

ROCHESTON®

Rocheston Certified
**SECURITY OPERATIONS
CENTER**

SOC ANALYST

Rocheston Certified **SOC Analyst**

This comprehensive **Rocheston Certified Security Operations Center (SOC) Analyst** course equips you with the skills and knowledge to excel in this critical role. It's designed for both aspiring SOC professionals and current IT specialists seeking to enhance their cybersecurity expertise. **The course goes beyond theory, offering a blend of practical exercises and real-world simulations.** You'll learn by doing, putting your newfound knowledge to the test in scenarios that mimic the fast-paced environment of a real SOC.



This comprehensive **Rocheston Certified Security Operations Center (SOC) Analyst** course equips you with the skills and knowledge to excel in this critical role. It's designed for both aspiring SOC professionals and current IT specialists seeking to enhance their cybersecurity expertise. **The course goes beyond theory, offering a blend of practical exercises and real-world simulations.** You'll learn by doing, putting your newfound knowledge to the test in scenarios that mimic the fast-paced environment of a real SOC.



By the end of the course, you'll be a confident and capable SOC Analyst, equipped to protect your organization from today's ever-evolving cyber threats.

The course also prepares you for the **Rocheston Certified SOC Analyst (RSOC) exam,** a valuable credential demonstrating your proficiency in SOC operations.

Target Audience

IT security professionals seeking a career in SOC operations

Network security analysts looking to expand their skillset

Security professionals transitioning to a SOC analyst role

Anyone interested in gaining a comprehensive understanding of SOC operations



The cyber world, awash in the glow of our connected devices, presents a double-edged sword. While opportunities abound, a hidden war wages behind the scenes. **Cybercriminals, like shape-shifting adversaries, constantly adapt their tactics, rendering traditional security measures a never-ending game of catch-up.** This is where **Security Operations Center (SOC) Analysts** emerge as the valiant defenders of our digital realm.

Their expertise is in high demand for a confluence of reasons. The battlefield of cyber threats is a constantly shifting landscape, demanding analysts with the keen eye to identify and neutralize these evolving attack methods. Secondly, a talent shortage plagues **the cybersecurity industry, creating a competitive job market where skilled SOC analysts are highly sought-after assets.**

Beyond acting as reactive firefighters, SOC analysts play a crucial, proactive role. **They become digital hunters, actively seeking out potential threats, meticulously analyzing vulnerabilities, and taking preventative measures to thwart attacks before they can wreak havoc.** This proactive approach minimizes downtime and safeguards the crown jewels – our critical data.



The skills honed as a SOC analyst are highly versatile, translating seamlessly across various cybersecurity domains. **This adaptability empowers you to explore and potentially specialize in areas like threat hunting, digital forensics, or security engineering, opening doors for a rewarding career trajectory within the ever-evolving landscape of cybersecurity.**



Rocheston Certified **SOC Analyst Certification Exam / Duration**

Exam Structure

Number of Questions: 100

Format: Multiple Choice,
True/False, Short Answer

Duration: 2 Hours

Passing Score: 70%

Duration

Duration: 3 days

Delivery options:

- **Instructor-led classroom training (traditional or virtual)**
- **Blended learning** (combination of classroom sessions and online modules)
- **Self-paced online learning** (optional)

SOC Course Outline

Module 1: Introduction to Security Operations

Module 2: Security Information and Event Management (SIEM)

Module 3: Incident Detection and Analysis

Module 4: Incident Response (IR) Process

Module 5: Network Security Fundamentals

Module 6: Threat Analysis

Module 7: Threat Hunting

Module 8: Rochester Vulnerability Vines

Module 9: Rochester Cybersecurity Framework



Vines Methodology

Vines The Comprehensive Solution for SOC Operations



In the ever-evolving landscape of **cybersecurity**, having a **robust and reliable tool** is **paramount to effective security operations**. Rochester Vulnerability Vines is that all-encompassing solution. Designed to be the backbone of any **Security Operations Center (SOC)**, **Vulnerability Vines integrates everything you need to manage and protect your digital environment**. From Security Information and Event Management (SIEM) and comprehensive log management to advanced Endpoint Detection and Response (EDR/XDR) and incident response capabilities, **this software is a one-stop-shop for all your SOC needs. All-in-One Solution, Eliminate the need for multiple disparate tools, saving time and resources.**

SOC Vulnerability Vines

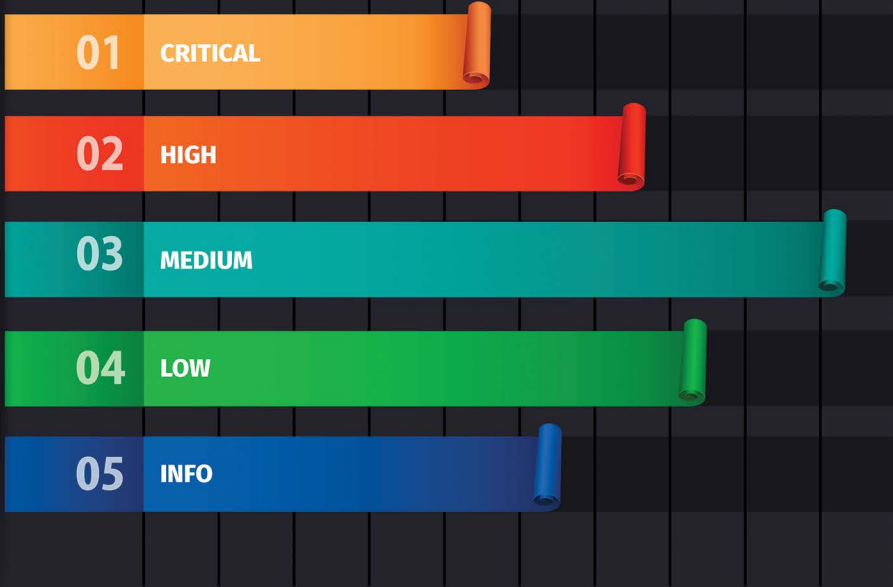


Rocheston's **Vulnerability Vines** is an advanced network scanning platform built from the ground up using **open-source components**.

The software is seamlessly integrated into the **Rocheston Certified Cybersecurity Engineer (RCCE) training program**, allowing students to deploy and manage their servers **using Vines without any additional costs**.

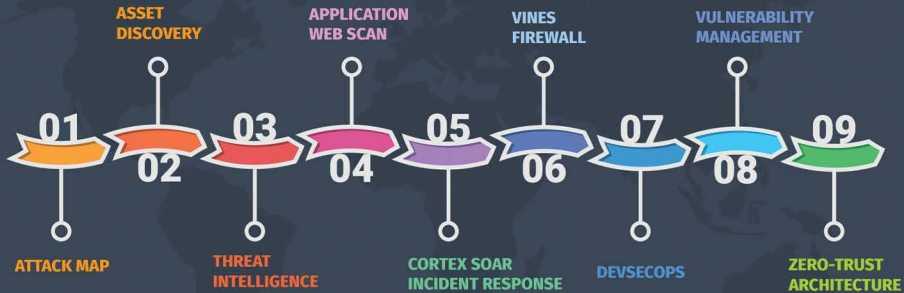
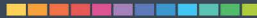
Vulnerability Vines serves as an indispensable resource for organizations aiming to strengthen their cybersecurity measures and safeguard their networks and systems against potential threats.

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%



Vines Severity Levels

Vines Services



The Most **Comprehensive Solution**

Vines is designed to detect vulnerabilities in servers, applications, source code, and Docker Kubernetes containers. **The tool offers a comprehensive security solution with features including SOAR, XDR, Threat Intelligence, DevSecOps, Compliance, Network Discovery, and Asset Management.**

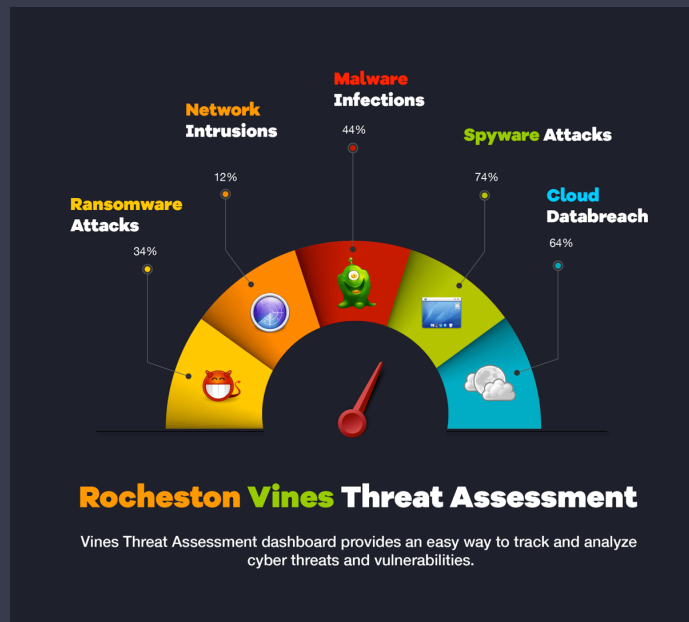


Endpoint Security & XDR

Vines's Endpoint Security & XDR is a comprehensive cybersecurity solution designed to **protect your organization's devices, networks, and data** from evolving cyber threats.

By integrating advanced endpoint protection, network security, and threat intelligence, this solution provides real-time visibility, monitoring, and response across your entire digital environment.

With its extended detection and response (XDR) capabilities, **Vines's Endpoint Security can identify, analyze, and remediate threats across various security layers, ensuring a proactive and robust defense against sophisticated attacks.** Stay ahead of cybercriminals and safeguard your organization with Vines's Endpoint Security & XDR.

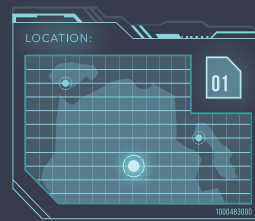


Intuitive Threat Intelligence

Introducing Intuitive **Threat Intelligence**, a cutting-edge feature of **Vulnerability Vines'** product suite designed to keep your digital assets secure.

Our advanced algorithms analyze global threat data in real-time, providing actionable insights and prioritizing risks to your organization. **Stay ahead of the ever-evolving cybersecurity landscape with our comprehensive, up-to-date threat intelligence, and safeguard your business from potential vulnerabilities.**

Empower your security teams with the **knowledge they need to make informed decisions and protect your digital ecosystem with Vulnerability Vines' Intuitive Threat Intelligence.**





CYBER ATTACKS

Global Threat Map

Defend Your **Digital Identity with Vines IAM**



Embrace the power of cutting-edge technology to safeguard your digital identity using our **advanced** Identity Protection feature.

Designed to provide comprehensive security, this innovative solution continuously monitors and secures your personal information, ensuring it remains protected from cyber threats and identity theft.

As the digital landscape evolves and cybercriminals become more sophisticated, the need for robust identity protection has never been greater. **Vulnerability Vines understands this need and delivers a multi-layered defense system, guarding your sensitive data from potential harm.** Our Identity Protection feature not only keeps your personal information secure but also alerts you to any suspicious activity, enabling you to take control and mitigate risks promptly.

Experience peace of mind knowing that your online presence is shielded from cyber-attacks and that your personal data remains confidential. With **Vulnerability Vines' Identity Protection**, you can navigate the digital world confidently, knowing that your identity is in safe hands. Don't compromise on security – choose the reliable and advanced protection you deserve.





Asset Discovery

Embrace the power of complete visibility in **your digital ecosystem with our revolutionary Asset Discovery feature.**



Vulnerability Vines' cutting-edge solution delves deep into your network, unearthing every device, application, and system to ensure nothing remains hidden. **This comprehensive view empowers you to proactively identify and manage potential risks and blind spots, fortifying your cybersecurity defenses.**

Stay ahead of emerging threats and maintain a robust security posture with Vulnerability Vines' Asset Discovery. Experience unparalleled insights, seamless integration, and a user-friendly interface that elevates your organization's security to new heights. **Discover your digital assets and safeguard your digital landscape with Vulnerability Vines today!**

Swift and Seamless **Incident Response**

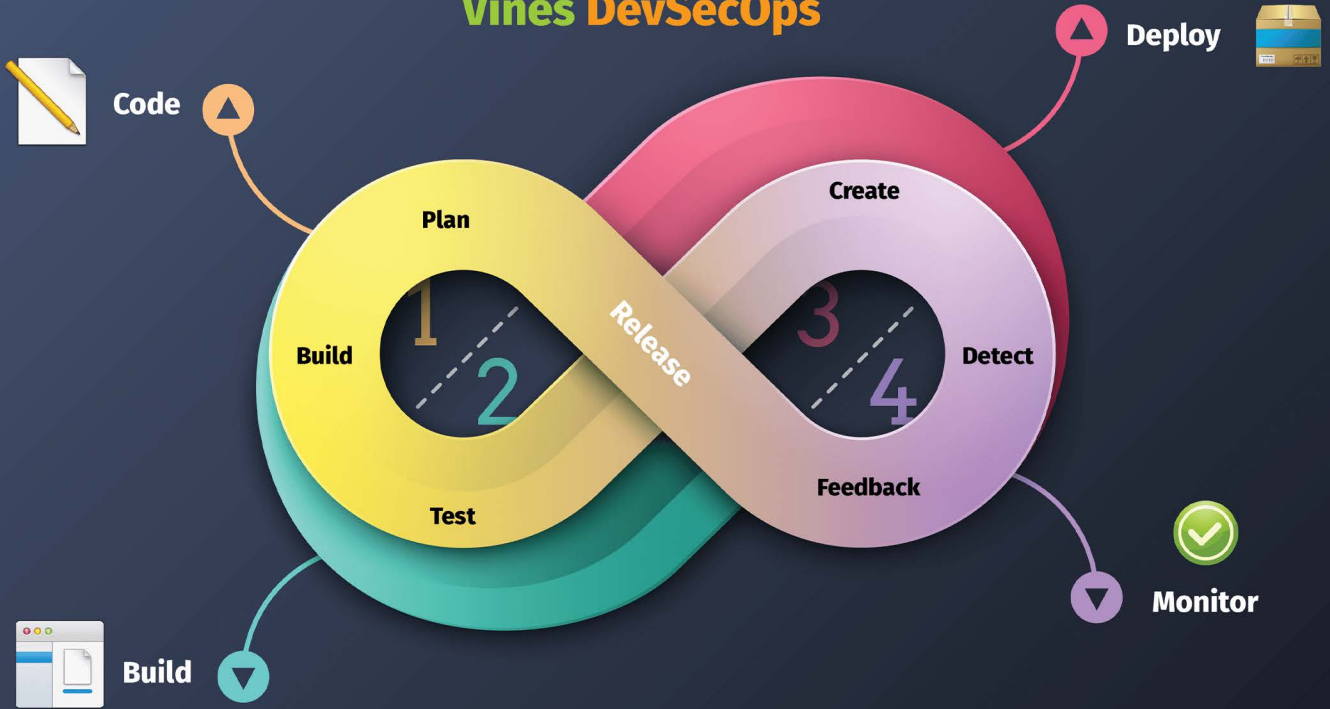
Our **Vulnerability Vines** product proudly boasts a cutting-edge **Incident Response** feature designed to ensure your organization's digital infrastructure is protected at all times.

With Incident Response, you can swiftly identify, assess, and remediate any security breaches or potential vulnerabilities in your systems.

Our user-friendly interface makes it easy to track and manage incidents, ensuring a quick and efficient resolution. Stay ahead of **cyber threats and maintain the highest level of security for your business with Vulnerability Vines' unparalleled Incident Response capabilities.**



Vines DevSecOps



Robust DevSecOps Integration

Embrace the **power of seamless DevSecOps with Vulnerability Vines, ensuring robust security throughout your development lifecycle.**



Why Vines

Ransomware

Misconfigurations



Insider Attacks

Lack of Patches

Upgrade your security, downgrade your threats.

Our innovative product integrates flawlessly with **your existing DevOps pipeline, enabling continuous security assessments and proactive vulnerability management.** With Vulnerability Vines, you get a comprehensive view of your security posture, automated remediation guidance, and real-time risk analysis.

Stay ahead of threats and ensure **the highest level of protection for your applications, infrastructure, and data with our cutting-edge DevSecOps feature.**

Experience unparalleled security, compliance, and efficiency with Vulnerability Vines – your ultimate DevSecOps partner.



Comprehensive Cloud Security Assessment

Safeguard your cloud infrastructure with our **advanced Cloud Security Assessment feature**.

This essential component of Vulnerability Vines product is **designed to identify and mitigate potential security risks** in your cloud environment, ensuring the safety and integrity of your data and applications.

Our expert-driven approach combines automated scanning with manual testing to provide a thorough evaluation of your cloud security posture.

Gain critical insights into misconfigurations, access control issues, and other vulnerabilities that may expose your organization to cyber threats. **With our Cloud Security Assessment, empower your business with the confidence to operate securely and efficiently in the cloud.**

The screenshot shows the Vines Manager interface with a list of findings. The interface includes a navigation bar with options like Assets, Findings, Scans, Engines, Alerts, and Rules, along with a search bar and a user profile for 'admin'. The findings list is as follows:

Asset	Title	Severity	Status	From	Last update	Actions
10.31.112.21	Microsoft Windows SMB Service Detection	Info	new	NESSUS	2023-03-21	[Info] [Close] [X]
10.31.112.21	DCE Services Enumeration	Info	new	NESSUS	2023-03-21	[Info] [Close] [X]
10.31.112.21	Windows NetBIOS / SMB Remote Host Information Disclosure	Info	new	NESSUS	2023-03-21	[Info] [Close] [X]
10.31.112.21	Microsoft Windows SMB NativeLanManager Remote System Inform...	Info	new	NESSUS	2023-03-21	[Info] [Close] [X]
10.31.112.21	Microsoft Windows SMB Log In Possible	Info	new	NESSUS	2023-03-21	[Info] [Close] [X]
10.31.112.21	Nessus SYN scanner	Info	new	NESSUS	2023-03-21	[Info] [Close] [X]
10.31.112.21	Microsoft Windows SMB Registry : Nessus Cannot Access the W...	Info	new	NESSUS	2023-03-21	[Info] [Close] [X]
10.31.112.21	Nessus Windows Scan Not Performed with Admin Privileges	Info	new	NESSUS	2023-03-21	[Info] [Close] [X]
10.31.112.21	Traceroute Information	Info	new	NESSUS	2023-03-21	[Info] [Close] [X]
10.31.112.21	Host Fully Qualified Domain Name (FQDN) Resolution	Info	new	NESSUS	2023-03-21	[Info] [Close] [X]
10.31.112.21	Inconsistent Hostname and IP Address	Info	new	NESSUS	2023-03-21	[Info] [Close] [X]
10.31.112.21	Service Detection	Info	new	NESSUS	2023-03-21	[Info] [Close] [X]
10.31.112.21	SMB Signing Disabled	Medium	new	NESSUS	2023-03-21	[Info] [Close] [X]

Attack Statistics

Password Brute-force

124,334 +21%

Threats detected today

Threat Categories

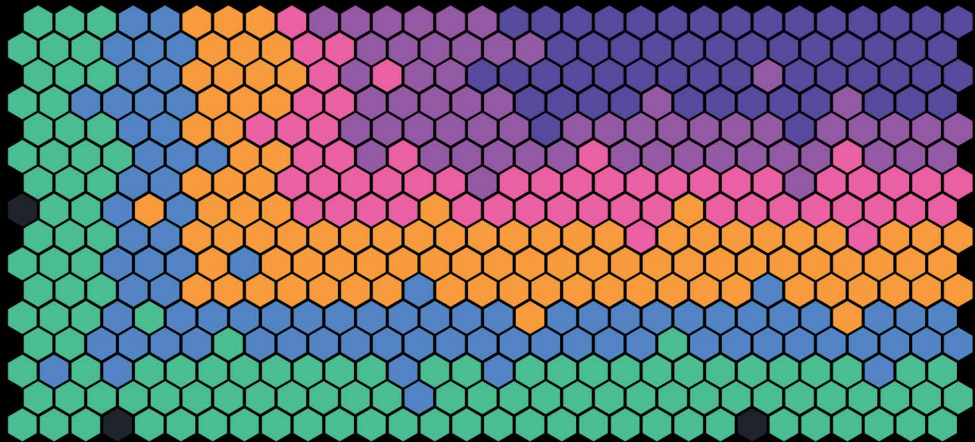
DDOS	PHP	Backdoors
34,00	83,666	93,845



Total: 734,003 +21%

Vines Attack Dashboard

🚫 Low Security Alert
🚫 High Security Alert
🚫 Critical Security Alert



1W 1M 3M 1Y ALL



Robust Compliance Management

In today's highly regulated digital landscape, **ensuring compliance with industry standards is a top priority for organizations of all sizes.**

That's why Vulnerability Vines is designed to help you effortlessly manage and maintain compliance with the leading regulatory frameworks: **PCI, NIST-53, GDPR, and HIPAA.**



Our comprehensive solution streamlines the process of identifying, tracking, and addressing potential vulnerabilities, enabling you to stay one step ahead of the ever-evolving compliance landscape.

With **Vulnerability Vines' robust compliance management feature, your organization can easily assess and align its security posture with industry-specific regulations, reducing the risk of non-compliance penalties and reputational damage.** Our automated solution saves time and resources by simplifying the process of tracking and updating your compliance status across multiple frameworks.

Our platform empowers your team with actionable insights and recommendations, enabling them to prioritize and address vulnerabilities more efficiently.

You can gain peace of mind knowing that your sensitive data is protected and that your organization's security practices are up to date with the latest regulatory requirements.

Stay ahead of the compliance curve with Vulnerability Vines, and safeguard your organization's reputation, customer trust, and financial stability.



Web Application Firewall for Unmatched Security

Safeguard your online presence with our **advanced Web Application Firewall (WAF) feature, integrated into the Vulnerability Vines platform.**

Our WAF is designed to provide robust and comprehensive protection for your **web applications against a wide range of threats, including SQL injection, cross-site scripting, and other malicious attacks.**

By continuously monitoring and analyzing web traffic, our WAF intelligently detects and blocks any suspicious activities, ensuring that your website remains secure and your data stays protected.

With an easy-to-use interface, customizable security policies, and **real-time alerts, you can gain complete control over your web application's security and stay one step ahead of evolving threats.**



SOAR CORTEX



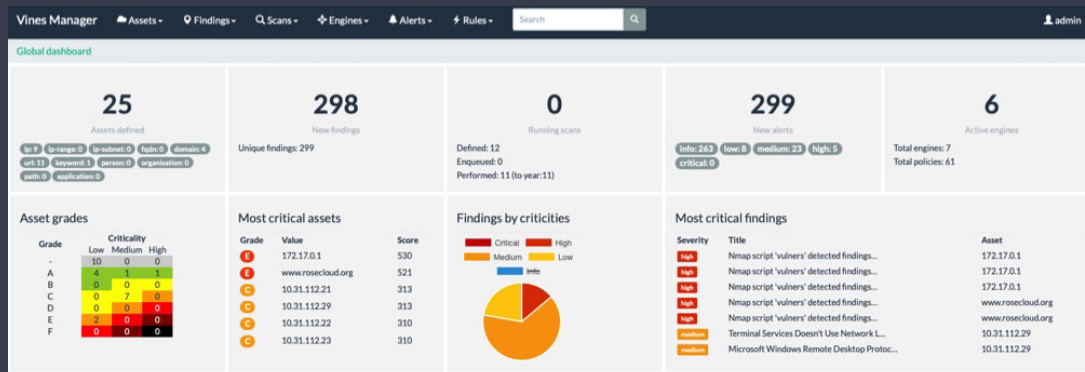
SOAR: Secure, Optimize, Analyze & Respond

Empower your cybersecurity with our cutting-edge SOAR feature - Secure, Optimize, Analyze, and Respond.

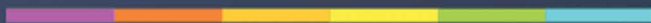
Designed to amplify the efficiency and effectiveness of your vulnerability management, **SOAR is an intelligent integration within our vulnerability vines product that automates and enhances your security operations.**

With SOAR, you can streamline threat identification, accelerate incident response, and safeguard your digital assets against ever-evolving cyber threats.

Unleash the full potential of your security team and stay a step ahead of **attackers with vulnerability vines and SOAR - your ultimate defense against cyber threats.**



Vulnerabilities



Broken Access Control

20%



Cryptographic Failures

25%



Insecure Design

10%



Security Misconfiguration

15%

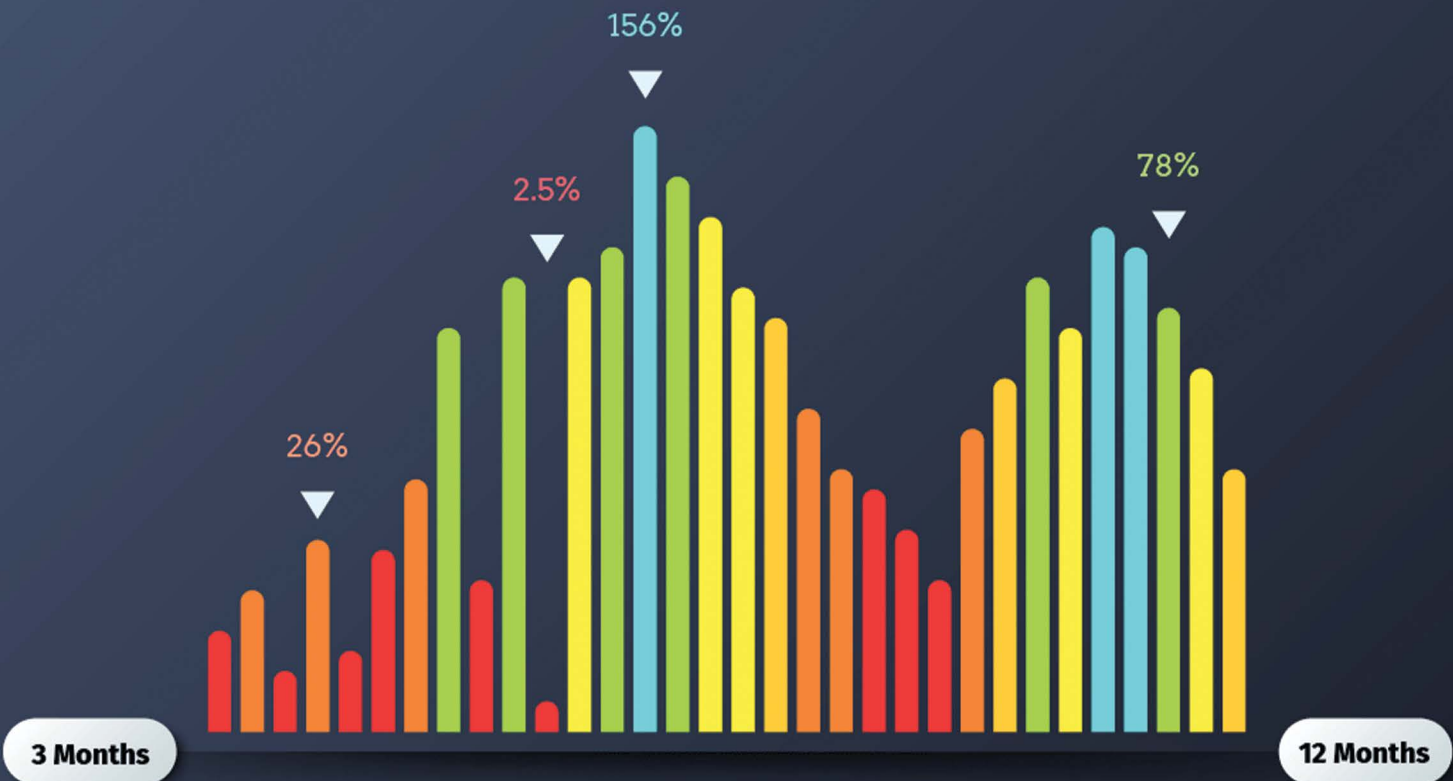


30%



Outdated Components

Threat Levels



High



Medium



Low



Info

Patch Management for Optimal Security

Our vulnerability vines product brings you the powerful feature of Patch Management, designed to effectively address security vulnerabilities and enhance the overall protection of your digital infrastructure.

This advanced functionality **automates the process of detecting, assessing, and deploying vital patches to your systems, ensuring that you always stay ahead of potential threats.**

With our streamlined Patch Management system, you can confidently maintain the integrity of your network while minimizing risks and maximizing productivity.

Experience a seamless and secure environment with the cutting-edge solution that vulnerability vines has to offer.

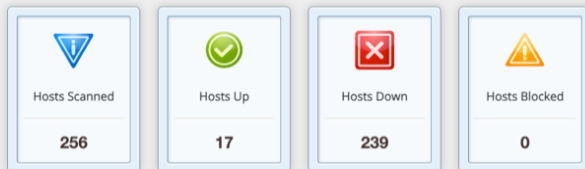


Comprehensive **Vulnerability Management**

Our Vulnerability Management feature offers an all-encompassing solution to identify, assess, and remediate potential security threats in your digital ecosystem.

NETWORK DISCOVERY REPORT

Scan date: Sun Apr 30 06:39:53 2023



256 hosts scanned. 17 hosts up.

17

With our cutting-edge technology, **we continuously monitor and analyze your systems, networks, and applications, ensuring that vulnerabilities are detected and addressed** before they can be exploited by cybercriminals.

By prioritizing risk levels and streamlining remediation processes, our Vulnerability Management feature empowers your organization to maintain a strong security posture, safeguarding your critical assets and data from cyber threats.

Stay ahead of the curve and protect your organization with our proactive and intelligent Vulnerability Management solution.

MONITORING

MANAGEMENT

SETUP

NETWORK

DATABASE

LOGS

HELP

LOG

Processing

```

>> [16/05/2020] -- Progressive monitoring
>> 18:32
-----
natoque penatibus et
  magnis dis parturient montes,
  nascetur ridiculus mus.
- sector 3X-3B-5A-7T-9D
Maecenas accumsan sapien sed cursus ultricies.
Mauris molestie sodales cursus.
-----
>> [16/05/2020] -- Progressive monitoring
>> 18:34
-----
Nunc ultrices porttitor quam eu consectetur. Nunc ultrices porttitor quam eu consectetur
> ____Ut sed tempor neque.
-----
Mauris molestie sodales cursus.
--Input.
  Donec sollicitudin ullamcorper mi.
-----
>> [16/05/2020] -- Progressive monitoring
>> 18:34
-----
Quisque in aliquam est.
Quisque sed commodo lorem.
  Proin quis tempus mauris. - sector 3X-3B-5A-7T-9D
  Fusce auctor sapien sed congue sagittis.
-----
>> [16/05/2020] -- Progressive monitoring
>> 18:34

```

Station 1
Station 2
Profile c33
Profile c33
Profile c33
Station 1
Station 2
Station 3
Profile c33
Profile c33
Profile r87
Profile r87
Eng s55
Eng s55
Eng s77

Setting

General:

- Input latency: 100ms
- Memory: 2048mb
- Units: Metric

Network:

- Workgroup: SES-008
- Securit: 256-bit encryption
- Firewall: enabled
- AdvSec: enabled
- IP status: Static

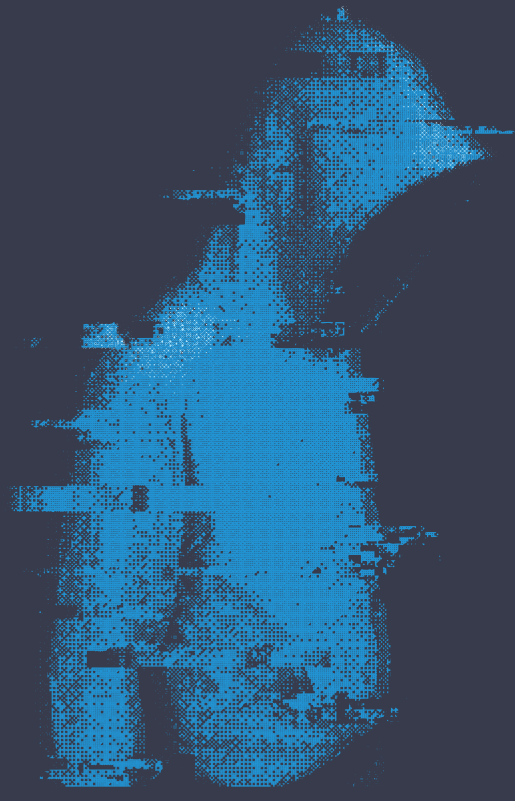
Time and Date:

- Time zone: +2:00
- Date Format: dd/mm/yy
- 24H: enabled
- Time Format: 00:00:00

Monitoring Options:

- Refresh Rate: 100
- Sensors buffer: 1024

Cyber Wargames **Red Team / Blue Team Exercises**



Unleash the power of friendly competition to bolster your **organization's cyber defenses with our Red Team / Blue Team Exercises feature**, an integral part of our Vulnerability Vines product suite.

This immersive and interactive training experience pits two opposing teams against each other, simulating real-world cyber-attack and defense scenarios to identify and fortify potential weaknesses in your security infrastructure.

The **Red Team, our skilled and certified ethical hackers, will emulate the tactics, techniques, and procedures of real-world adversaries**, attempting to infiltrate your organization's network, applications, and systems.

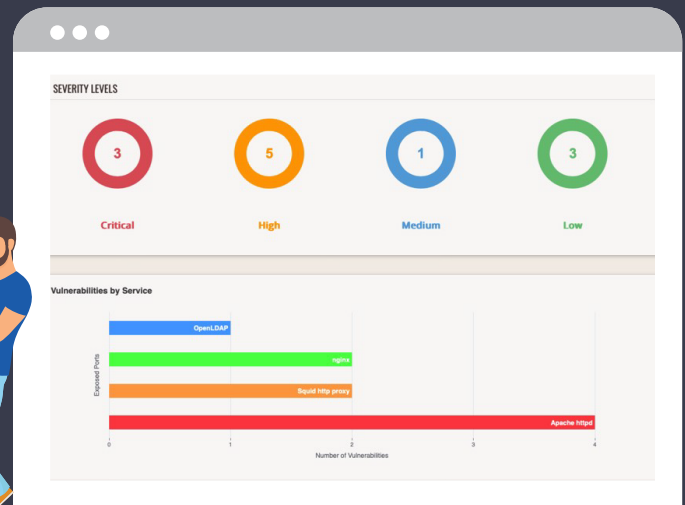
Simultaneously, the **Blue Team, comprising your in-house security personnel, will work tirelessly to detect, respond, and mitigate these simulated attacks**, honing their skills and testing the robustness of your security measures.

Container Security for Uncompromised Protection

Secure your Docker and Kubernetes containerized applications with **our advanced Container Security feature, tailored to provide uncompromised protection for your infrastructure.**

Experience seamless integration with **your CI/CD pipeline, ensuring vulnerabilities are detected and addressed early in the development process.**

Our Container Security solution offers continuous **monitoring and protection for both Docker and Kubernetes environments**, giving you complete visibility and control over your container ecosystem.



Embrace the power of containerization with confidence, knowing that our state-of-the-art technology shields your applications from risks and empowers you to maintain a secure and compliant ecosystem.

Attack Surface Management

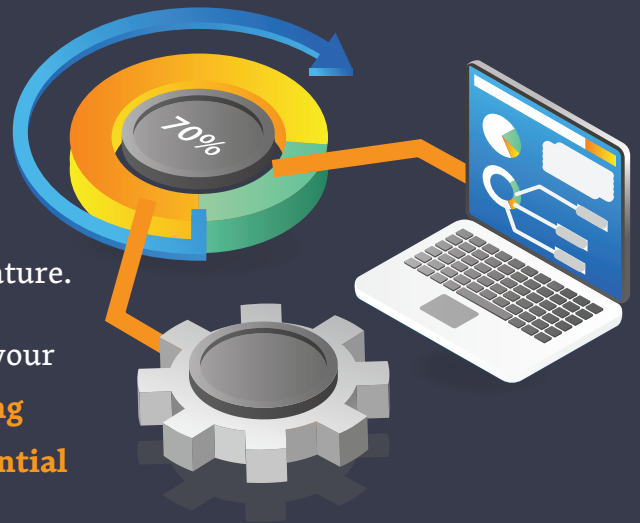
In today's ever-evolving digital landscape, securing your organization's network and data assets is a top priority.

With our **Vulnerability Vines** product, you can now effectively manage and secure your entire attack surface with our comprehensive Attack Surface Management feature.

This advanced solution continuously monitors your organization's digital infrastructure, **identifying vulnerabilities, misconfigurations, and potential threats in real-time.**

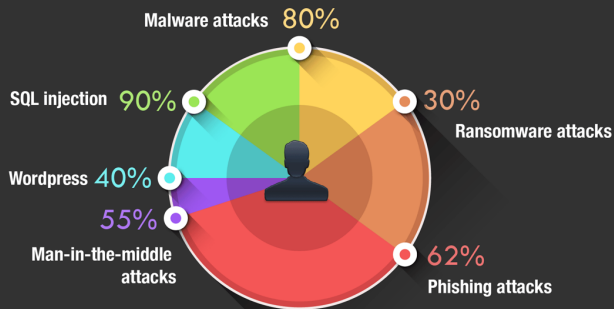
With a holistic view of your network, our Attack Surface Management empowers you to proactively assess, prioritize, and remediate security risks, ensuring a robust defense against cyberattacks.

Don't leave your organization exposed – **choose Vulnerability Vines for end-to-end security and peace of mind.**



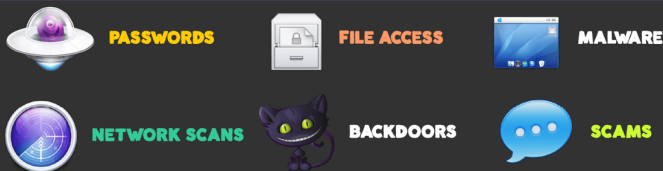
Zero-Trust Architecture

Vulnerability Vines is a cutting-edge **cybersecurity product that incorporates the zero-trust model to provide robust protection** against various cyber threats.



The zero-trust approach is a **key feature of the product, ensuring that no entity, whether internal or external, is granted automatic access to the network or resources.**

The zero-trust feature of Vulnerability Vines product revolves around the principle of "never trust, always verify." This means that all users, devices, and applications must be authenticated and authorized before gaining access to any part of the network.



By implementing the zero-trust model, Vulnerability Vines ensures that potential attackers can't exploit any inherent trust within the system, making it much harder for them to access critical data and resources.





- HOME
- LATEST CVE VULNERABILITIES
- VINES ATTACK MAP
- QUICK SCAN
- MANAGED SCAN



SERVICES

 Asset Discovery Launch	 Vines Manager Launch	 Application Deepscan Launch	 Vines Firewall Launch
 Red Team Blue Team	 Vulnerability Database	 Attack Map	 Wazuh EDR
 Monkey Island	 SSH Shell	 Threat Intelligence	 Live Threats
 Incident Response	 SOAR Cortex	 Mitre Attack Visualizer	 DevSecOps Jenkins

Vines Firewall Dashboard

Today's Stats

- SQL Attacks: 0
- Bad Bots: 0
- Proxies: 0
- Spammers: 0

Overall Statistics

Threat Statistics

Threat Type	Count
SQL INJECTIONS	1
BAD BOTS	0
PROXIES	0
SPAMMERS	0

Protection Modules

Module	Status
SQL Injection Protection	ON
Bad Bots Protection	ON
Proxy Protection	OFF
Spam Protection	OFF

Logging Settings

Module	Status
SQL Injection Logging	ON
Bad Bots Logging	ON
Proxy Logging	ON
Spam Logging	ON

VULNERABILITY VINES DASHBOARD

HOME | LATEST CVE VULNERABILITIES | LIVE VINES ATTACK MAP | QUICK SCAN | MANAGED SCAN

IP Address	Type of Attack	Port	Country
83.56.46.145	CVE-2023-0041 Stack Overflow in PHP	25 SMTP	USA
158.54.252.230	CVE-2023-0019 Buffer Overflow in BIND	80 HTTP	USA
10.96.162.149	CVE-2023-0042 Cross-site Scripting in Java	123 NTP	USA
92.122.12.103	CVE-2023-0055 Buffer Overflow in Perl	123 NTP	USA

SERVER STATISTICS

Vines Manager

Assets | Findings | Scans | Engines | Alerts | Rules

admin

Global dashboard

25 Assets defined | 298 New findings | 0 Running scans | 299 New alerts | 6 Active engines

Info: 243 | low: 8 | medium: 23 | high: 5 | critical: 0

Total engines: 7 | Total policies: 61

Asset grades

Grade	Criticality		
	Low	Medium	High
-	10	0	0
A	4	1	1
B	0	0	0
C	0	7	0
D	0	0	0
E	2	0	0
F	0	0	0

Most critical assets

Grade	Value	Score
E	172.17.0.1	530
E	www.rosecloud.org	521
C	10.31.112.21	313
C	10.31.112.29	313
C	10.31.112.22	310
C	10.31.112.23	310

Findings by criticalities

Most critical findings

Severity	Title	Asset
High	Nmap script 'vulners' detected findings...	172.17.0.1
High	Nmap script 'vulners' detected findings...	172.17.0.1
High	Nmap script 'vulners' detected findings...	172.17.0.1
High	Nmap script 'vulners' detected findings...	www.rosecloud.org
High	Nmap script 'vulners' detected findings...	www.rosecloud.org
High	Nmap script 'vulners' detected findings...	10.31.112.29
Medium	Terminal Services Doesn't Use Network L...	10.31.112.29
Medium	Microsoft Windows Remote Desktop Proto...	10.31.112.29

Asset group grades

Grade	Criticality		
	Low	Medium	High
-	1	0	0
A	0	0	0
B	0	0	0
C	0	0	0
D	0	0	0
E	0	0	0
F	0	0	0

Most critical asset groups

Grade	Name	Score
-	New URLs	0

Last scans

Title	Findings	Status	Date
nessus_2023-03-21	213	Finished	2023-03-07 12:10:54
Scan Haja.me Website	10	Finished	2023-03-03 10:21:15
Haja Domain	10	Finished	2023-03-03 08:39:01
Scan Vines Website	10	Finished	2023-03-03 08:29:05
Rosecloud Scan	25	Finished	2023-03-03 07:52:13
Juggypshop Scan	2	Error	2023-03-03 07:52:13

Top CVSS Score / Findings

#CVSS = 10: 0
 9.0 <= #CVSS < 10: 0
 7.0 <= #CVSS < 9.0: 5
 5.0 <= #CVSS < 7.0: 14
 #CVSS < 5.0: 280

Top CVE

CVE-2005-1794: #5 | CVE-2006-20001: #5 | CVE-2021-44224: #5 | CVE-2022-22719: #5
 CVE-2022-22720: #5 | CVE-2022-22721: #5 | CVE-2022-23943: #5 | CVE-2022-26377: #5
 CVE-2022-28614: #5 | CVE-2022-28615: #5

Top CWE

VINES ATTACK MAP

1:22:35

ATTACK VECTORS

1246305



```
Indonesia (52.230.191.204) attacks Australia (220.4.150.201) (Ping of Doom)
United States (230.59.100.1) attacks Ethiopia (251.247.101.71) (SNAILshock)
Canada (196.87.215.60) attacks Japan (225.22.162.110) (Conficker)
United States (4.136.52.119) attacks United States (43.69.172.145) (Po_ODLE)
China (52.128.19.160) attacks China (45.229.28.155) (Ping of DDoM)
Egypt (178.141.208.232) attacks EL Salvador (96.238.76.90) (Conficker)
Germany (35.108.132.31) attacks Argentina (151.129.37.136) (Po_ODLE)
United States (113.69.246.243) attacks United States (56.102.179.72) (CORGI Attack)
Canada (122.9.182.31) attacks Bolivia (186.207.134.236) (Conficker)
Gambia (124.191.24.173) attacks China (240.59.20.200) (SMILshock)
China (132.178.73.142) attacks China (208.180.210.217) (Thought Leader Tweet)
Brazil (165.119.9.223) attacks Oman (27.254.7.114) (Sharknado)
Iceland (68.82.21.136) attacks Greenland (38.26.201.251) (Spotty)
```





<https://cert.rocheston.com/security-operations-center/>

ROCHESTON®