case, if you're typing in a website name and your username, and your password, it can collect that and send it back to the attacker. It even has the ability to take screenshots of what you're seeing on the screen, and send that back at routine intervals through email or instant message.

Every 39 seconds one cyber attack takes place worldwide.

HARDWARE ISSUES

Are you sure that the hardware that your infrastructure uses is still licensed and not outdated? Outdated legacy systems can be expensive to maintain. It's really not much different than maintaining a very old home or vehicle, except that technology ages at a much faster rate. If you are using old computers, hard drives and etc. one day your system will be crashed, or it can get infected with viruses because the manufacturers stop giving support. So you want to make sure that your infrastructure is not vulnerable to security risks and viruses due to them being outdated.

OUR SERVICES

Red Team Service

We train your existing IT team

Red Team service is a test process for auditing and strengthening your existing security infrastructure against possible external attacks against your company. Your team, which is involved in this process, learns about potential attackers and various attack methods which could take place against your system. We also carry out attack scenarios in which we apply possible attack methods in real-time, therefore gaining the ability to think like an attacker and increasing your ability to be ready for attacks.

Blue Team Service

Defend against attack

In order to increase the level of readiness against possible cyber-attacks against your company and to respond to the attacks in a timely and adequate manner, we include your internal security team in the Blue Team Service training progress.

Therefore, your internal security team will have a sufficient level of readiness during real attack situations or Red Team scenarios against your systems.

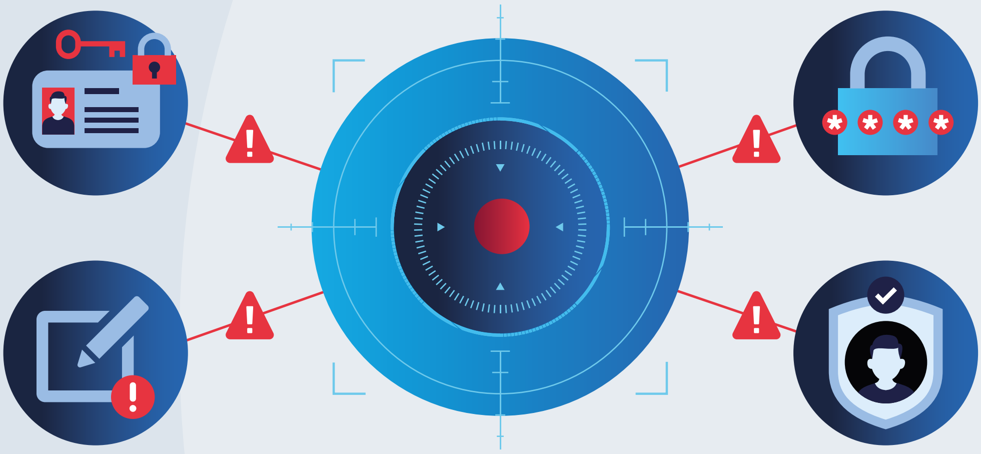
Snipesec
CYBER SECURITY AGENCY

DETECT DEFEND SECURE

ÜRÜNLERİMİZ

Cyber Polygon

Designed with inspiration from a real shooting range, Snipesec's Cyber Polygon is a focused platform that enhances the attack and defense skills of cybersecurity teams. This service is intended for public and private sector organizations, increasing their capacity to effectively use cyber tools and thus addressing the shortage of qualified experts in the field of cybersecurity.



In the Cyber Polygon, teams face various cyber attack scenarios in a realistic and controllable environment. For instance, participants work on scenarios such as ransomware attacks or advanced persistent threats (APT), where they develop their skills to detect, analyze, and respond to these threats. Trainings are conducted through simulations and real-time exercises guided by Snipesec experts. Participants reinforce their theoretical knowledge with practical applications, achieving proficiency to respond to cyber incidents effectively.

With the Cyber Polygon service, Snipesec aims to strengthen the internal cybersecurity capacities of organizations, contributing to their resilience against national and international cyber threats.

Jupiter

The Jupiter Cloud Backup Service offers businesses and individual users a highly secure and cost- effective solution for safely backing up and protecting their data.

Through automated backup processes, the risk of data loss is eliminated, and data can be quickly restored. Jupiter also scales storage according to your needs, providing flexibility that adapts to the growth and downsizing of businesses.

Jupiter protects your data from various threats, including unauthorized access and potential dangers such as natural disasters. By backing up data in the cloud, you ensure its security independent of physical storage environments. Furthermore, since backup processes are automated, manual intervention is unnecessary, which enhances operational efficiency.

Jupiter Cloud Backup Service provides high-security backup solutions at affordable prices.

By reducing data center and backup device costs, it offers a budget-friendly solution for both businesses and individuals.

Our expert team is available 24/7 to provide support throughout the backup process, ensuring you're always covered.

OUR PRODUCT

Neptune (Virtual Desktop Service)

You don’t need to rent a physical office anymore!

Sign up and Log in to our website

Select the package suitable for you

Choose the payment method and pay

Get your credentials via email

Remotely connect from any device, anywhere, anytime

Your connection goes through our servers and is protected by our Next-Gen Cyber-Firewall

With our unique anonymity system you can browse web without being traced

Having an office for your company is great! All your employees come to the office in the morning and they work in synergy. But let's think for a moment about how much you pay for the office. Did you think about its rent or its price? But what about other things that an office needs to fully operate? Furniture, computers, phones, refreshments, internet and most importantly, electricity. However, you have to have an office! Actually no. The pandemic showed us that as long as we have a stable internet connection any company can continue its operation. Everyone now is used to working online. But that work wasn't well organized because businesses had to adapt very fast and there was no elaborate, organized online office.

Well, the pandemic is finished but many companies realized that it is possible to work remotely and it is more cost-effective. That is why we present you witha unique product called Neptune. It is a virtual office for your enterprise. Your employees can work online as if they are in the same office. It is a virtual environment where everyone is connected to one network and it is a more efficient way of operating from distance. Neptune turns your physical workplace into a digital office for your remote staff.

Create your own digital office and enable remote work

Neptune is a secure remote desktop service (VDI) infrastructure designed to reduce the IT infrastructure investment costs of enterprises, eliminate maintenance and repair burdens, and provide a high-performance and flexible working environment. Your employees can use Neptune from anywhere.

Virtual Desktop Service (VDI) is a service that supports Remote Desktop Services (RDS) and was created to minimize the IT investment costs for companies and to eliminate the technical difficulties and inefficiencies faced by most organizations while managing these services.

This service is a widely used service in order to reduce investment, and maintenance-repair costs and to provide quality service for application laboratory infrastructures used in education and training activities in educational institutions and organizations beyond office workers.

WHO CAN USE THIS SERVICE?

Apart from companies operating in the field of technology, Neptune is preferred for many small and medium-sized businesses due to its ease of useand cost advantages.
For example:

- Educational institutions (classrooms, colleges, high schools, and universities)
- Hotels and casinos
- Accounting offices
- Pharmacies
- Supermarkets
- Gas stations
- Travel agencies
- Construction markets

ÜRÜNLERİMİZ

Neptune (Virtual Desktop Service)

WHY NEPTUNE?

HIGH PERFORMANCE

Neptune offers you and your employees high-performance virtual desktop machine packages with state-of-the-art high-quality hardware and software. There are different high-speed internet bands, storage capacities, processors, and memory options you can choose for these virtual machines. In the Neptune system, your Neptune network performance is not affected in any way by the increase in the number of employees included in the closed network specially prepared for you, thanks to the load-balancing systems it uses.

LOWER COSTS

Neptune keeps you away from all hardware failure and maintenance-repair costs. Thanks to Neptune, you do not need to think about hardware updates or maintenance-repair processes in the developing world of informatics, all hardware updates and maintenance-repair activities in Neptune infrastructure are carried out by us. This gives your business the advantage of using high-performance computers with very low investment costs.

SECURE FILTERED NETWORK

Neptune creates high- performance and low-cost virtual machines at the rate of computing workload your company needs, allowing all your company employees to access a flexible and secure working environment 24/7 without interruption within a secure closed network. Thanks to this closed network created in Neptune, all your employees will have the opportunity to connect to the same lab environment as if they were working in the same office (file sharing, etc.)

ANONYMOUS VPN CONNECTION

Neptune offers a secure VPN connection in line with your anonymity request for your internet connection on the machines within the virtual network you want to create belonging to your company. You can choose the type of VPN connection you want for your employees among the VPN options offered upon your request, and you can use them safely and uninterruptedly on virtual machines belonging to all your employees in your Neptune network.

SEAMLESS CONNECTION

Thanks to its powerful and redundant communication infrastructure, Neptune offers uninterrupted connections to your virtual machines. You can connect to your Neptune Virtual machine 24/7/365 without any interruption, from any point you want, with Neptune's connection program. The physical system connection lines in the Neptune infrastructure are backed up and any maintenance/repair/update operations to be carried out on the Neptune infrastructure are done within your knowledge and all operations are carried out without interruption in the system.

DYNAMIC BACKUP

Neptune dynamically performs dynamic backup operations of all virtual machines your employees use, in line with your requested time intervals (daily, weekly, monthly, etc.) The performance of the systems used by your employees during the backup process is not affected and continues to work without losing any data or work. This situation is of critical importance in terms of protecting all data on your virtual machines belonging to you and your employees.

BASIC SOFTWARE INSTALLATION

Neptune offers you all the basic software you need in virtual machines with the operating system you demand. All additional software you will request is installed in your virtual desktop Neptune machine under license. This helps you get rid of workloads such as software procurement, licensing, or installation.

GDPR-COMPLIANT SECURE SYSTEM

The Neptune system has a GDPR (Global Data Protection Rule) compliant infrastructure. Neptune system infrastructure ensures the security of your company's virtual machines with its proactive security technologies against current cyber-attacks and its expert professional team. All your data hosted on your virtual machines is protected under GDPR.

BRING YOUR OWN DEVICE

Employees can use their personal devices to connect to secure desktop sessions that contain the applications necessary for them to get their work done.

EASY MANAGEMENT

Thanks to Neptune, you can easily perform any hardware or software update or change (processor power increase, RAM increase, Disk space upgrade, etc.)

OUR TRAININGS

SnipeSec aims to raise public awareness about information technology and cybersecurity through various training programs and courses, contributing to the development of a safer and more informed digital society.

BASIC TRAININGS

We provide basic trainings in various fields such as IT laws and regularions, network, security, cryptology, and operating systems

DATABASE TRAININGS

Database trainings are designed to give proficient knowledge about databases such as NoSQL Oracle

SECURTIY TRAININGS

These trainings will help you gain in-depth knowledge about security. It covers all the aspects of cyber security i.e. Penetration testing, analysis of cyber attacks and more.

WEB TRAININGS

Web trainings include FrontEnd and BackEnd, working with API, Web security and everything you need to know in order to become a Web developer or enhance your skills.

VIRTUALIZATION

Nowadays virtual reality is becoming more and more popular. That is why we offer trainings in Kubernetes, Backup and Virtualization in general.

MOBILE TRAININGS

These trainings include all the needed information in order to become a mobile app developer such as mobile app development in IOS, Android, and its security.

Why snipesec is the best cyber security company for your business?

- ☑ Snipesec is an international organization that has branches in Turkey, Cyprus, and Estonia which are successfully operating and providing high- quality services to its customers.
- ☑ Snipesec has over 10 years of experience in the IT industry providing high-quality services
- ☑ Snipsec introduced the new Remote Desktop Service Neptune. It is an innovation in the market which helps start-ups, businesses and other organizations work remotely as if they are in one office.
- ☑ Snipsec has ISO 9001:2015 (Quality Management System standards), ISO 27001:2013 (Security Management System standards), and General Data Protection Rule (GDPR) accreditation. Meaning that the company meets all the standards of quality.
- ☑ All the employees undergo continuous training in order to keep updated about new types of threads and learn new methods of cybersecurity.
- ☑ When working with Snipesec you will be provided with weekly, and monthly reports so you will be informed about all the operations that are being conducted.
- ☑ Snipesec works with small-scale companies as well as with large-scale companies. Regardless of the size of your enterprise, you will find corresponding services that will satisfy the needs of your company.
- ☑ We work only with legitimate companies in providing the services listed above. We do not conduct unethical operations under any circumstances.
- ☑ All the employees of the company are highly trained certified professionals who love challenges and are driven by results.

REFERENCES

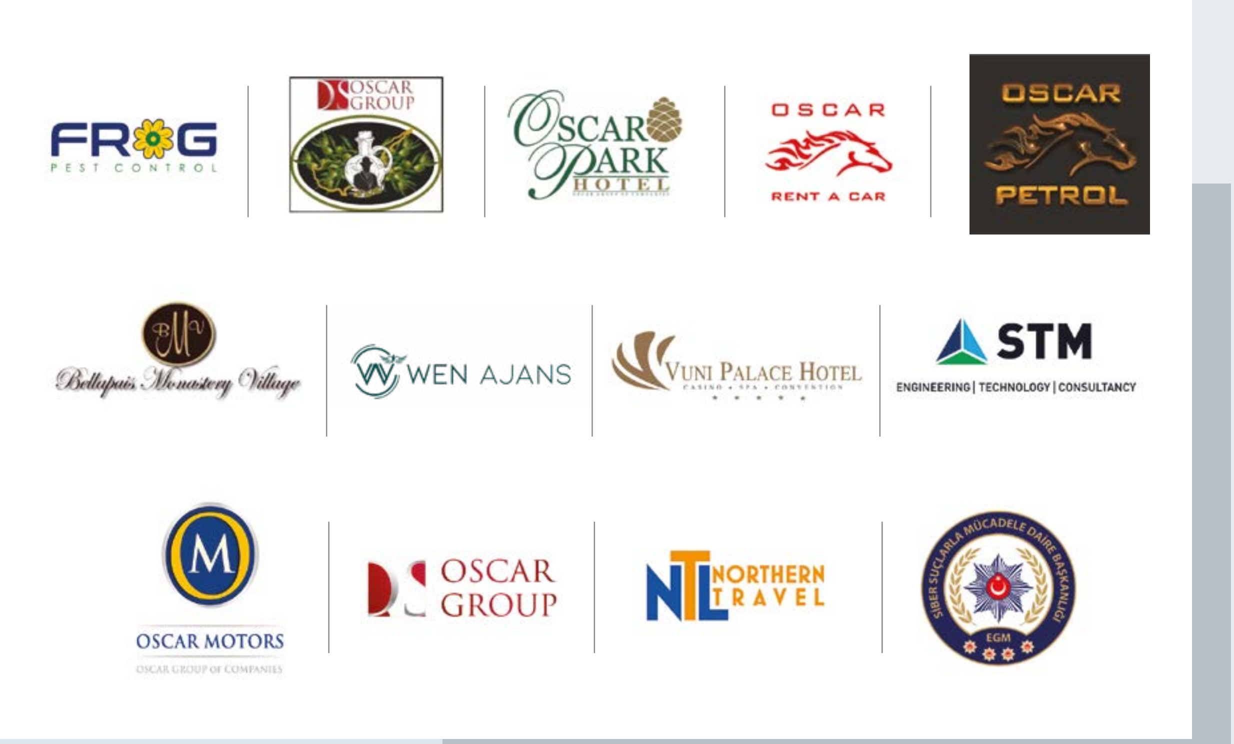
We aim to deliver results and every client should be our best case

Nowadays not digitalizing your business simply means not evolving. Our mission is to help enterprises grow in a digital world and ensure their security and safety. Every customer is a unique case whom we approach individually. However, we show the same level of concern to each and every one of them.

The most important thing for us is to immediately respond to any kind of incident. Whenever something occurs in any place at any time we take action straightaway, because we realize that every minute when there is an issue in the system equals a loss for a company.

We cannot afford for our clients to freeze their functioning and lose any profit due to technical issues.

That is why no matter the time of the day and day of the year we are always alert.



PARTNERS

COMODO SSLCERTIFICATE

eset

Microsoft Solutions Partner

RUCKUS COMMSCOPE REGISTERED SOLUTION PROVIDER

veeAM

ACCREDITATIONS

Snipesec
CYBER SECURITY AGENCY

The first and only
Accredited IT and Cyber Security Company
in Northern Cyprus

International Organization for Standardization
ISO
9001:2015
Kalite Yönetim Sistemi

International Organization for Standardization
ISO
27001:2013
Bilgi Güvenliği

TSE-HYB

TI
TF-CSIRT
Trusted
Introducer

www.**snipesec**.com

Snipesec
CYBER SECURITY AGENCY

DETECT DEFEND SECURE

TURKEY OFFICE
Eti Mahallesi Gazi Mustafa Kemal Bulvarı No 94/8 Çankaya, Ankara, Türkiye

CYPRUS OFFICE
Şht. Mehmet Bayram Yaşar Sokak No:3/A , Yenişehir, Lefkoşa, Kuzey Kıbrıs.

✉ info@snipesec.com | ☎ +90 (850) 303 27 04

www.**snipesec**.com