



# PRODUCT CATALOG

## SNAPSEC



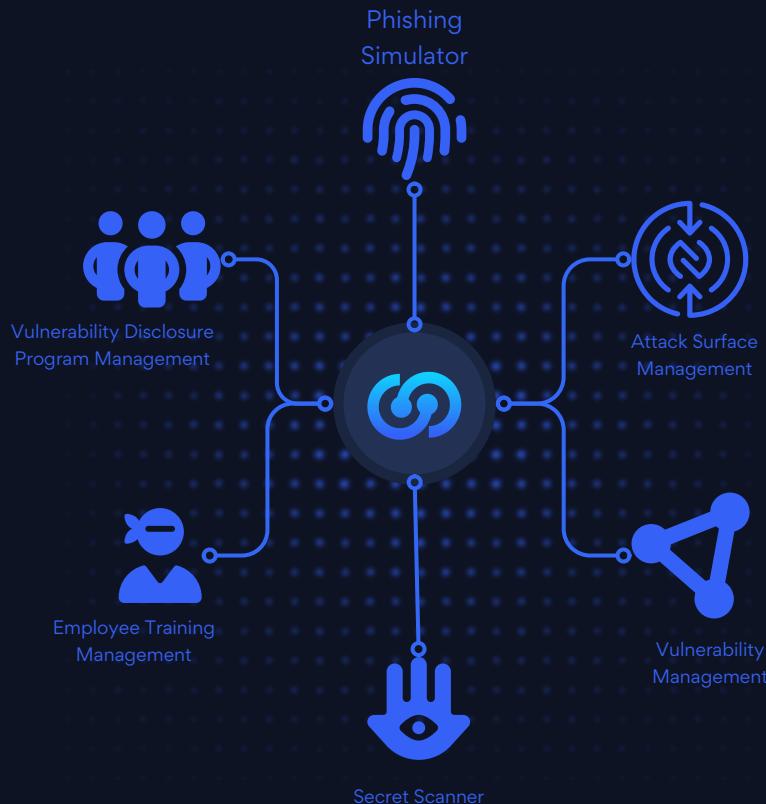
The image displays a composite screenshot of the Snapsec product catalog, showcasing several key features:

- Organization Overview:** A dashboard showing 170 findings, 78 in progress, 11 un-reviewed, 56 resolved, 02 pending review, and 31 false positives. It includes a bar chart for severity classification and a list of top 5 vulnerabilities.
- Upcoming Assessments:** A section listing two assessments: "Assessment 1" (Not Scheduled, Not Configured, Gray Box, 4 members) and "Assessment 2" (Not Scheduled, Not Configured, Gray Box, 3 members).
- Phishing Simulator:** A feature for generating phishing campaigns to educate users about online security threats. It includes sections for "Generating Phishing Everywhere", "Interactive Phishing Simulation", and "Pre-built Templates".
- Codebase:** A dashboard for managing social engineering attacks, showing a course titled "Social Engineering Attacks" created by "Invan Pency". It includes sections for "Phishing Simulation", "Cyber Attacks", "SSL Security and API Config", and "Insecure Santa Hacker".
- VDP (Vulnerability Data Platform):** A detailed dashboard showing 123 findings across three categories (123 Active, 123 In Progress, 123 Resolved). It includes a "Severity Classification" section with a donut chart and bar chart, and a "Top 50 Vulnerabilities" table.
- Highest Critical Reputation:** A table listing users with their highest critical reputation scores, such as "User 1" (2334), "User 2" (12), "User 3" (4545), etc.

# SNAPSEC SUITE

Our suite brings together six powerful products into one centralized platform, providing a unified approach to securing your digital environment. These products include Attack Surface Management, Vulnerability Management, Phishing Simulation, Secret Management, VDP Management, and Employee Training Management.

By centralizing these tools, we streamline your cybersecurity operations, making it easier to monitor and manage all aspects of your security. Additionally, our suite achieves advanced correlation of the data collected, offering deeper insights and a more robust defense against threats.



## CORE VALUES OF SOLUTION

### Centralization

Our platform unifies multiple cybersecurity tools into a single, centralized solution for easier management.

### Co-Relation

We correlate data from various tools to provide deeper insights and more effective threat detection.

## OUR PRODUCTS



# ATTACK SURFACE MANAGEMENT

ASM is a valuable solution for any organisation that wants to improve its security posture and protect itself from cyber threats. By continuously identifying and remediating vulnerabilities, ASM can help organisations to reduce their attack surface and prevent attackers from exploiting vulnerabilities to gain access to their systems and data.

## KEY FEATURES

### Key Benefits of Our Attack Surface Management

#### Continuous Vulnerability Scanning

Regular scans to identify and address security weaknesses across your digital assets, ensuring your infrastructure remains secure against potential threats.

#### Data Breach Protection

Proactive Scanning against online data-beaches to safeguard sensitive information, minimizing the risk of data breaches.

#### Enhanced Visibility

Real-time monitoring and insights into your exposed infrastructure, helping you quickly identify and mitigate risks.

#### AI-Powered Report Writing

Automated generation of detailed security reports using artificial intelligence, delivering actionable insights and saving time on manual documentation.

#### Comprehensive Asset Catalog

An organized inventory of all digital assets, providing a clear overview and enabling efficient management and security of your resources.

#### 360 Approach

Run comprehensive scans identify issues across domains, personnel, data breaches, leaks, and more, ensuring thorough protection from all angles.

TRY DEMO

## OUR PRODUCTS



# VULNERABILITY MANAGEMENT

SnapSec's Continuous Security Management System provides a simple and intuitive solution for effective vulnerability management. With our platform, you can easily identify, track, and resolve vulnerabilities within your organization's digital infrastructure.

## KEY BENEFITS

Key Benefits of Our Vulnerability management

<b>Centralized Screen for All Reports</b>	Provides a unified dashboard for easy access and management of all vulnerability reports generated from multiple assessments	<b>Customized PDF Report Pентest Generation</b>	Enables you to create tailored PDF reports at any time for comprehensive documentation and sharing.
<b>Automatic Prioritization</b>	Automatically classification of vulnerabilities based on risk, allowing you to focus on the most critical threats first.	<b>Team Collaboration</b>	Facilitates collaboration by inviting your entire team, assign tasks, track blockers, add comment for coordination.
<b>Overview of All Assessments</b>	Offers a holistic view of all your security assessments, helping you track progress and identify areas needing attention.	<b>Remediation Tracking</b>	Monitors the progress of vulnerability remediation efforts, ensuring timely resolution of identified issues.

[TRY DEMO](#)

## OUR PRODUCTS



The screenshot shows a dark-themed LMS interface. At the top, there's a navigation bar with icons for 'Code base', 'ASW', and a user profile for 'Sheena Smith'. Below the navigation is a course card for 'Social Engineering Attacks'. The card includes a star rating of 4.5 out of 5 from 1765125 employees, created by 'Imran Paray' last updated on 'Imran Paray', in English, with a duration of '24 Minutes'. There are two buttons at the bottom of the card: 'Enroll' and 'Take Assessment'. To the right of the card is a decorative graphic of a digital lock inside a hexagonal network of lines and dots. Below the main card, there are four smaller thumbnail images with titles: 'Phishing Simulation Cyber Attacks', 'SSL Security and API Config', 'Imran the Sasta Hacker', and 'Cyber Business Boom in India'. Each thumbnail has a brief description below it.

# EMPLOYEE TRAINING MANAGEMENT

Our employee training management solution offers a comprehensive platform for security training. It provides a centralized view of employees' security scores, allowing administrators to track progress and identify areas for improvement easily. With customizable course assignment capabilities, admins can assign relevant security courses to employees based on their roles and responsibilities. This ensures that employees receive targeted training to enhance their cybersecurity awareness and skills.

## KEY BENEFITS

Key Benefits of Our Employee training management

### Access to the Latest Cybersecurity Courses

Employees can stay updated with the newest cybersecurity practices through regularly updated courses.

### Employee Leaderboard

Tracks and displays employee scores, fostering a competitive and engaging learning environment.

### Auto Course Assignment

Automatically assigns relevant courses to employees compromised in phishing simulations or if their email is leaked online.

### Assessment Tests

Provides comprehensive assessments to evaluate employee understanding and retention of course material.

### Manual Course Assignment

Allows administrators to assign specific courses to employees based on their roles or needs.

### Admin Progress Tracking

Enables administrators to monitor and track the training progress of all employees.

[TRY DEMO](#)

## OUR PRODUCTS



The screenshot shows the SnapSec Phishing Simulator interface. At the top, there's a navigation bar with icons for Home, Products, Services, Support, and Contact. The main header reads "Phishing Simulator" and "No Human Errors with the Phishing Simulator". Below the header, a sub-header says "Deploy simulated phishing to educate users, mimicking real-world scenarios for staff readiness, enhancing awareness about online security threats in organizations." There are three main sections: "Empowering Protection Everywhere.", "Interactive Phishing simulation", and "Pre-built Templates". Each section has a brief description and a button: "Create A Campaign", "Create A Contact", and "Make Your Plan". Below these sections, there's a table titled "300 Total Contacts" with three rows of data: Imran Paray, Faheem Hussain, and Mubashir Ahmed, each with an "Edit" and "Delete" icon. A "View All" button is at the top right of the contacts table. Below the contacts is a section titled "Recent Campaigns" with three entries: "#1 Attack on titan successful", "#2 Software Upload Failed", and "#3 MubbPorrauy died", each with an "Email" and "Success" status indicator and a timestamp.

## PHISHING SIMULATOR

SnapSec Phishing Simulator is a sophisticated tool designed to help organizations assess and improve their resilience against phishing attacks. It offers a range of features such as creating realistic phishing email templates, launching simulated phishing campaigns, and tracking employee responses. With SnapSec Phishing Simulator, organizations can identify vulnerabilities in their workforce's awareness and behavior related to phishing attacks. This tool allows for targeted training interventions, helping employees recognize and avoid falling victim to real phishing threats, ultimately enhancing the overall cybersecurity posture of the organization.

## KEY BENEFITS

### Key Benefits of Our Phishing Simulator System

#### Real-World Training

Provides employees with hands-on experience in identifying and responding to phishing attempts, enhancing their awareness and skills.

#### Behavioral Insights

Tracks and analyzes employee responses to phishing simulations, providing valuable insights into overall security awareness and areas for improvement.

#### Pre Build Phishing Templates

Pre-built SaaS templates not only enhance phishing simulations but also make them more realistic.

#### Phishing Attempt Reporting Portal

A dedicated portal where employees can report suspected phishing emails to admins, who can then review and mark these emails as either phishing or safe.

#### Contact Categorization

Customized phishing campaigns target departments and roles effectively, improving training relevance and impact.

#### Training Portal Integration

Automatically assigns courses based on user activity, streamlining the learning process and ensuring relevant content delivery.

TRY DEMO

## OUR PRODUCTS



The screenshot shows a dark-themed dashboard titled "Code base". On the left is a sidebar with various icons. The main area displays eight user profiles in a grid. Each profile card includes a user photo, the name, GitHub Repos count, and Leaks count. A button at the top right says "+ Import Github Profiles".

User	Github Repos	Leaks
Hannah North	1235	15
Danny Canson	123	0
Cari Johnson	0	0
Kissa Sins	5565	45
Ashwariya Rai	15	15
Imran Kamzmi Paki	15	15
Miana Erwin	15	15
Ching Mong Lee	15	15

## SECRET SCANNER

SnapSec Phishing Simulator is a sophisticated tool designed to help organizations assess and improve their resilience against phishing attacks. It offers a range of features such as creating realistic phishing email templates, launching simulated phishing campaigns, and tracking employee responses. With SnapSec Phishing Simulator, organizations can identify vulnerabilities in their workforce's awareness and behavior related to phishing attacks. This tool allows for targeted training interventions, helping employees recognize and avoid falling victim to real phishing threats, ultimately enhancing the overall cybersecurity posture of the organization.

## KEY BENEFITS

Key Benefits of Our Secret SCanner

### Extensive Token Scanning

Employs advanced algorithms to scan for over 4000 types of secret tokens, ensuring thorough detection of potential security breaches.

### Comprehensive Integration

Seamlessly integrates with over 300 SaaS platforms including GitHub, Slack, and more, providing extensive coverage for detecting secret leaks.

### Centralized Dashboard

Presents identified leaks on a centralized dashboard, providing clear visibility and easy management of security risks.

### AI-Powered Reporting

Automatically generates detailed reports for using artificial intelligence

### Integration with Vulnerability Management

Integrates with our vulnerability management tool, enabling seamless transfer of findings for prioritized remediation.

### Scheduling and Quick Scans

Offers scheduling options for regular scans and quick scan capabilities.

[TRY DEMO](#)

## OUR PRODUCTS



## VULNERABILITY DISCLOSURE PROGRAM MANAGEMENT

Our solution is a comprehensive Vulnerability Disclosure Program Management platform. It offers structured guidelines and channels for external parties to report potential security vulnerabilities. With intuitive reporting mechanisms and clear communication channels, it ensures that vulnerabilities are efficiently directed to the appropriate teams for prompt resolution. By facilitating smooth communication and collaboration between finders and internal teams, our solution helps organizations effectively manage and mitigate security risks identified by external sources.

## KEY BENEFITS

### Key Benefits of Our Vulnerability Disclosure Program Management

#### Policy Definer

Customizable policies for defining scope, assets, rewards, and more, ensuring clear and consistent guidelines for reporting and managing vulnerabilities.

#### Streamlined Communication

Directly communicate from platform with individuals who submit bugs via email.

#### Leaderboard for Reporters

Customised company leaderboard which motivates and recognises external parties by ranking their contributions.

#### Efficient Triage and Prioritization

With structured reporting mechanisms, our solution helps organizations prioritize and address vulnerabilities based on their severity and impact.

#### Improved Collaboration

By fostering collaboration between finders and internal teams, our solution promotes a proactive approach to vulnerability management.

#### Community Engagement

We actively engage with the bug bounty community and can attract researchers to your program based on your specific needs.

TRY DEMO

# OUR PRODUCTS



## KEY BENEFITS

### Key Benefits of Our Snapsec Suite

<b>Continuous Vulnerability Scanning</b>	Regular scans to identify and address security weaknesses across your digital assets, ensuring your infrastructure remains secure against potential threats.	<b>Data Breach Protection</b>	Proactive Scanning against online data-beaches to safeguard sensitive information, minimizing the risk of data breaches.	<b>Centralized Screen for All Reports</b>	Provides a unified dashboard for easy access and management of all vulnerability reports generated from multiple assessments.
<b>Enhanced Visibility</b>	Real-time monitoring and insights into your exposed infrastructure, helping you quickly identify and mitigate risks.	<b>AI-Powered Report Writing</b>	Automated generation of detailed security reports using artificial intelligence, delivering actionable insights and saving time on manual documentation.	<b>Automatic Prioritization</b>	Automatically classification of vulnerabilities based on risk, allowing you to focus on the most critical threats first.
<b>Comprehensive Asset Catalog</b>	An organized inventory of all digital assets, providing a clear overview and enabling efficient management and security of your resources.	<b>360 Approach</b>	Run comprehensive scans identify issues across domains, personnel, data breaches, leaks, and more, ensuring thorough protection from all angles.	<b>Overview of All Assessments</b>	Offers a holistic view of all your security assessments, helping you track progress and identify areas needing attention.
<b>Customized PDF Report Ptest Generation</b>	Enables you to create tailored PDF reports at any time for comprehensive documentation and sharing.	<b>Access to the Latest Cybersecurity Courses</b>	Employees can stay updated with the newest cybersecurity practices through regularly updated courses.	<b>Employee Leaderboard</b>	Tracks and displays employee scores, fostering a competitive and engaging learning environment.
<b>Team Collaboration</b>	Facilitates collaboration by inviting your entire team, assign tasks, track blockers, add comment for coordination.	<b>Auto Course Assignment</b>	Automatically assigns relevant courses to employees compromised in phishing simulations or if their email is leaked online.	<b>Assessment Tests</b>	Provides comprehensive assessments to evaluate employee understanding and retention of course material.
<b>Remediation Tracking</b>	Monitors the progress of vulnerability remediation efforts, ensuring timely resolution of identified issues.	<b>Manual Course Assignment</b>	Allows administrators to assign specific courses to employees based on their roles or needs.	<b>Admin Progress Tracking</b>	Enables administrators to monitor and track the training progress of all employees.
<b>Real-World Training</b>	Provides employees with hands-on experience in identifying and responding to phishing attempts, enhancing their awareness and skills.	<b>Behavioral Insights</b>	Tracks and analyzes employee responses to phishing simulations, providing valuable insights into overall security awareness and areas for improvement.	<b>Comprehensive Integration</b>	Seamlessly integrates with over 300 SaaS platforms including GitHub, Slack, and more, providing extensive coverage for detecting secret leaks.
<b>Pre Build Phishing Templates</b>	Pre-built SaaS templates not only enhance phishing simulations but also make them more realistic.	<b>Phishing Attempt Reporting Portal</b>	A dedicated portal where employees can report suspected phishing emails to admins, who can then review and mark these emails as either phishing or safe.	<b>AI-Powered Reporting</b>	Automatically generates detailed reports for using artificial intelligence
<b>Contact Categorization</b>	Customized phishing campaigns target departments and roles effectively, improving training relevance and impact.	<b>Training Portal Integration</b>	Automatically assigns courses based on user activity, streamlining the learning process and ensuring relevant content delivery.	<b>Scheduling and Quick Scans</b>	Offers scheduling options for regular scans and quick scan capabilities.
<b>Extensive Token Scanning</b>	Employs advanced algorithms to scan for over 4000 types of secret tokens, ensuring thorough detection of potential security breaches.	<b>Policy Definer</b>	Customizable policies for defining scope, assets, rewards, and more, ensuring clear and consistent guidelines for reporting and managing vulnerabilities.	<b>Streamlined Communication</b>	Directly communicate from platform with individuals who submit bugs via email.
<b>Centralized Dashboard</b>	Presents identified leaks on a centralized dashboard, providing clear visibility and easy management of security risks.	<b>Leaderboard for Reporters</b>	Customised company leaderboard which Motivates and recognises external parties by ranking their contributions	<b>Efficient Triage and Prioritization</b>	With structured reporting mechanisms, our solution helps organizations prioritize and address vulnerabilities based on their severity and impact.
<b>Integration with Vulnerability Management</b>	Integrates with our vulnerability management tool, enabling seamless transfer of findings for prioritized remediation.	<b>Improved Collaboration</b>	By fostering collaboration between finders and internal teams, our solution promotes a proactive approach to vulnerability management	<b>Community Engagement</b>	We actively engage with the bug bounty community and can attract researchers to your program based on your specific needs.

TRY DEMO

CONTACT US



# GET IN TOUCH

SNAPSEC



[SCHEDULE A DEMO](#)



+917780908136



[support@snapsec.co](mailto:support@snapsec.co)



[snapsec.co](http://snapsec.co)



Office 1098C, 182-184 High Street North, East Ham, London E6 2JA, UK

