



MITIGATOR™
VULNERABILITY & THREAT MANAGER

VULNERABILITY & THREAT MANAGER

Mitigator is a Vulnerability and Threat Management Platform for Network, Cloud and Web Applications that makes tracking and remediating vulnerabilities easier.

305-921-3871

INFO@MITIGATORVM.COM

The centralized console allows you to analyze and track vulnerabilities, track threat trends and schedule remediation. The fact is some vulnerabilities can't be fully remediated and must be managed. Additionally, many applications today leverage open-source code. The Cloud and AI will bring new threats at velocity and zero days vulnerabilities will persist and assist Organized Cybercrime in monetizing threats. Mitigator offers an interactive remediation management tool, streamlines reporting, and enhances the overall value of our assessments. It's versatile, serving both ad-hoc and ongoing assessment needs.

Unlike off-the-shelf solutions, Mitigator is a white glove service, setting a new standard by offering comprehensive support and active involvement in the entire vulnerability management process.

WHITE GLOVE SERVICES!



Pen Test Assist – Whether a' la' carte, or as part of our Enterprise Subscription, allow us to attempt that exploit and provide the results you need to accurately quantify the risk!



Remediation Assist – Not enough time in the day for remediation, or maybe a different skill is needed? No worries allow us to step-in and harden your environment when you need it most!



Virtual ISO (vISO) Assist – Auditors or Cyber Insurance Carriers asking for deliverables you don't have or need assistance with? Or maybe your new to the ISO role and just need some coaching. Our vISO's have decades of experience in regulated industries and can advise you on the best path forward, and even assist with the deliverables themselves!

MULTIPLE MSP REVENUE OPPORTUNITIES

- » Create a new Managed Service by offering Vulnerability Management as a Service (VMaaS).
- » Deliver one-time Cybersecurity Assessment consulting services.
- » Resell Mitigator as a Vulnerability Management platform to larger clients with in-house IT staff.
- » Become a Reseller or Referral Partner



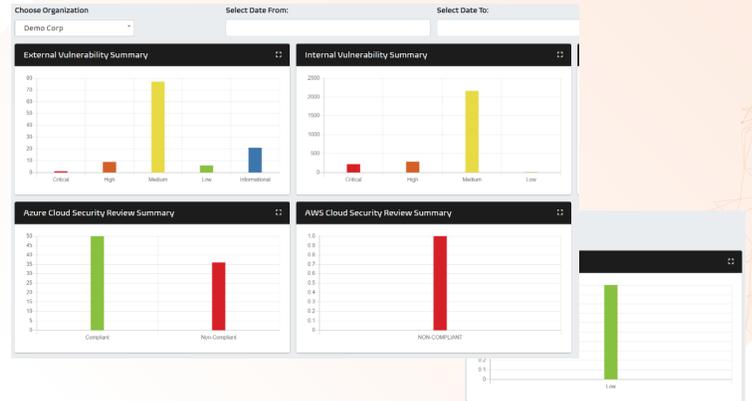
DESIGNED WITH MSPS IN MIND!

- » White labeling allows you to brand the platform as your own!
- » Reporting branded for your MSP! See all your clients' vulnerabilities for multiple instances in one single pane of glass.
- » Multi-tenant environment with isolated databases.



ATTACK THREATS HEADS-ON!

WWW.MITIGATORVM.COM

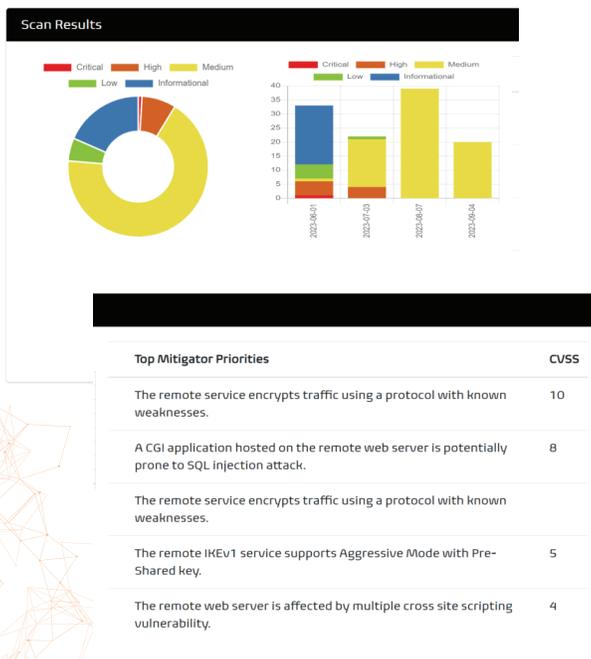


BENEFITS INCLUDE:

- ✔ Spot Vulnerabilities and track remediation quicker.
- ✔ Achieve higher patch compliance levels. Run Authenticated scans to compare to Patch Management reports.
- ✔ Improves your defense posture to create cyber resiliency.
- ✔ Prevents the potential for lateral movement during a compromise.
- ✔ Reduces your attack surface.
- ✔ Stops duplicate findings on reports where remediation is complete to the highest level

FEATURES INCLUDE:

- A Centralized Dashboard to analyze vulnerabilities, track trends and schedule remediation.
- Create Remediation tickets in your RMM with the click of a button.
- Request “on-demand” Pen Testing of vulnerabilities.
- Request Remediation Assistance
- Analyze vulnerabilities by asset and criticality.
- Export vulnerability data by date, source, criticality etc.
- Search for specific time periods and vulnerabilities.
- Search by criticality
- Adjust risk scores based upon context and compensating controls to create accurate risk reporting.
- Executive level reporting for 3rd parties and upper management and technical reporting with data exporting



Cybersecurity Assessment

Executive Summary Report

Executive Summary

Scope of Work

Methodology Stat

Penetration Test A

Risk Level Ratings

Composite Risk Rating

External Vulnerabilities

Next Steps

Executive Summary

Client has engaged InfoSight as a security partner to conduct an Information Security Posture review in the form of a Cybersecurity Assessment. The Assessment is a multi-disciplinary, multi-faceted review of the security posture of the company's information systems. The review conforms to regulatory requirements, statutory directives, and security best practices which the company operates under. It

Methodology Statement

The Assessment shall be focused on reviewing the information systems in use by the client and addressing as much as possible the risk of compromise to the network and data. This includes a comprehensive review of the security posture of the company's information systems. The review conforms to regulatory requirements, statutory directives, and security best practices which the company operates under. It

Risk Level Ratings

This level of risk is most serious as it relates to a potential breach in network security. Findings listed as Critical represent the highest level of risk and require immediate attention and remediation. A Critical rating indicates that a single network device is

Next Steps

Immediately following the assessment, Client should create a prioritized remediation plan to address any vulnerabilities identified, starting with critical and high findings first. By remediating the findings listed as Critical, the risk of compromise will be reduced or eliminated. This remediation plan should be implemented as soon as possible. This may involve making changes to the organization's systems, processes, or policies. Additionally, regularly performing security assessments, penetration testing, and implementing security best practices will also strengthen the Client's overall security posture.

Both Technical and Executive Level Reporting in multiple file formats (HTML PDF & Word) for Upper Management, BOD, and external 3rd Parties.