activebytes innovations

ACTIVESENSE

Cyber Learning Platform

REVOLUTIONIZING CYBER SECURITY EDUCATION AND AWARENESS

activesense

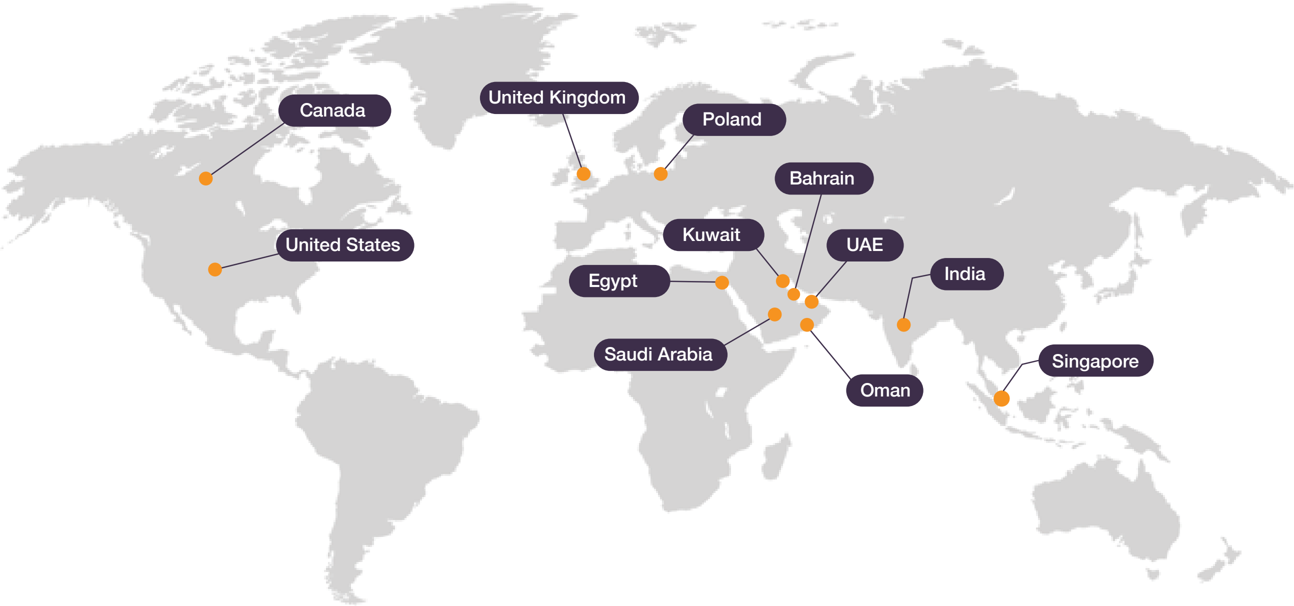
CONTENTS

Who We Are

Building Cyber-resilient Organizations

ActiveBytes Innovations has a proven track record of executing successful Information Security Projects for numerous large enterprises across different locations around the globe.

We proudly serve clients from multiple industry sectors, demonstrating our ability to adapt and provide tailored solutions to diverse business environments. Here are a few notable examples showcasing our expertise across various industries:



Why ActiveBytes?

Our Team

- Highly experienced
- Diverse
- Business-oriented

ActiveBytes team comprises highly experienced professionals with diverse expertise, all dedicated to a business-oriented approach.

With a proven track record of top-notch quality, our team is ready to exceed expectations.

Quality and Efficiency

- Exceptional
- Efficient
- Cost-effective Services

Experience the transformative power of our innovative service delivery and quality management procedures.

Enhancing security services, we aim for improved efficiency without compromising on quality.

ActiveBytes Methodology

Industry accepted methodologies, Tailored further with experience for the efficient outcome.

Outstanding Team, Technology, and Knowledge Foundations .

As your trusted partner, we promise to exceed expectations, delivering transformative value

Safeguarding Diverse Industry Sectors With State of the Art Managed Security Service

- Financial
- Education
- Government
- Oil & Gas
- Logistics & Supply Chain
- Healthcare
- Aviation
- Real Estate & Hospitality

Our Range of Services

IT Security Service:

ActiveBytes Innovations delivers comprehensive IT Security solutions, including risk assessment, threat detection, and incident response, safeguarding clients' digital assets and ensuring business continuity.

Compliance:

ActiveBytes Innovations' Compliance services help clients meet regulatory requirements, manage data protection, privacy, and incident response, ensuring a strong security posture and continuous improvement.

Governance:

ActiveBytes Innovations' Governance services establish effective security management, compliance with regulations, and swift incident response, safeguarding digital assets and ensuring exceptional results

CYBOT - Threat Management Platform

CYBOT, our Threat Management Platform, is an essential cybersecurity service designed to enhance your defense strategies. This user-friendly platform utilizes advanced technology to detect and neutralize threats in real time. Offering simplicity in threat detection and management, it provides actionable insights for swift response.

Risk:

Our Risk services proactively identify and manage security threats through comprehensive risk assessments, threat intelligence, and robust incident response strategies for secure infrastructure and data protection.

Managed Security Services:

Our MSOC is your cybersecurity ally, providing constant threat detection, swift incident response, and cutting-edge CTI. We excel in proactive threat hunting, vigilant security monitoring, robust vulnerability management, and user-friendly endpoint protection. Tailored solutions ensure resilience against evolving threats, fortifying your organization with a personalized touch for proactive cybersecurity.

ActiveSense

Immerse your team in real-world cybersecurity scenarios with our training platform. Through simulations, exercises, and hands-on training, we elevate your organization's preparedness for cyber threats. Experience the practical side of cybersecurity, ensuring your teams are adept at handling evolving challenges and enhancing their skills to safeguard your organization effectively.

ActiveSense

Empowering Everyone

In today's ever-changing threat landscape, cybersecurity training is vital. At Active Bytes, we recognized this need and developed ActiveSense - a revolutionary platform to address it. Through meticulous research and innovation, ActiveSense combines cutting-edge technology with practical training. Our Awareness Platform fosters a security-conscious culture, while the Cyber Range provides hands-on skill development. Our University offers continuous learning opportunities. ActiveSense equips organizations with the tools to navigate modern cybersecurity threats effectively. Join us in embracing proactive education and safeguarding digital assets with ActiveSense.

Core Components of ActiveSense

EMULATE

activesense AWARENESS

SIMULATE

activesense RANGE

LEARN

activesense UNIVERSITY

Experience the future of cybersecurity education with ActiveSense

- Utilizing our emulation technology, we accurately recreate real-world cyber attacks, enabling organizations to assess the cyber awareness of their employees.
- Our dynamic simulation feature challenges your defenses with real-time scenarios, guaranteeing preparedness against constantly evolving threats.
- Augmenting these immersive experiences is our all-encompassing learning platform, providing online and classroom training options, along with certifications and badges.

EMULATE, SIMULATE, and LEARN with ActiveSense.

activesense AWARENESS

- Email/SMS through awareness
- Emulate phishing/vishing/smishing scenarios
- Deep Fake Audio and Deep Fake Video awareness
- Pre-loaded USB attacks emulation
- Hands-on cyber defence practice
- English and Arabic training materials
- 500+ Out-of-box Pre-Designed Templates

activesense RANGE

- Lifelike threat scenarios
- Realistic simulations
- Diverse practice
- Seamless integration
- Robust tool stack
- Involvement of SOC, network, IT, and endpoint teams

activesense UNIVERSITY

- Tailored instructor-led and self-paced courses
- Flexibility in learning styles
- Comprehensive cybersecurity education
- Engaging labs reinforce skills
- Seamless integration via ActiveSense
- Cultivate security awareness
- Certification and Badges

ActiveSense Awareness

Educate and Empower Everyone

Introducing ActiveSense Awareness component designed to both educate and assess your employees. ActiveSense Awareness is a core component of the ActiveSense platform, designed to immerse participants in an interactive cybersecurity training environment using Email /SMS. Through simulated phishing, vishing, and smishing assessment campaigns, and advanced features like Deepfake technology and USB assessments, ActiveSense Awareness provides practical experience in defending against real-world cyber threats.

Features of ActiveSense Awareness:

ActiveSense Awareness Training focuses on educational content via email and SMS with real-world assessments to educate and elevate security consciousness.

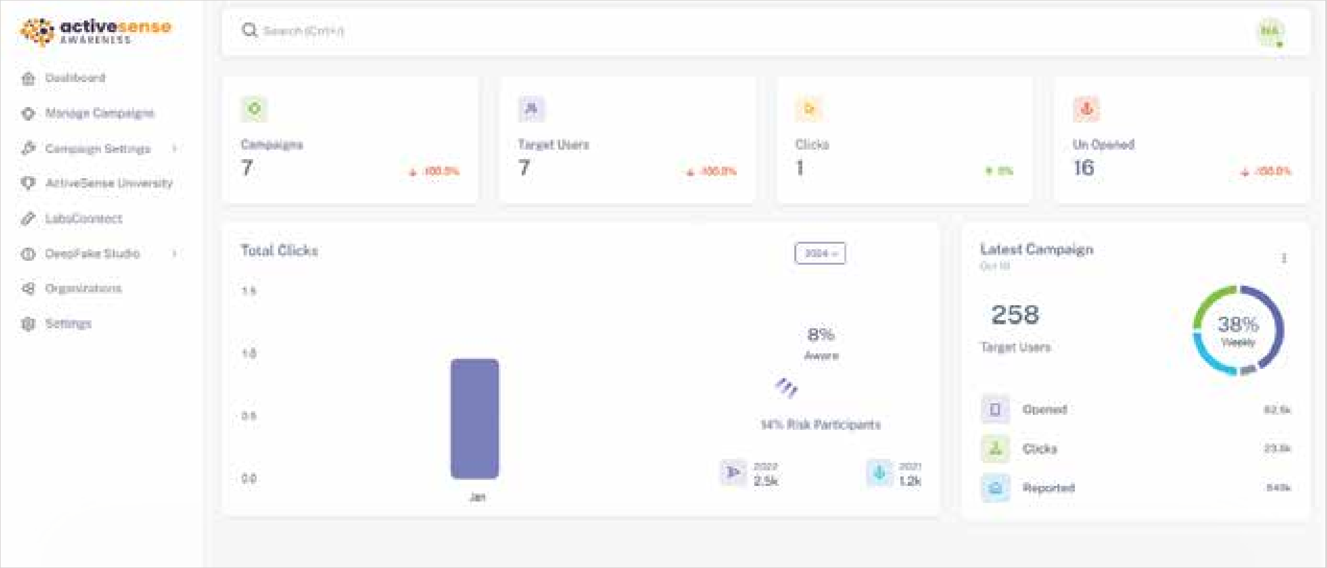
Email | SMS

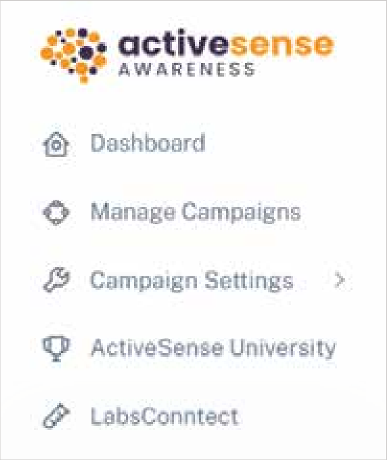
ActiveSense Awareness Assessment gauge the effectiveness of cybersecurity awareness initiatives through simulated real-world Phishing, Smishing, and Vishing attacks.

Phishing | Smishing | Vishing

Active Sense Awareness Advanced Features simulated Deep Fake videos or Deep Fake audio recordings mimicking various scenarios, such as phishing attempts, social engineering attacks, or CEO fraud.

Deep Fake Studio | USB





Dashboard

Get a comprehensive summary of all campaigns, including information about target users, Phishing URL click summaries, unread messages, total clicks, and more. This dashboard offers platform admins an easy-to-understand overview of different campaigns and their responses.

Manage Campaigns

Effortlessly streamline campaign initiation and monitoring. Admins can seamlessly send informative training emails or SMS messages through Awareness Campaigns. Additionally, Assessment Campaigns simulate phishing, smishing, or vishing scenarios to gauge training effectiveness. Use Manage Campaigns to enhance team awareness and readiness in cybersecurity by launching training or assessment initiatives.

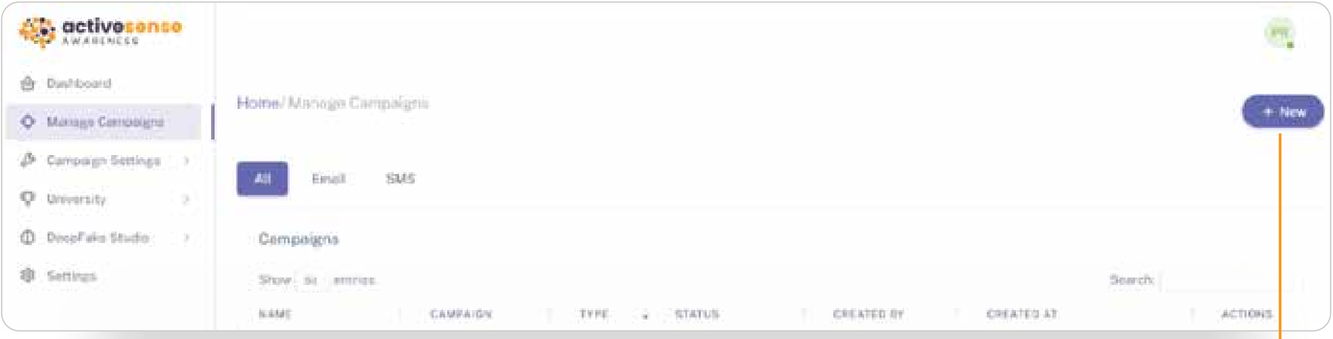
Campaign Settings

Empower administrators with comprehensive control over campaign management. Customize target user groups, integrate new templates and scripts for training or assessment, configure sending profiles, and access an extensive repository of content. Unlock a wealth of features to tailor and optimize your campaigns effortlessly.

ActiveSense Awareness

Educate and Empower Everyone

TRAINING: Email | SMS



activesense AWARENESS

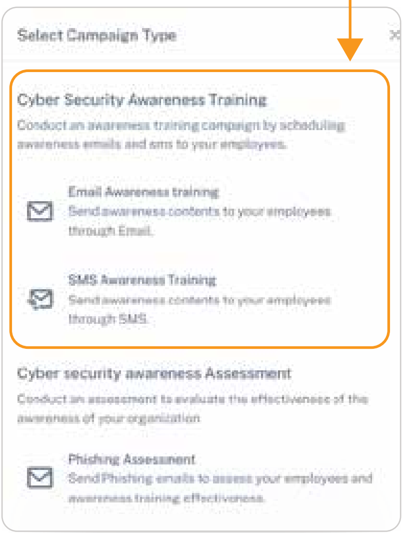
Campaigns

Show 10 entries

Search:

NAME	CAMPAIGN	TYPE	STATUS	CREATED BY	CREATED AT	ACTIONS

- Effortlessly create and schedule training campaigns for your employees by email or SMS.
- Track and record interactions to measure user engagement and assess the effectiveness of awareness and assessment campaigns.
- Enjoy user-friendly navigation for seamless interaction and improved user experience.



Select Campaign Type

Cyber Security Awareness Training

Conduct an awareness training campaign by scheduling awareness emails and sms to your employees.

Email Awareness training

Send awareness contents to your employees through Email.

SMS Awareness Training

Send awareness contents to your employees through SMS.

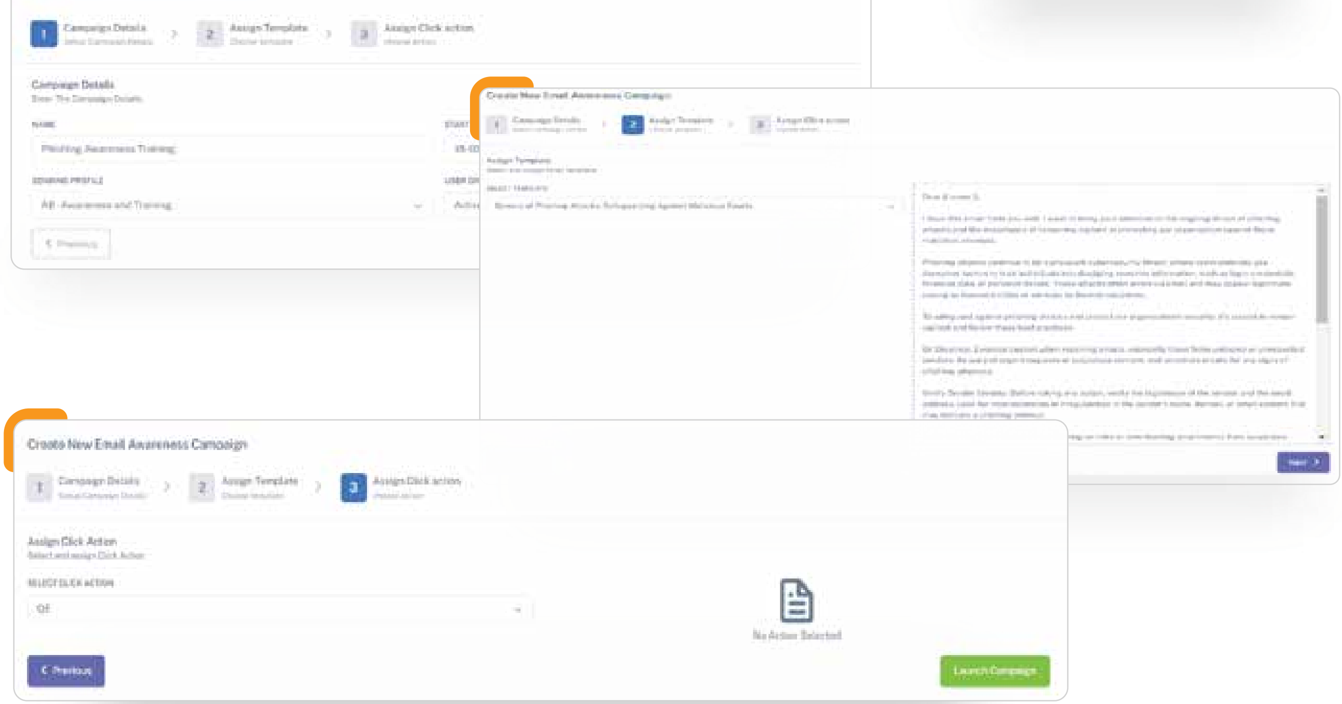
Cyber security awareness Assessment

Conduct an assessment to evaluate the effectiveness of the awareness of your organization

Phishing Assessment

Send Phishing emails to assess your employees and awareness training effectiveness.

Home/ Campaigns/ New



Create New Email Awareness Campaign

Campaign Details

Enter The Campaign Details

NAME: Phishing Awareness Training

SENDING PROFILE: AB - Awareness and Training

Create New Email Awareness Campaign

Assign Template

SELECT TEMPLATE: Science of Phishing Attacks: Safeguarding Against Malicious Emails

Create New Email Awareness Campaign

Assign Click Action

Select and assign Click Action

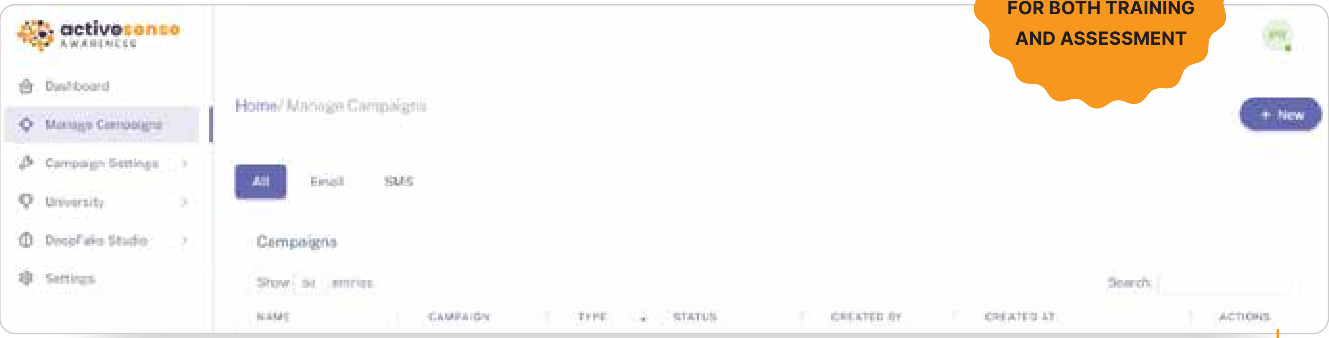
SELECT CLICK ACTION: Off

ActiveSense Awareness

Educate and Empower Everyone

ASSESSMENT: Phishing | Smishing | Vishing

500+ PRE-BUILT TEMPLATES IN ENGLISH AND ARABIC FOR BOTH TRAINING AND ASSESSMENT

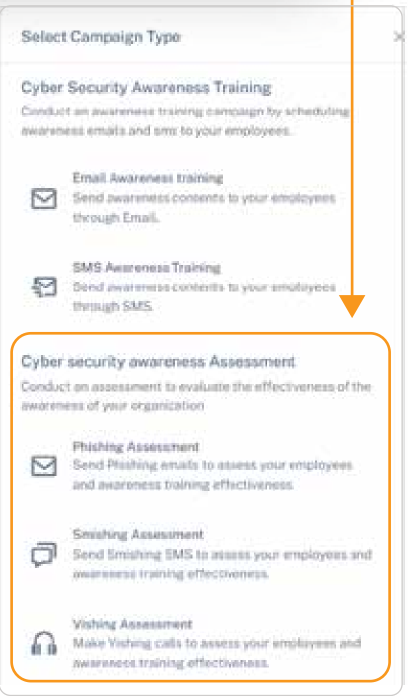


Emulate Assessment Campaigns:

These campaigns mimic real-world cyber-attacks to simulate phishing, smishing, and vishing scenarios:

- **Phishing:** Simulated emails imitate legitimate sources to test users' responses.
- **Smishing:** Fraudulent text messages are sent to assess users' reactions to SMS-based attacks.
- **Vishing:** Phone calls with social engineering tactics gauge users' susceptibility to voice-based phishing attempts.

Our platform enables organizations to emulate these campaigns effectively for training and assessment purposes, enhancing their cybersecurity readiness.



Select Campaign Type

Cyber Security Awareness Training

Conduct an awareness training campaign by scheduling awareness emails and sms to your employees.

Email Awareness training

Send awareness contents to your employees through Email.

SMS Awareness Training

Send awareness contents to your employees through SMS.

Cyber security awareness Assessment

Conduct an assessment to evaluate the effectiveness of the awareness of your organization

Phishing Assessment

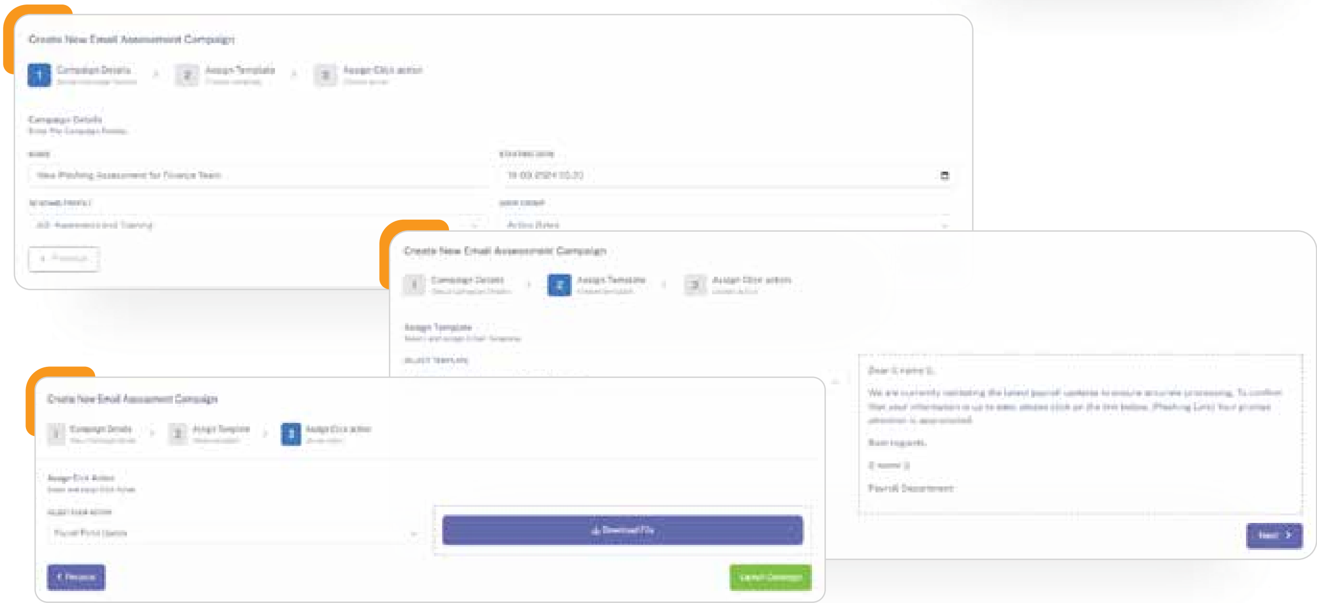
Send Phishing emails to assess your employees and awareness training effectiveness.

Smishing Assessment

Send Smishing SMS to assess your employees and awareness training effectiveness.

Vishing Assessment

Make Vishing calls to assess your employees and awareness training effectiveness.



Create New Email Assessment Campaign

1 Campaign Details › 2 Assign Template › 3 Assign Click action

Campaign Details

Enter the Campaign Details

NAME: New Phishing Assessment for Finance Team

STARTING DATE: 19-03-2024 10:20

USER GROUP: Active Rules

Create New Email Assessment Campaign

Assign Template

SELECT TEMPLATE

Dear {{ name }},

We are currently validating the latest payroll updates to ensure accurate processing. To confirm that your information is up to date, please click on the link below. {Phishing Link} Your prompt attention is appreciated.

Best regards,

{{ name }}

Payroll Department

Create New Email Assessment Campaign

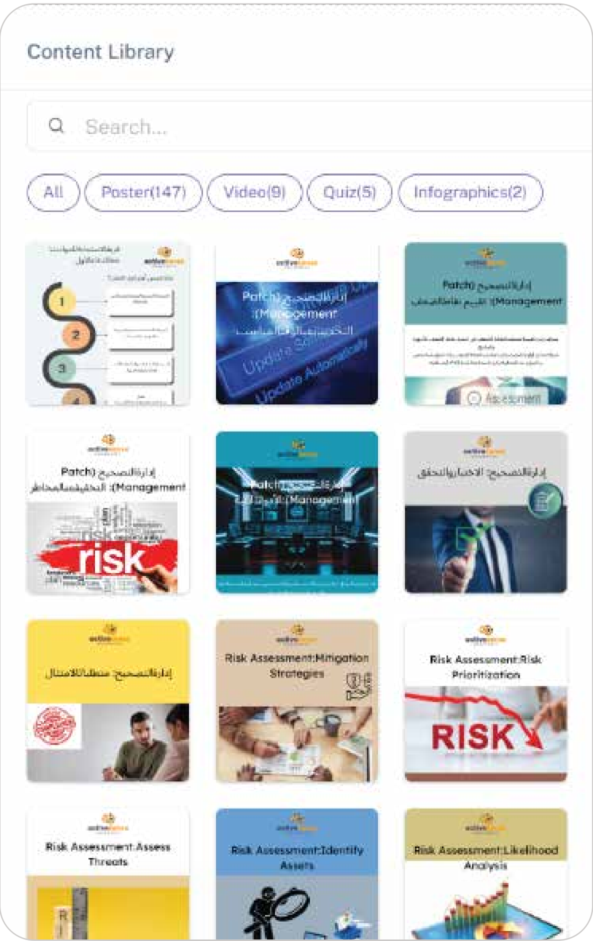
Assign Click Action

SELECT CLICK ACTION

Out-of-box contents for Campaigns

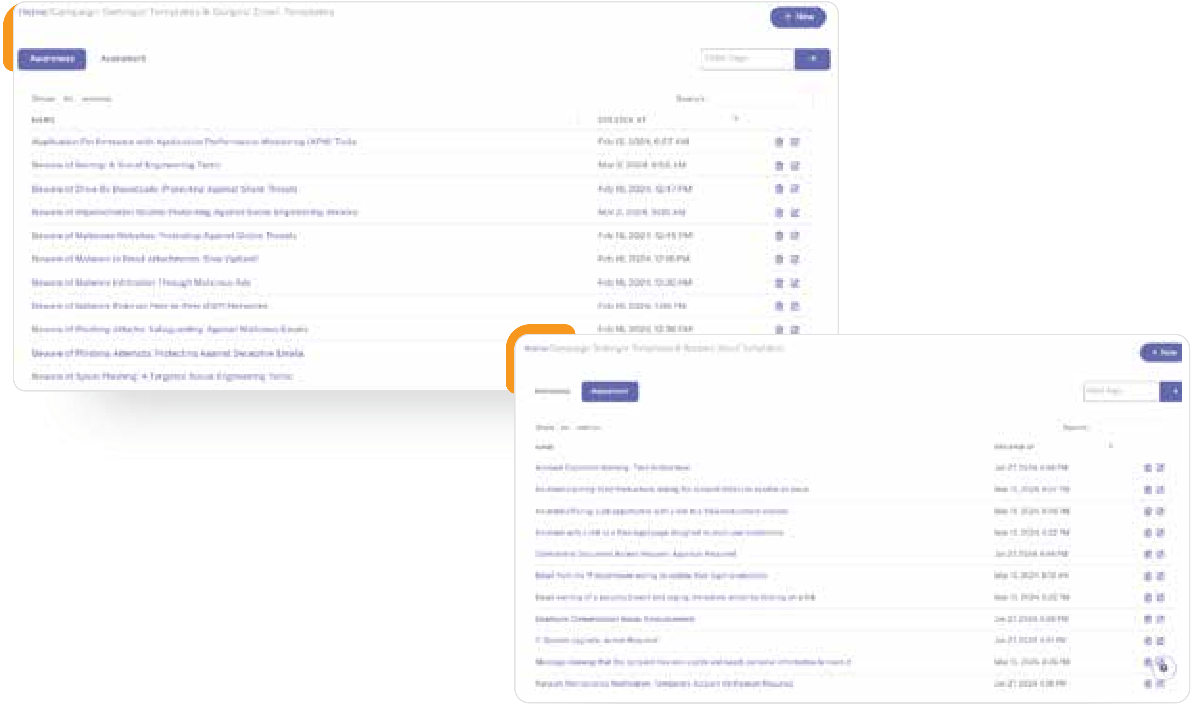
Access a wide range of educational materials in both English and Arabic to enrich your campaigns. From interactive quizzes to informative videos and captivating awareness posters, effortlessly strengthen your team's understanding and promote best practices at work.

- Poster
- Video
- Quiz
- Infographics


Content Library
Search...
All
Poster(147)
Video(9)
Quiz(5)
Infographics(2)
Patch) إدارة التصحيح
:Management)
Update Software
Update Automatically
risk
Risk Assessment:Mitigation Strategies
Risk Assessment:Risk Prioritization
RISK
Risk Assessment:Assess Threats
Risk Assessment:Identify Assets
Risk Assessment:Likelihood Analysis

Templates and Scripts

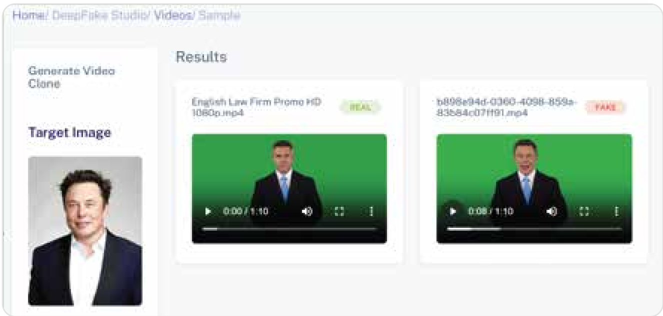
"500+ Pre-Designed Templates: Effortlessly create engaging communication materials for Email/SMS training and phishing, vishing, and smishing assessment campaigns in English and Arabic."



Deepfake Studio

Deepfake Studio help generate realistic simulated videos or audio recordings mimicking various cyber threat scenarios like phishing attempts or social engineering attacks. Users develop critical skills in identifying genuine versus manipulated content, enhancing their ability to spot potential cyber threats.

Deepfake Video: Challenge users with interactive training modules to identify deepfake videos. Admins receive guidance on creating deepfake videos, ensuring optimal results for users' training and simulation exercises.


Home/ DeepFake Studio/ Videos/ Sample
Generate Video Clone
Target Image
Results
English Law Firm Promo HD 1080p.mp4
REAL
0:00 / 1:10
b898e94d-0360-4098-859a-83b84c07ff91.mp4
FAKE
0:08 / 1:10

Deepfake Audio: Employ AI and machine learning to generate deepfake audio from minimal original voice data, heightening awareness of audio deepfakes' prevalence and impacts. Equip stakeholders with tools and knowledge to navigate audio deepfake complexities effectively.

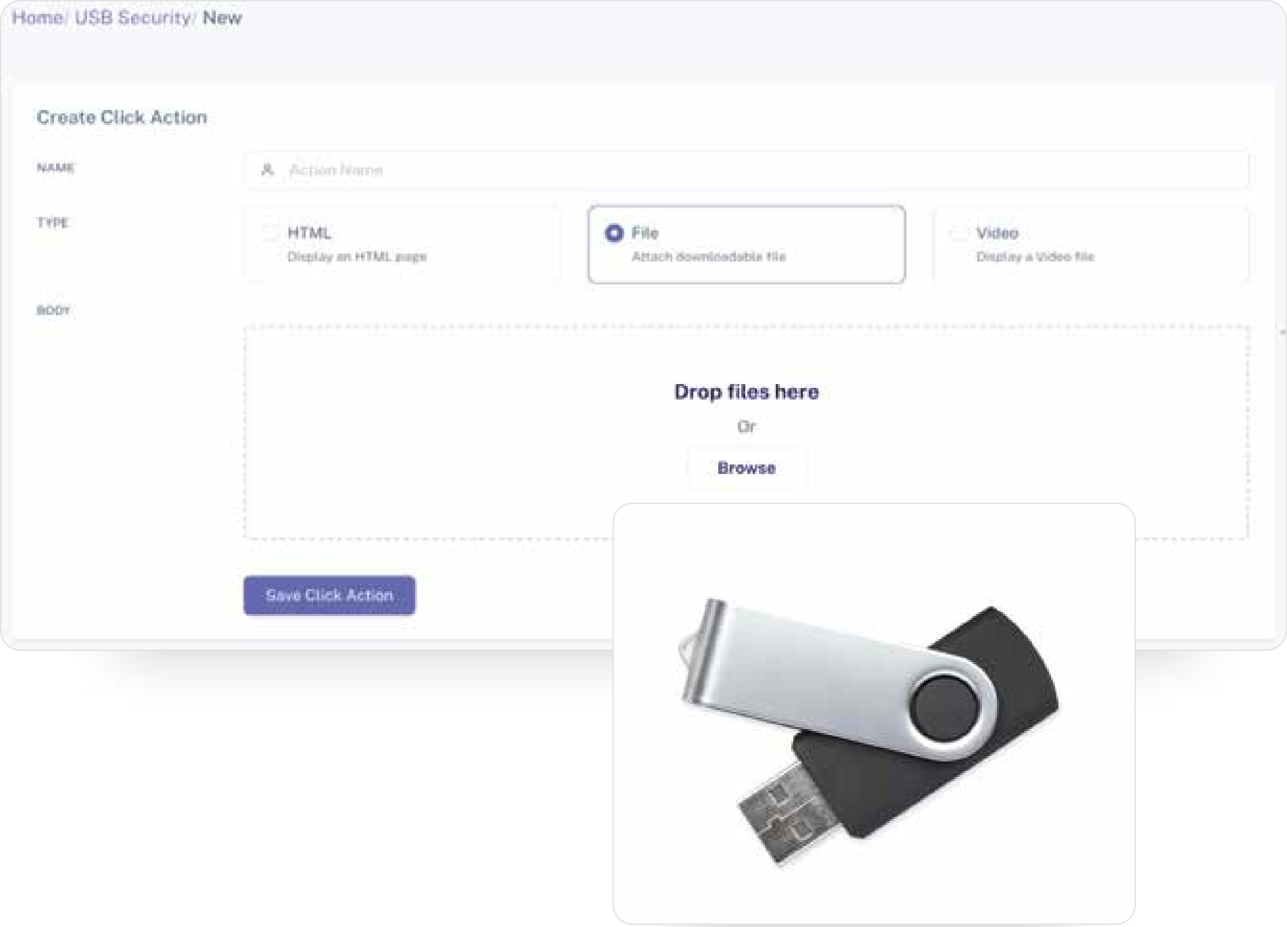
Dual-Level Approval Process

Our dual-level approval process, combining administrator and Active Sense approval, ensures responsible usage, while stringent verification processes authenticate audio/video samples and secure explicit consent from owners, all underscored by our commitment to transparency and ethical use throughout the deepfake creation process.

ADVANCED FEATURES: USB

USB Security Assessments

- **Tailored Document Generation:** Effortlessly generate documents tailored for USB security assessment scenarios. Easily copy these documents to USB drives for convenient assessment and enhancement of USB security measures.
- **User Tracking & Insights:** Track potential users connecting untrusted USB drives to enterprise devices. Gain valuable insights into USB usage patterns and potential security risks.
- **Proactive Threat Mitigation:** Take a comprehensive approach to proactively mitigate USB-related security threats.



Home/ USB Security/ New

Create Click Action

NAME: Action Name

TYPE: ○ HTML Display an HTML page ● File Attach downloadable file ○ Video Display a Video file

BODY

Drop files here
Or
Browse

Save Click Action

ActiveSense Cyber Range

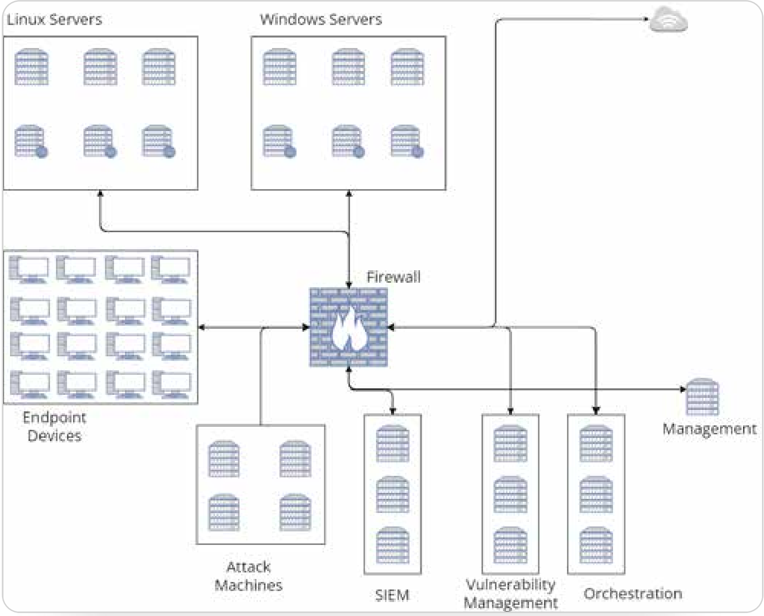
Where Virtual Realities Shape Digital Defenses

Experience immersive scenarios that elevate your readiness against diverse cyber threats.

Experience comprehensive simulation capabilities, covering various attack techniques such as defacement, malware, breaches, and ransomware, ensuring thorough security control evaluation. Benefit from integrated tools including SIEM, Firewall, and Vulnerability Management Tools, enhancing your cybersecurity training. Extend your defense beyond IT to include Operational Technology (OT) infrastructure, ensuring holistic protection against cyber threats.

Elevate your cyber defense with ActiveSense Cyber Range, where virtual realities shape digital defenses.

- Provide a controlled environment for cybersecurity training, testing, and simulation.
- Enhance the skills of cybersecurity professionals and students.
- Enable realistic and hands-on training exercises for responding to cyber threats.
- Strengthen our organization's overall cybersecurity posture.



Evaluating Cyber Readiness

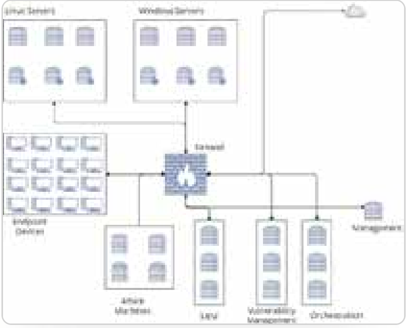
Improving Team Skills

No Infrastructure Required

Diverse Scenarios

Enhancing Incident Response Capabilities

Exposure to Real-Time Attacks

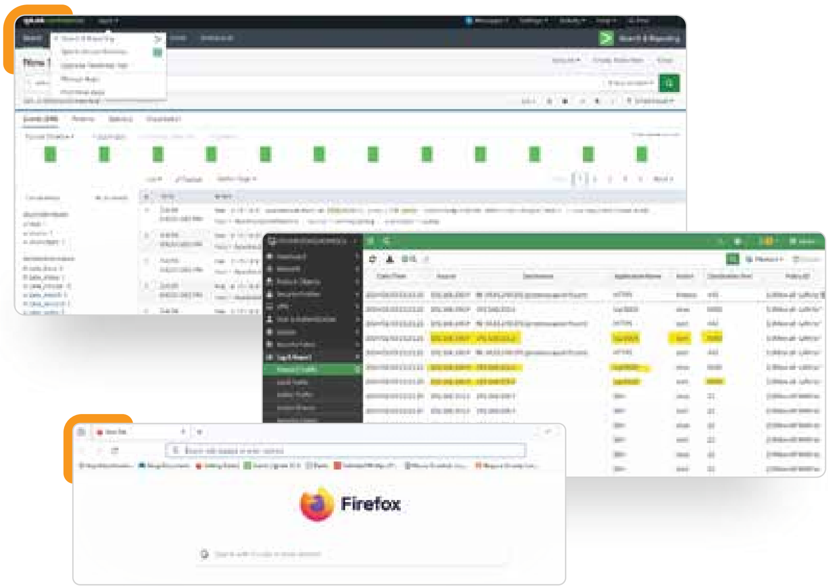


Comprehensive Simulation:

Engage in an enterprise simulation exercise that mirrors real-life IT infrastructure scenarios. This immersive experience allows you to simulate a variety of attack techniques, including defacement, malware intrusions, data breaches, and ransomware incidents. Through these simulations, you can thoroughly evaluate the effectiveness of your security controls and readiness to respond to cyber threats.

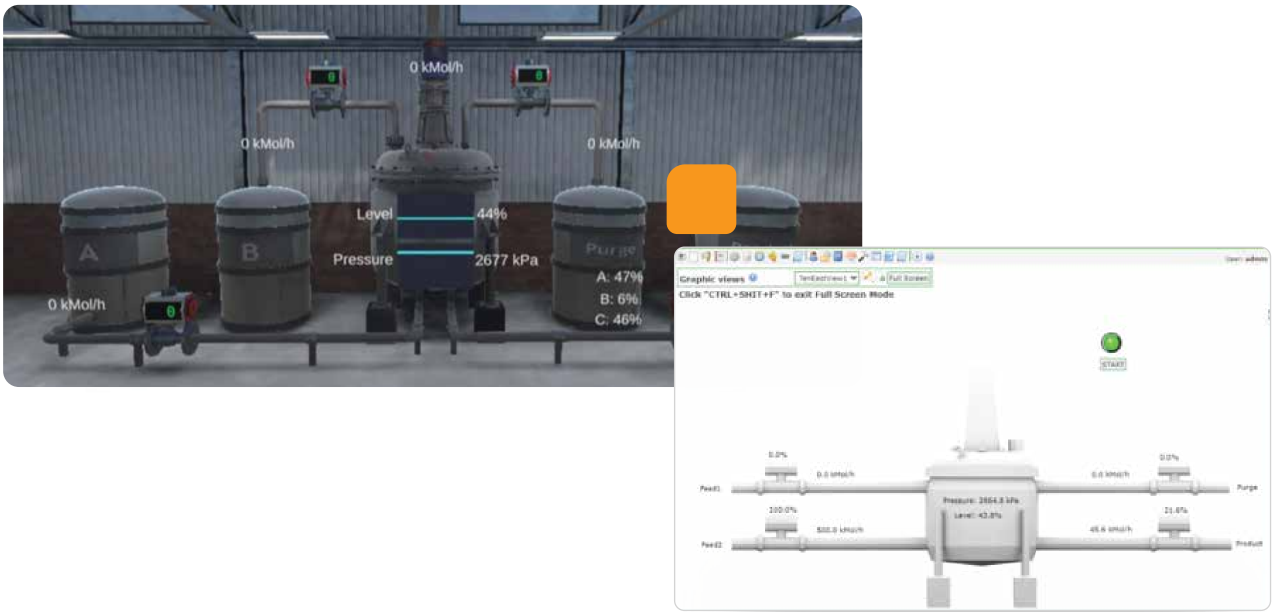
Integrated Tools

Utilize SIEM tools, Firewall, and Vulnerability Management Tools for comprehensive cybersecurity training.



Beyond IT

Extend your defense to Operational Technology (OT) infrastructure for holistic protection.



Click "CTRL+SHIT+F" to exit Full Screen Mode

Our Cyber Range Simulation Scenarios

ActiveSense offers a comprehensive array of attack simulations tailored to diverse proficiency levels, spanning from beginner to advanced.

Linux Webserver Compromise:
Assault on an Apache web server using SSH brute-force method.

Windows Webserver Compromise:
IIS server defaced via brute force on open port 80 and RDP, unauthorized access gained through Administrator account breach.

Kiosk Gateway Breach (OT):
Threat actor targets OT network, exploits misconfigured firewall rule to expose Windows 7 Kiosk system to employee network.

Pwning PLCs:
Threat actor executes various attacks in OT network including ARP Spoofing, Injecting malicious Modbus Command, and Uploading Malicious PLC program.

On the way to Active Directory:
Compromise of a supplier's credentials leads to webserver and eventually Active Directory compromise, simulating APT-27 attack vectors.

Temporarily Exposed Development Environment:
Attacker compromises a web application under development using weak credentials and vulnerabilities, executes commands, and exfiltrates data.

Ransomware Spread:
Attacker compromises an employee computer via social engineering attack and spreads ransomware within the organization.

Shadow Admin compromises Active Directory:
Threat actor compromises a user with unintended high privilege in Active Directory, leading to domain controller compromise.

Lazy Admin Datacentre Compromise:
Compromising data centre VMware hosting environment due to weak management of sensitive access by admin.

Shared Password Shares the Impact:
Threat actor compromises one Windows workstation via Active Directory attack and performs lateral movement to another workstation with higher privilege.

Bad Mail Got In:
Threat actor bypasses email security filters to deliver malicious mail to an employee, compromising the user workstation.

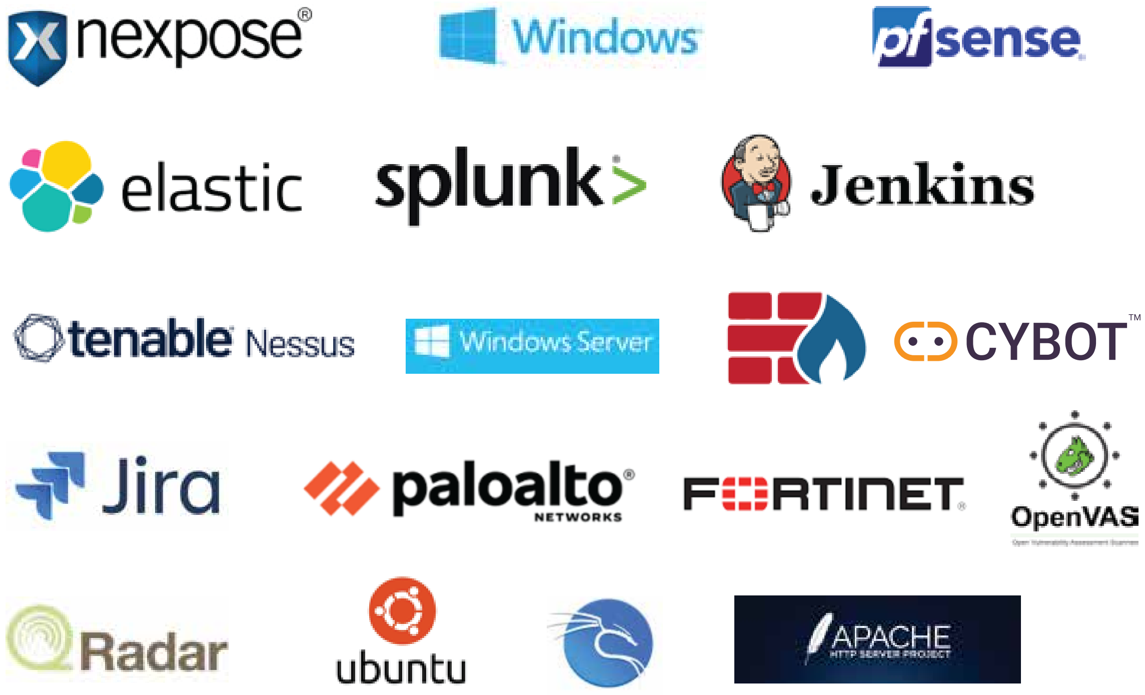
Charming Kitten APT on Microsoft Exchange:
Simulation of Iranian APT group charming kitten attack on Microsoft Exchange server, deploying a new backdoor along the way.

Proficiency of Commercial Tools

Explore the latest licensed cybersecurity tools and software preinstalled within the range. Conducting attack simulations enables teams to assess their proficiency in utilizing these tools effectively.

Evaluate the integration of tools into the security framework, their configuration efficiency, and their ability to deliver expected protection levels. Maximize investments in licensed tools and ensure they are properly utilized to defend against cyber threats.

Below are commercially available enterprise tools and solutions

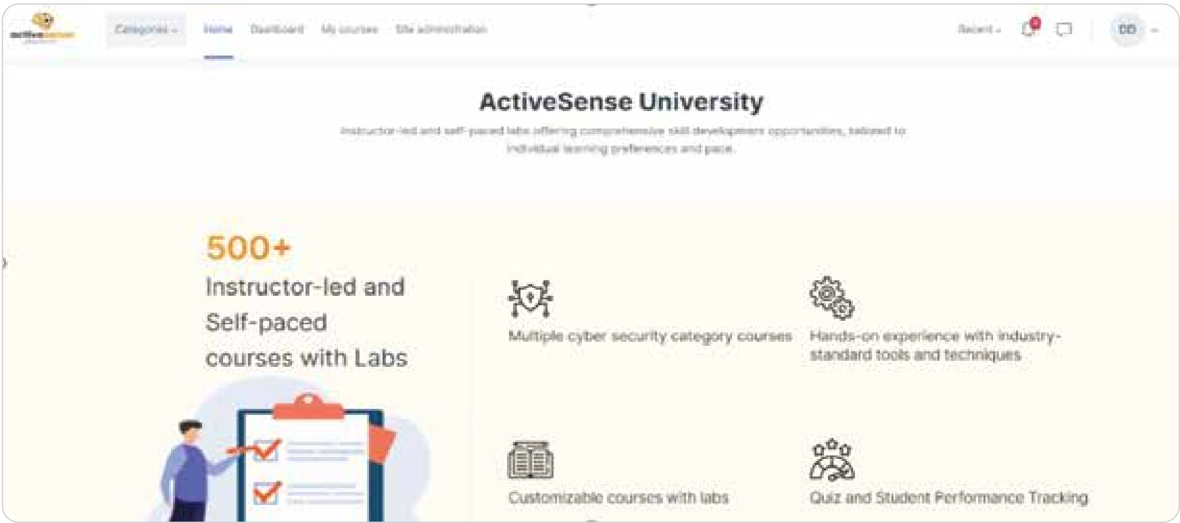


ActiveSense University

Where Theory Meets Practice

Introducing Next-Generation Learning Environment

Experience a dynamic learning environment tailored to your preferences and pace, ensuring comprehensive skill development opportunities that evolve with the ever-changing threat landscapes.



ActiveSense University

Instructor-led and self-paced labs offering comprehensive skill development opportunities, tailored to individual learning preferences and pace.

500+ Instructor-led and Self-paced courses with Labs

Multiple cyber security category courses

Hands-on experience with industry-standard tools and techniques

Customizable courses with labs

Quiz and Student Performance Tracking

Unique Blend of Instructor-led and Self-paced Courses:

Access over 250 courses covering multiple cybersecurity categories, from Cyber Security Basics to Penetration Testing, Web Application Security, and more.

Hands-on Approach with Industry-standard Tools:

Get practical experience with hands-on lab exercises reinforcing cybersecurity skills and tactics using industry-standard tools and techniques.

Flexible Learning Options

Access over 250 courses covering multiple cybersecurity categories, from Cyber Security Basics to Penetration Testing, Web Application Security, and more.

Tailored Learning Experience

Tailor your learning journey by selecting courses aligning with your specific interests and career goals.

Recognition and Achievement

Earn badges and certificates showcasing your expertise and accomplishments in the cybersecurity domain.

ActiveSense University – Platform

Designed to support your success, the ActiveSense University Platform offers two distinct access methods tailored to diverse learning needs and organizational structures.

Open Access for Self-Enrolment

Gain unrestricted access to all courses within the platform. Explore the full catalog, enroll in courses of interest, and shape your learning journey according to your pace and preferences.

Restricted Access for Enrolled Courses

Access is limited to enrolled courses, ensuring focus on specific curriculum, job roles, or organizational requirements. Streamline learning processes and align educational or professional development needs effectively.

Flexible access modes to accommodate various learning preferences and organizational structures.

Prefer exploring the full Catalog or focusing on specific courses, our platform ensures access to essential resources for cybersecurity education success.

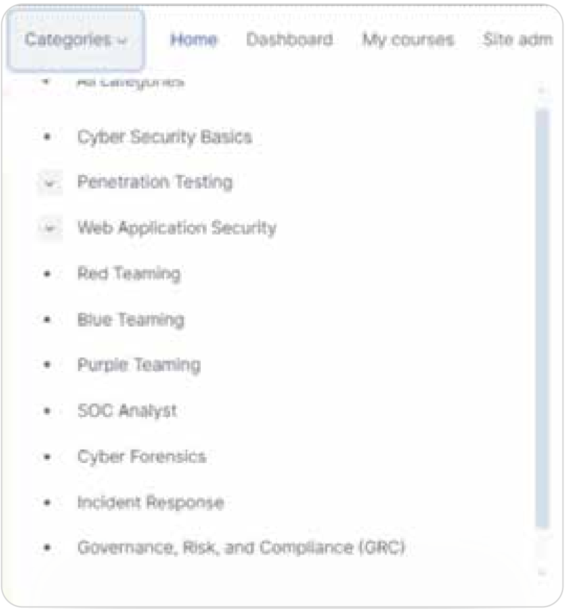
ActiveSense University course catalogue

The Course Category section is the heart of ActiveSense University, offering over **250 cybersecurity courses.**

Explore topics from basics to specialized areas using filters like keywords or subcategories. Includes Cyber Security Basics and Penetration Testing, finding relevant courses is easy.

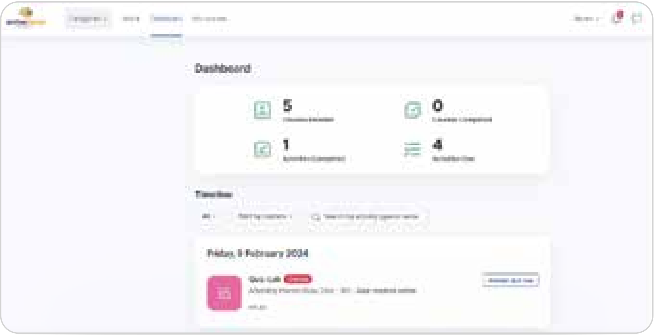
Ten distinct categories

- Cyber Security Basics
- Penetration Testing
- Web Application Security
- Red Teaming
- Blue Teaming
- Purple Teaming
- SOC Analyst
- Cyber Forensics
- Incident Response
- Governance, Risk, and Compliance (GRC)



ActiveSense University - Student Dashboard

Dashboard: Provides a central hub for your cybersecurity training journey, offering quick access to relevant labs, progress tracking, and personalized insights.



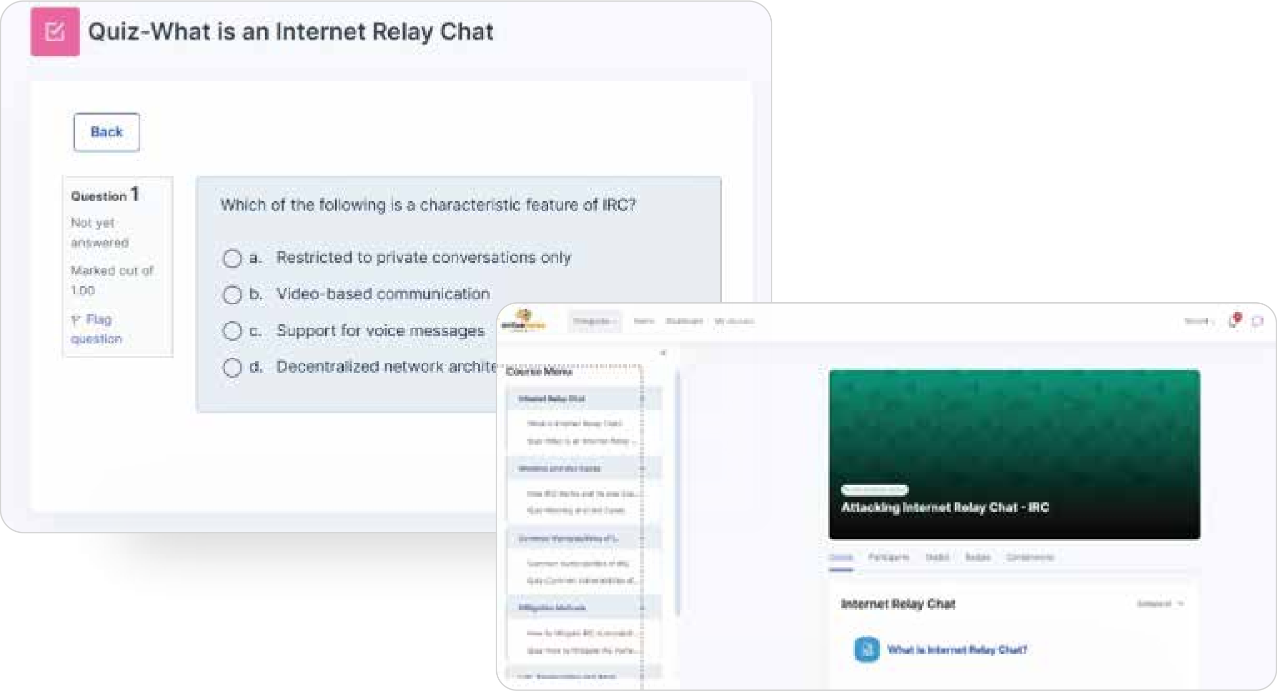
Timeline: Displays due dates, events, and deadlines from all your enrolled courses.

Search and Filter: Find specific labs by keyword, difficulty, topic, or completion status.

Calendar: View upcoming deadlines and scheduled instructor-led sessions.

ActiveSense University - Courses

Explore a selection of 500+ courses covering diverse categories in cybersecurity, each featuring hands-on lab exercises and quizzes.



Quiz-What is an Internet Relay Chat

Back

Question 1
Not yet answered
Marked out of 1.00
Flag question

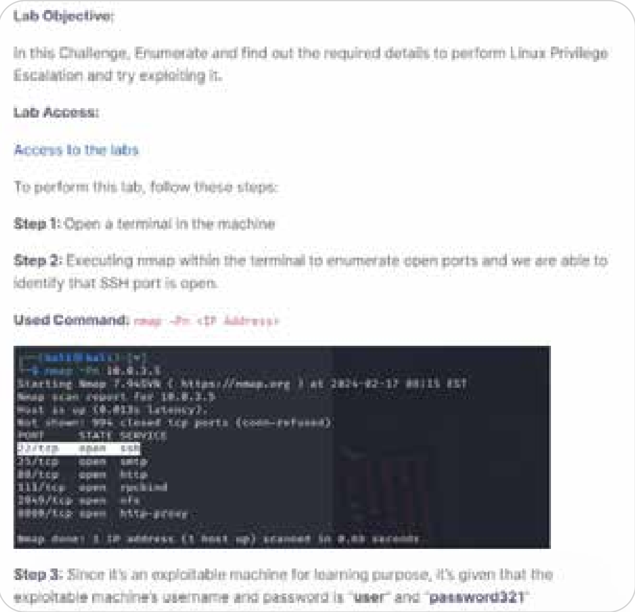
Which of the following is a characteristic feature of IRC?

○ a. Restricted to private conversations only
○ b. Video-based communication
○ c. Support for voice messages
○ d. Decentralized network archite

Course Menu
Attacking Internet Relay Chat - IRC
Internet Relay Chat
What is Internet Relay Chat?

ActiveSense University - Labs

ActiveSense University platform features interactive labs accompanying each course. These labs allow users to apply the knowledge gained in the course to real-world scenarios, reinforcing key concepts and enhancing practical skills. Users can access the labs directly from the course page, making it easy to seamlessly transition between theory and practice.



Lab Objective:

In this Challenge, Enumerate and find out the required details to perform Linux Privilege Escalation and try exploiting it.

Lab Access:

Access to the labs

To perform this lab, follow these steps:

Step 1: Open a terminal in the machine

Step 2: Executing nmap within the terminal to enumerate open ports and we are able to identify that SSH port is open.

Used Command: `nmap -Pn <IP Address>`

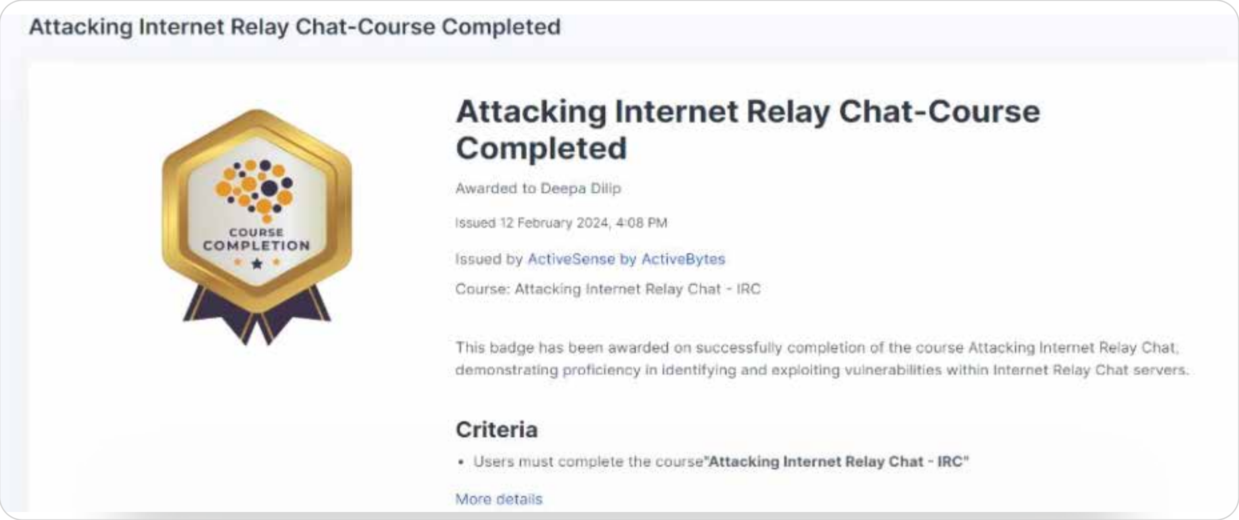
```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-17 08:15 EST
Nmap scan report for 10.0.2.5
Host is up (0.013s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
2049/tcp open  nfs
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Step 3: Since it's an exploitable machine for learning purpose, it's given that the exploitable machine's username and password is "**user**" and "**password321**"

ActiveSense University - Digital Badges

Introducing our new feature: Badges for Course Achievement!

- Earn badges that validate your participation and accomplishments in enrolled courses.
- These badges offer visual recognition, celebrating your milestones and completion of tasks within each course. Level up your learning experience with tangible acknowledgments of your progress!.



Attacking Internet Relay Chat-Course Completed

Attacking Internet Relay Chat-Course Completed

Awarded to Deepa Dilip

Issued 12 February 2024, 4:08 PM

Issued by ActiveSense by ActiveBytes

Course: Attacking Internet Relay Chat - IRC

This badge has been awarded on successfully completion of the course Attacking Internet Relay Chat, demonstrating proficiency in identifying and exploiting vulnerabilities within Internet Relay Chat servers.

Criteria

- Users must complete the course"**Attacking Internet Relay Chat - IRC**"

More details

Notice

This document contains information about the proprietary property of ActiveBytes Innovations. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of ActiveBytes Innovations.

Nothing in this document constitutes a guarantee, warranty, or license, express or implied. ActiveBytes Innovations disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to Fitness for a particular purpose; merchantability; not infringement of intellectual property or other rights of any third party or of ActiveBytes Innovations; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technology discussed herein and is advised to seek the advice of competent legal counsel, without obligation of ActiveBytes Innovations.

ActiveBytes Innovations retains the right to make changes to this document at any time, without notice. ActiveBytes Innovations makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein.

Copyright

Trademarks

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owner’s benefit, without any intent to infringe.

Contact Us

ActiveBytes Innovations

Sharjah Media City, Sharjah, UAE, Dubai, UAE +971 505676727
www.active-bytes.com