ISSP

Vulnerability Management

A managed security service provided by ISSP SOC, designed to address the information security vulnerability at the IT system of an organization.

Vulnerability Management functions through periodic scanning of network assets and end-user workstations to identify known vulnerabilities in network services, operating systems, or web applications.

TYPES OF SCANNING

The service can encompass all of the organization's network assets, including the external perimeter, internal corporate networks, and distributed assets such as remote employee workstations.

The frequency and types of scans are determined based on the criticality of assets or specific network segments.

Scanning of external (public) services and applications via the Internet.

Scanning of the internal corporate network's perimeter through an internally deployed scanning module.

Scanning of remote workstations or servers through a deployed scanning agent.

SOLUTIONS

Infrastructure Security

Everything you need for onpremises data center security: asset inventory, passive and active scanning, vulnerability management and more.

Web App Security

It's never been easier for employees to bypass IT and install unsafe web apps. ISSP continually detects all your web apps – approved and unapproved – and provides continuous protection.

Compliance

You enforce compliance with complex internal policies, industry mandates and external regulations, and assess vendor risk. ISSP gives you the clarity, control and flexibility to keep your company compliant.

Endpoint Security

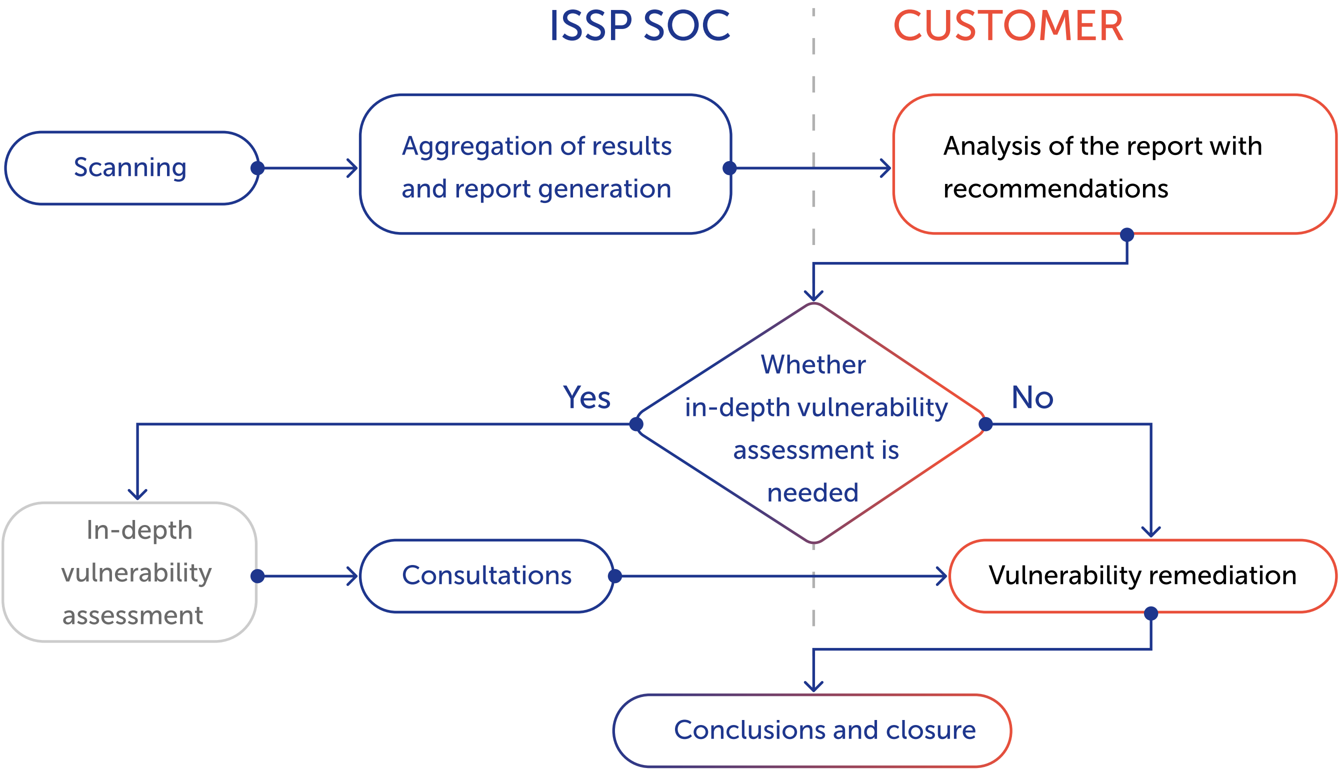
The variety and quantity of endpoints on your network continue to rise, and so do security and compliance risks. With ISSP, you'll continuously discover, track and protect PCs, laptops, IoT devices, smartphones, peripherals and other endpoints.

DevSecOps

ISSP puts security into your DevOps environment, automating the detection of coding and configuration errors in your iterative, collaborative software development lifecycle, prioritizing vulnerability remediation, shielding web apps and flagging hacker intrusions.

Cloud Infrastructure Security

You must secure the workloads being shifted to public clouds. With native AWS, Azure and GCP integrations, ISSP gives you instant visibility into these instances and full security and compliance control.



ISSP SOC
CUSTOMER
Scanning
Aggregation of results and report generation
Analysis of the report with recommendations
Whether in-depth vulnerability assessment is needed
Yes
No
In-depth vulnerability assessment
Consultations
Vulnerability remediation
Conclusions and closure

VULNERABILITY MANAGEMENT SERVICE FEATURES

Discover forgotten devices and organize your host assets

You can quickly determine what's actually running in different parts of your network—from your perimeter and corporate network to virtualized machines and cloud services. Uncover unexpected access points, web servers and other devices that can leave your network open to attack.

- Visually map your network
- Prioritize your remediation by assigning a business impact to each asset
- Identify which OS, ports, services and certificates are on each device on your network
- Control which hosts can be scanned by which users
- Continuously monitor your perimeter for unexpected changes

Scan for vulnerabilities everywhere, accurately and efficiently

Scan systems anywhere from the same console: your perimeter, your internal network, and cloud environments. You can scan deeply and then create custom reports.

- Select target hosts by IP address, asset group or asset tag
- Scan manually, on a schedule, or continuously
- Scan complex internal networks, even with overlapping private IP address spaces
- Securely use authentication credentials to log in to each host, database or web server
- Store configuration information offsite with secure audit trails

Remediate vulnerabilities

Ability to track vulnerability data across hosts and time lets you use reports interactively to better understand the security of your network. Use a library of built-in reports, change what's shown or choose different sets of assets — all without having to rescan.

- Automatically generate and assign remediation tickets whenever vulnerabilities are found
- Get consolidated reports of which hosts need which patches
- Integrate with third party IT ticketing systems
- Manage exceptions when a vulnerability might be riskier to fix than to leave alone

Identify and prioritize risks

You can identify the highest business risks using trend analysis, ZeroDay and Patch impact predictions.

- Track vulnerabilities over time: as they appear, are fixed, or reappear
- Monitor certificates deployed throughout your network—see what's about to expire, which hosts they are used on, what their key size is, and whether or not they are associated with any vulnerabilities
- See which hosts need updates
- Examine your network's vulnerabilities over time, at different levels of detail

1 hour

Time it takes for our SOC team to respond to a high-priority case assigned

99.9%

Vulnerability Management Platform availability

KEY BENEFITS OF VULNERABILITY MANAGEMENT SERVICE

Customizable Coverage

Tailor the scanning to fit your needs, from selective external scans to a comprehensive examination of your entire infrastructure, both inside and out.

Comprehensive Toolkit

Access all the necessary tools and resources, including the expertise of qualified professionals, for an effective vulnerability search process within your organization.

Targeted Vulnerability Focus

Concentrate your efforts on the most vulnerable areas within your organization's network.

Expert Consultation

Benefit from expert guidance and support in configuring scans and interpreting results.

Flexible Scanning Options

Easily choose scanning options, such as system load, scheduling, and setting limitations, to align with your preferences.

Personalized Scanning Policies

Receive scanning policies that are customized to your unique infrastructure and security requirements.

Tailored Reports

Receive reports that contain the specific information you require.

On-Demand Scans

The flexibility to conduct unscheduled scans as needed.

Support for Challenging Devices

For devices that are difficult to scan, like remote users and distributed offices, specialized agents can be installed to collect vital data on the operating system, installed applications, registry sections, processes, and system configurations.

Resource and Time Savings

Realize cost and time savings for your organization, making it an efficient and cost-effective choice.