Services Datasheet

Table Of Contents

Services at a Glance

At Guardanet we provide information security services that help examine, improve and maintain your organization's security posture. These services include:

- Reconnaissance
- Vulnerability Assessment
- Penetration Testing

In addition to these Guardanet also offers Consulting Services, such as:

- General Data Protection Regulation (GDPR) Tune-Up
- Virtual Chief Information Security Officer (CISO)
- Network / Security Architecture consulting

See the below charts to understand which services are best suited to your particular case as well as what business drivers' requirements you can meet with them

	Consulting	Reconnaissance	Vulnerability Assessment	Penetration Test
I created a service / application and need a reliable platform to run it from	✓			
I need a security consultant to come in and secure my existing infrastructure	✓			
What information is publicly available about me?		✓		
What are my weaknesses?			✓	
Can my infrastructure be compromised by an external threat				✓
Am I well protected from internal attacks / sabotage?				✓
Is my cloud-based web service secure?				✓
Is my employee security awareness program effective?				✓

Consulting	Reconnaissance	Vulnerability Assessment	Penetration Testing
I am building a new solution and security needs to be part of it from day one.	Protect critical business data and intellectual property (Data Leak Prevention)	Vulnerability and Patch Management Program verification	Validation of existing security controls
I need someone to secure my existing infrastructure	Brand Image / Reputation Protection	Compliance requirements (GDPR, PCI-DSS, HIPAA, FISMA)	Compliance requirements (GDPR, PCI-DSS, HIPAA, FISMA)
I need guidance on implementing a specific security solution (ex. Secure remote access for my employees/partners/ customers)		Information security continuous monitoring (ISCM)	Information security continuous monitoring (ISCM)
I need to implement security controls to meet compliance requirements (GDPR, PCI-DSS, HIPAA, FISMA)			Improve employee security awareness as part of your Enterprise-wide Awareness Program

Reconnaissance

Guardanet's reconnaissance services include researching your organization's Internet footprint, monitoring its resources, people, and processes, scanning for network information such as IP addresses and systems types and social engineering public services such as help desk. Reconnaissance can reveal information such as:

- Your company's background and business focus
- Your company's partners, customers and vendors
- Your company's people
- Your company's network
- Your company's defenses
- Your company's technologies

Our reconnaissance methodology consists of two areas, namely: Passive Reconnaissance and Active Reconnaissance.

Passive reconnaissance includes:

- Open-source intelligence (OSINT) - intelligence produced from publicly available information
- DNS reconnaissance and route mapping
- Obtaining user information
- Profiling users for password lists
- Metadata gathering and analysis

Active reconnaissance builds on the results of open-source intelligence and passive reconnaissance, and aims to identify the exposed attack surface of the target. We achieve it through:

- Stealth scanning techniques
- Identifying devices and running services
- Identifying previously compromised or leaked information

Vulnerability Assessment

Guardanet's vulnerability assessment program employs a myriad of automated processes and applications as well as manual testing and analysis to identify vulnerabilities in target's IT infrastructure that may be exploitable.

The customer can choose between internal and external vulnerability assessment.

- The internal vulnerability assessment reveals target's security posture from the perspective of its employees, contractors, visitors and others who have physical access to target's premises.
- The external vulnerability assessment is conducted from outside the organization's security perimeter. This offers the ability to view the environment's external security posture with the goal of revealing weaknesses that could be exploited by an external threat.

The outcome of this process is a detailed report including all systems scanned together with identified vulnerabilities, their corresponding CVE ids and severities as well as Guardanet's mitigation recommendation. Guardanet's vulnerability reports help you decide on risk management strategy and safeguard selection based on your business strategy and safeguard ROI calculations.

Penetration Testing

Guardanet's Penetration Tests attempt to attack vulnerabilities, identified during the Guardanet's Vulnerability Assessment process, emulating typical attackers' activities in order to verify which vulnerabilities are genuine and to reduce the real list of found vulnerabilities to a handful of security weaknesses. In our penetration testing methodology we leverage various existing standards and guidelines, such as:

- Penetration Testing Execution Standard (PTES),
- Open Source Security Testing Methodology Manual (OSSTMM),
- National Institute of Standards and Technology Special Publication NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment,
- Open Web Application Security Project (OWASP) and
- Payment Card Industry Data Security Standard (PCI-DSS).

Depending on your needs you choose from the following range of Guardanet's penetration testing services:

- Network Penetration Testing
- Web Application Penetration Testing
- Wireless Penetration Testing
- Social Engineering Penetration Testing

Network Penetration Testing

This type of penetration testing is best suited for organizations that own their IT infrastructure and want to increase awareness of security issues related to it. Guardanet offers two types of Network Penetration Tests, namely External and Internal.

In the **External Network Penetration Test** we test the following elements from outside the perimeter of your infrastructure:

- Firewalls, IDS/IPS
- Target's Website, web servers (HTTP/HTTPS) and other available public facing services such as: Email, DNS and proprietary services
- VPNs
- Remote administration interfaces (Web, RDP, etc.)
- External network equipment

In the **Internal Network Penetration Test** our testing is conducted from within your premises and covers elements such as:

- Firewalls, IDS/IPS
- Routers and Switches
- Servers and Workstations
- VOIP equipment
- Printers, Scanners, Fax, etc.

Web Application Penetration Testing

Web applications are omnipresent and are de-facto standard for internet-based applications nowadays. Be it for an organization's use or as a consumer product/service they often consist of multiple tiers (web servers, application servers, databases, etc.) and interface with a large variety of devices ranging from workstations, remotely connected portable computers to smartphones, tablets or even IoT devices. We take all of these factors into consideration while defining a scope of every Web Application Penetration Test.

The central objective of Guardanet's Web Application Penetration Testing is to exploit the inherent security weaknesses of the network perimeter, web domain, and web application delivery. Adjacent application delivery elements, such as backend databases and middleware, are evaluated as well.

Wireless Penetration Testing

As an organization that owns a wireless infrastructure you are certainly aware of its related security concerns among which access control, confidentiality, availability and rogue infrastructure abuse are the most predominant. Guardanet meets these challenges with its Wireless Penetration Testing program to identify and verify present weaknesses in order to help you tighten your WLAN infrastructure security controls.

Social Engineering Penetration Testing

As humans always present the biggest challenge in your organization's overall security posture, social engineering attacks have become the most popular attack vector that an organization should be aware of and prepared for.

Guardanet Social Engineering Penetration Test uses a combination of human and electronic methodologies to manipulate your personnel into performing actions of divulging proprietary information or granting access/rights to unauthorized individuals.

Guardanet's Social Engineering Penetration Test is a great way to validate the adoption level of your security policy and an integral part of your security policy development life cycle.

Consulting

Guardanet also provides consulting services to those organizations that do not have in-house information security expertise and require guidance and help in securing their existing infrastructure or in building a new secure environment from scratch. We can help you:

- Create a sound security program consisting of policies, standards, procedures and guidelines
- Ensure a robust Disaster Recovery Plan and Backup solution are in place
- Create security baselines and recommend suitable security controls,
- Design and build a secure in-house or cloud-based infrastructure,
- Secure your existing footprint
- Implement secure authentication mechanisms (Multi Factor Authentication, Biometrics, One Time Passwords, Tokens)
- Implement an identity management system (LDAP, Single Sign On)
- Design secure remote access for your employees
- Apply best practices pertaining to WLAN implementations
- Put into place a program to oversee security of mobile devices in your enterprise

GDPR Tune-Up

The General Data Protection Regulation (GDPR) replaces the European Data Protection Directive 95/46/EC [82] and is the new data protection regulation that shall apply from May the 25th of 2018 directly in every EU Member State without the need for national legislation.

Whether you collect data from EU residents (Data Controller) or process EU resident data on behalf of those who collected it (Data Processor) and regardless of your business being EU based or not, you are subject to the new GDPR regulation.

At Guardanet we created a program that helps you prepare for the new data protection regulation. Our program starts with a GDPR Assessment that is essentially a gap analysis between where your organization is at the moment and where it needs to be to meet the regulation's requirements.
The results of the assessment process feed directly into a detailed preparation plan where new policies, standards and procedures are created or existing ones modified in order to achieve GDPR compliance.
Our preparation process addresses all the new key elements of the GDPR regulation, such as: accountability and governance, individuals' rights, privacy notices and consents, processing of children data, data breach detection and notification procedures and Data Protection By Design that introduces measure such as pseudonymisation of user data.

At Guardanet we can also help carry out Data Protection Impact Assessments (DPIAs) that according to the new regulation are required in situations where data processing is likely to result in high risk to individuals.

Virtual CISO

Guardanet offers the virtual Chief Information Security Officer (CISO) service to companies that do not have a full-time chief information security officer on board and look for guidance in designing and implementing a sound and robust information security program.

Our virtual CISO provides the following benefits to your organization:

COST SAVINGS

You will get a CISO for a fraction of the expense of an on board full-time CISO

SUBJECT MATTER EXPERT

You will be working with an ISC2 Certified Information Systems Security Professional (CISSP) who possesses a strong balance of business acumen and technology knowledge

TIME SAVINGS

Take advantage of the virtual CISO immediately without needing to spend 6 months looking for someone qualified

KNOWLEDGE GAIN

Your internal staff will gain expertise from working with the virtual CISO, which you will benefit from upon the completion of the engagement

PEACE OF MIND

You can focus on your core business while the virtual CISO takes care of your information security management system

Guardanet's virtual CISO objectives may include but not be limited to:

Security Governance
Creating / modifying Policies, Standards, Procedures and Guidelines

Compliance, Laws and Regulations

Risk Management

Personnel Security

Business Continuity Planning

Identity and Access Management

Security Assessment and Testing
Vulnerability Assessment and Penetration Testing
Information Security Continuous Monitoring (ISCM)

Security Operations
Investigations, Computer Forensics
Incident Response Management, Computer incident response teams (CIRTs)
Security Information and Event Management (SIEM)
Data leak prevention (DLP)
Disaster Recovery Planning

Why Guardanet?

Guardanet is a worldwide company, registered in Poland, which provides information security services to customers in the European Union as well as in the United States of America. We currently operate out of Portugal, Poland and the United States of America

Krzysztof Waberski, the founder and CEO of Guardanet, has 13 years of industry experience in the areas of information and network security as well as technical pre-sales. He designed and implemented two mission-critical computer data centers based in Silicon Valley, California, delivering e-commerce and ASP-like services meeting 99.99% availability figures. He also worked with most major mobile operators in Europe and in the United States.

Throughout his career he has taken on the role of a systems and network engineer, lead security and network architect and a technical account manager. He holds a MS degree in CS (major: Corporate Networks Security). He also received ISC2's Certified Information System's Security Professional (CISSP) certification (ID: 525907).

CISSP®
Certified Information Systems Security Professional