CYBERSAINIK

RISK MANAGEMENT FOR THE MODERN COMPANY:

Vulnerability Management Services

Created by Cyber Sainik

Table of Contents

Mary Anne Gunn

Yazmin Hernandez

Thomas Cumberland

Our Team

Mary Anne Gunn | Chief Marketing Officer

Yazmin Hernandez | Account Manager

Thomas Cumberland | Sr. Lead Analyst

Hadyn Peffer | Moderator & Digital Marketer

About us

CYBERSAINIK

Company History

Est. January 2022

Comprehensive Managed Detection & Response Provider

Simplifying Security Operations for SMEs

24x7x365 human-led, turnkey, modern SOC functions

Company Overview

Offices in Denver (CO), Austin (TX), and Bengaluru (India)

Product development (XDR) scheduled for release in Fall 2023

Provides a comprehensive, enterprise-grade suite of cyber security solutions:

Managed Detection & Response (MDR)

Security Event & Information Management (SIEM)

Penetration Testing

Vulnerability Scanning & Assessments

Virtual CISO

Managed Firewall

Security Training

Multifactor Authentication (MFA)

Driving Factors: Macro Trends in Cybersecurity

The Human Element

2025: Lack of talent/human failure responsible for more than ½ of significant incidents

Today: Worldwide, open jobs grew 350% (2013 -2021), from 1 million to 3.5 million, problem continues to worsen

Consolidation & Simplification

2025: 60% of orgs will be using threat detection & containment by MDR providers, up from 30% today (Gartner)

2023: 80%+ of orgs will have completed an XDR project to reduce vendor complexity (Gartner)

SMEs Underserved & Under Attack

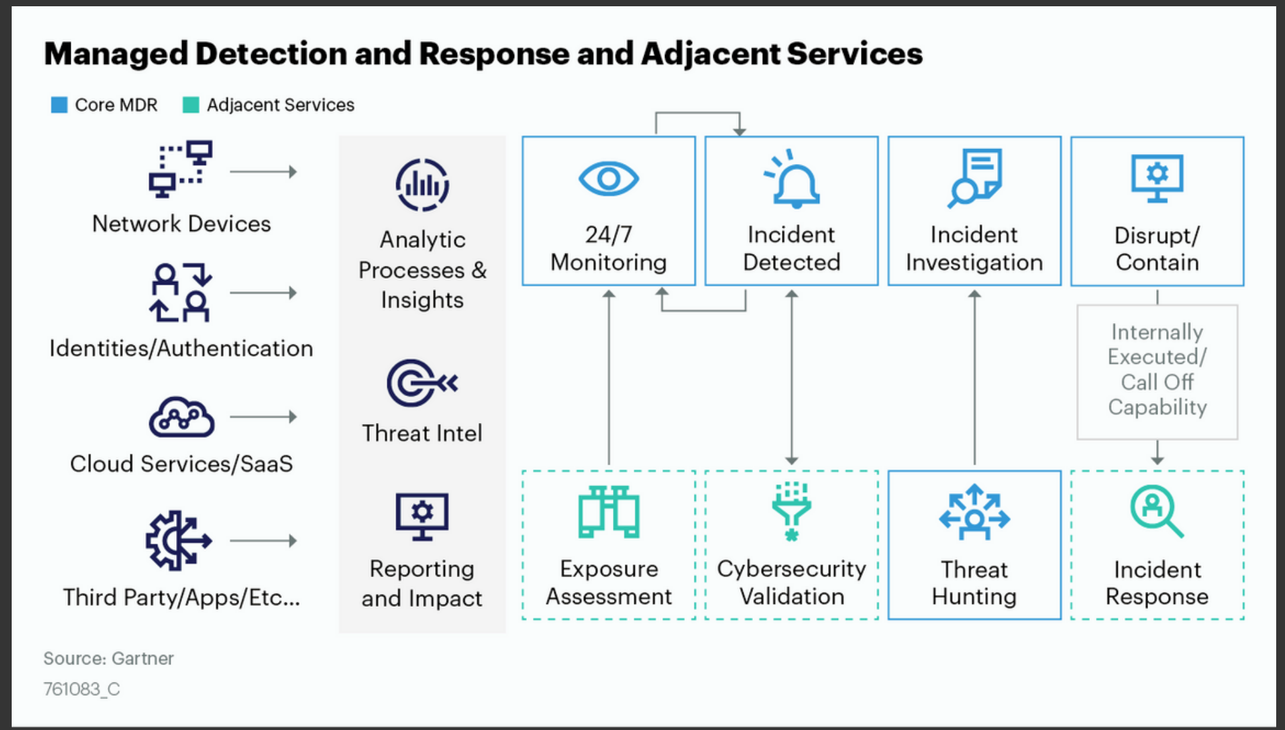
46% of attacks target orgs with fewer than 1000 employees

75% could not continue after a ransomware attack

2021: 700K small and medium enterprise attacks, totaling $2.8B in damages

Managed Detection & Response (MDR)

- Remotely-delivered, human-led security operation capabilities
- Extension of your team and resources

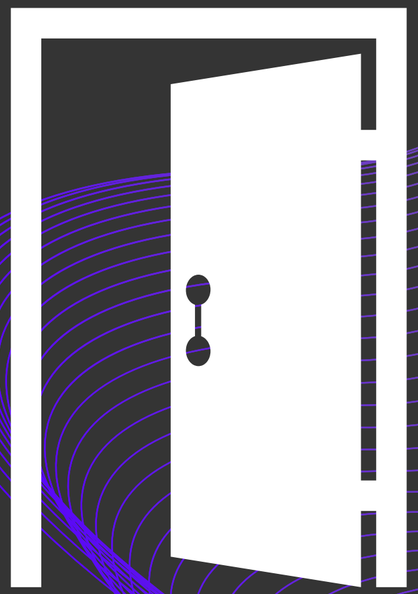


Gartner

- Qualifications:
  - Tier 1-3 analysts
  - Virtual CISO
  - 24x7x365
- Thomas went to India for a month to train the India team hands-on

Our Security Operations Team

What is a vulnerability?



Vulnerability Management (VM)

MDR & VM

Why are they like milk & cookies? Why are they two peas in a pod?

WHAT WE HEAR FROM SMEs

Unsure where to start

Unsure of the value of VM

Lacking manpower

Lacking expertise

Vulnerability Management (VM)

DEFINED

A vulnerability management (VM) program is an ongoing process of identifying, assessing, and mitigating vulnerabilities in an organization's assets to reduce the risk of exploitation.

METHOD

Cyber Sainik's VM program involves multiple processes, including:

Asset discovery and inventory

Vulnerability scanning and assessment

Risk-based vulnerability prioritization

Active remediation

Configuration and risk management

The Value of VM

Why should your organization incorporate VM to your overall security program?

The Value of VM

- What does it prevent?
  - Identify risks before they become an event
  - Prevents potential and likely attacks

- What are the most common vulnerabilities? What do we generally find?
  - Misconfigurations, delayed security updates…

VALUE

Streamline compliance requirements

Create efficiencies and create money

Continual improvement!

Case Study

- Industry: Retail
- Customer: A non-profit organization whose mission is to support programs that benefit individuals living with developmental disabilities and their families.

PROBLEM

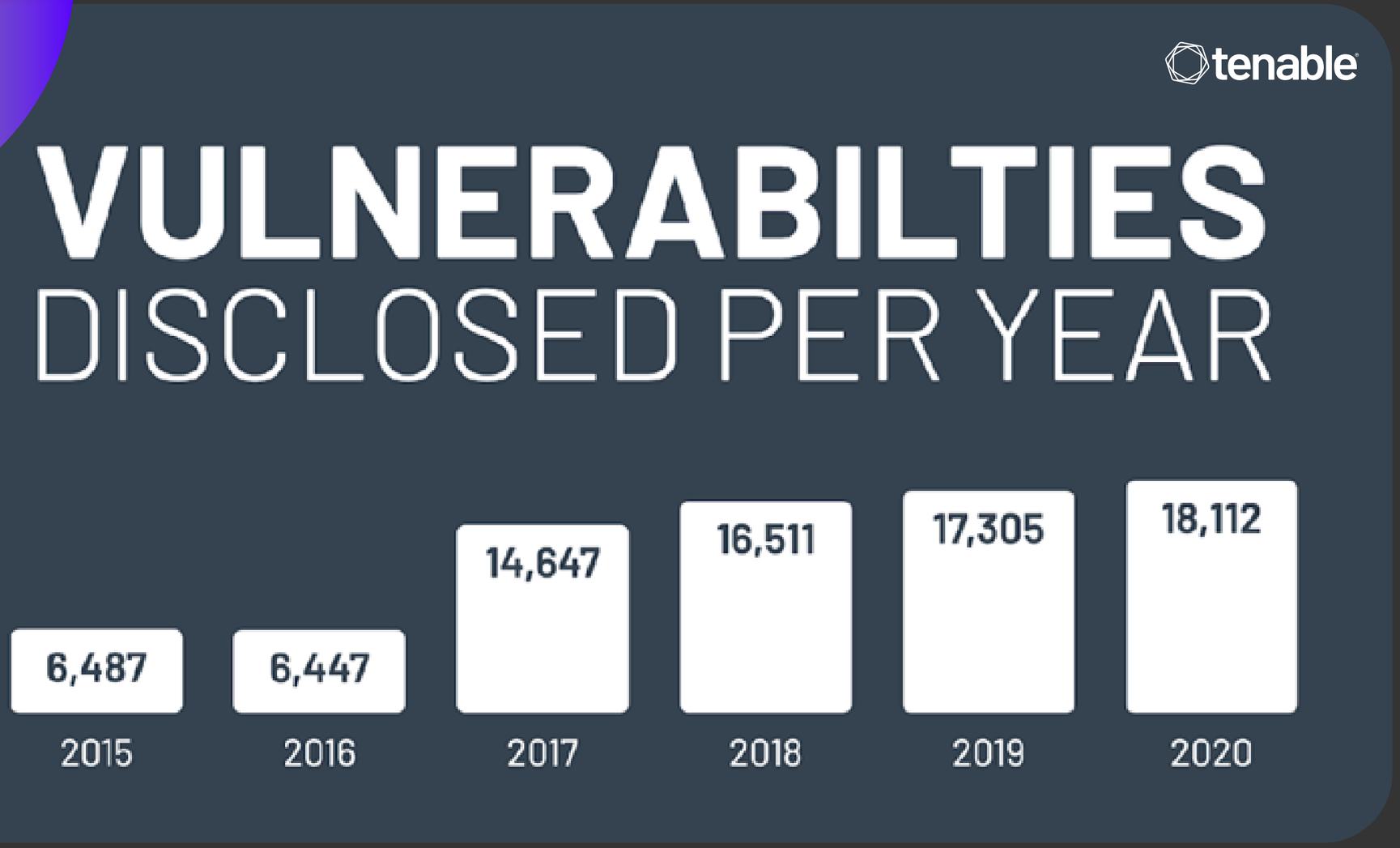
The company faced challenges due to legacy environments, and limited staff. After experiencing a breach in 2021, the customer looked to Cyber Sainik to improve their current cybersecurity approach alongside their existing IT staff.

SOLUTION

Cyber Sainik developed a Solution that would enhance visibility via VM, facilitate business operations, and integrate legacy devices deployed throughout the customer's environment, while also securing critical systems from potential cyber-attacks using next-gen technology.

RESULT

Cyber Sainik developed a co-managed Solution that provided the customer with additional expertise, deep insights into their own environment, proactive threat detection, and improved cybersecurity controls.



Where do these vulnerabilities exist?

Why does the number increase?

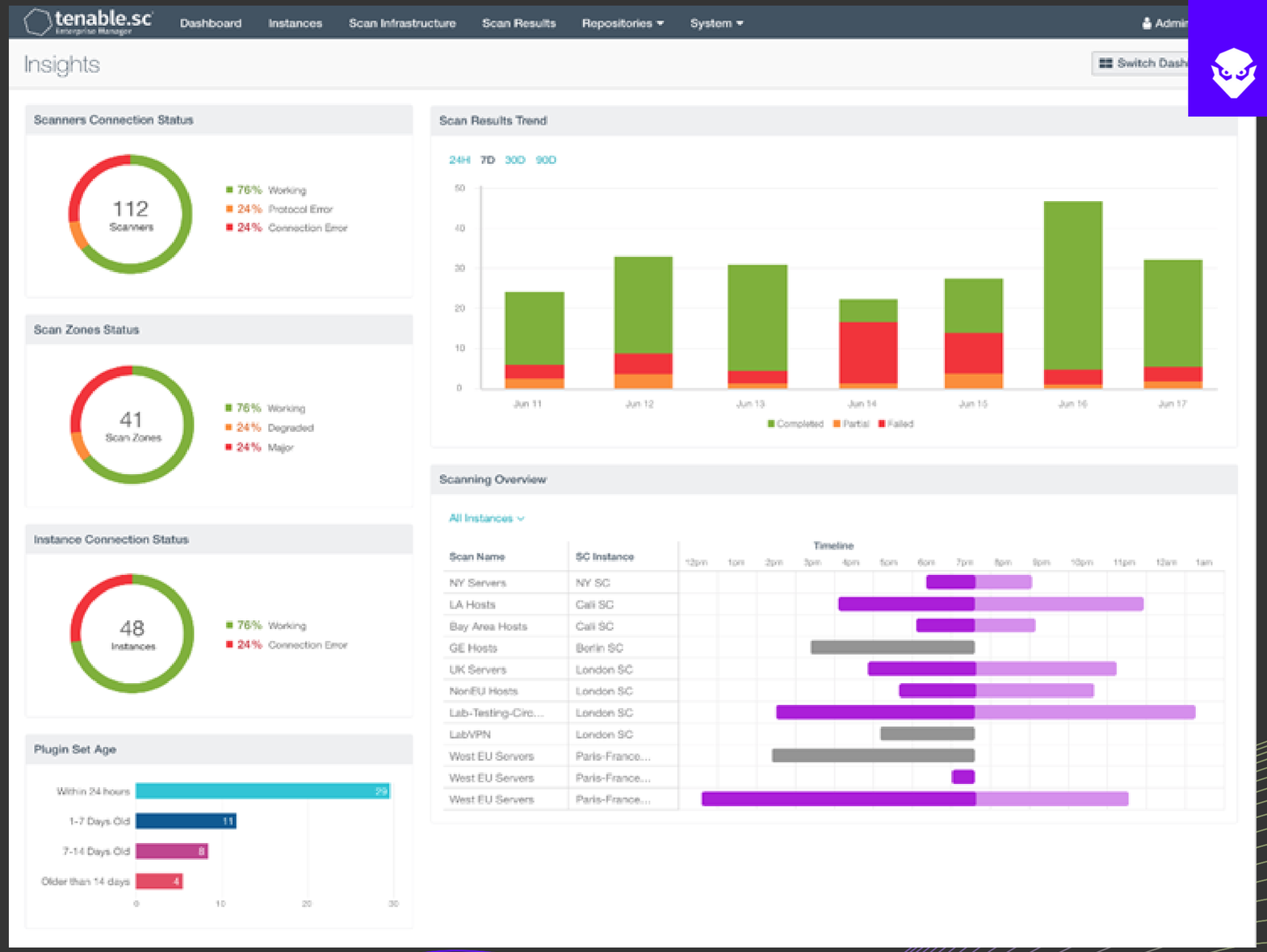
Vulnerability Assessment

Capability	tenable.sc
Centralized vulnerability management with multiple scanners	●
Dynamic asset classification (mail server, web server, etc.)	●
Policy-based configuration auditing	●
Malware detection with built in threat intelligence	●
Pre-defined dashboards and reports with automatic feeds from Tenable	●
Incident response with configurable alerts, notifications, ticketing	●
Assurance Report Cards (ARCs)	●
Predictive Prioritization	●
Solution View page with clear insight into how to reduce risk	●

How we do it?

Security operations center (SOC) expertise, risk-based prioritized list, recommended courses of action

What does it look like?



tenable

What are your next steps?

1. Check out our Complimentary Vulnerability Assessment
   (this link will be shared in our follow-up email)
2. Talk to your team about where you currently stand in your vulnerability management program
3. Consult with Cyber Sainik about areas for improvement
4. Schedule regular assessments!

Questions?

Please now indicate if you have a question you would like answered. Otherwise, please contact us for any other questions!

www.cybersainik.com

303-867-7500

5299 DTC Blvd. Suite 510 Denver, CO 80111

[Webinar] Risk Management Series

- W1: Security as a Service
- W2: Vulnerability Management Services
- W3: Will MDR solve your talent gap?
- W4: What is the future of cybersecurity?