IT NATION™ SECURE

hosted by CONNECTWISE

Measuring & Maturing Your Security Program

Presented by: Anup Ghosh, CEO, ThreatMate

IT NATION™ SECURE

THREATMATE™

INQUISITIVE SECURITY

Agenda

1 Attack Surface Area

2 Inquisitive Security

3 Minimum Security Stack

4 Security Maturity Models

5 Security Metrics

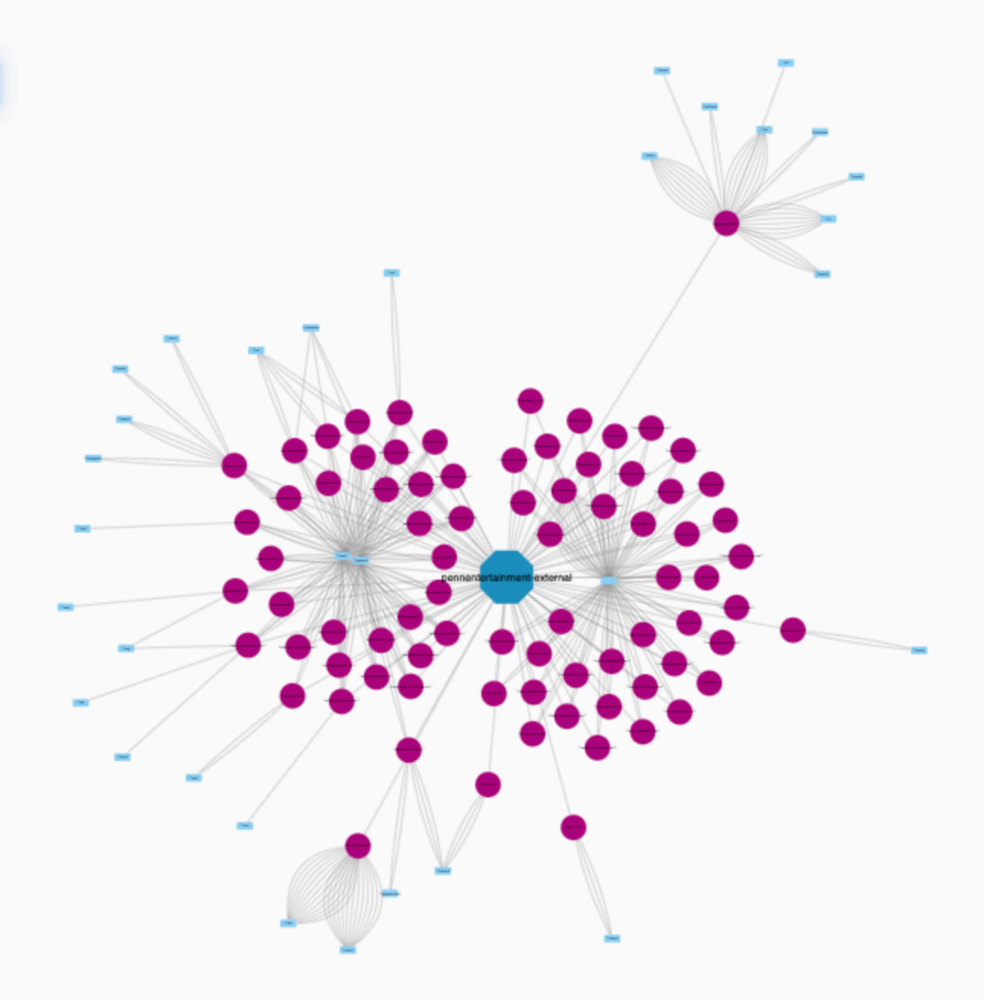
6 Industry Measures of Risk

Your Digital FootPrint is your Attack Surface

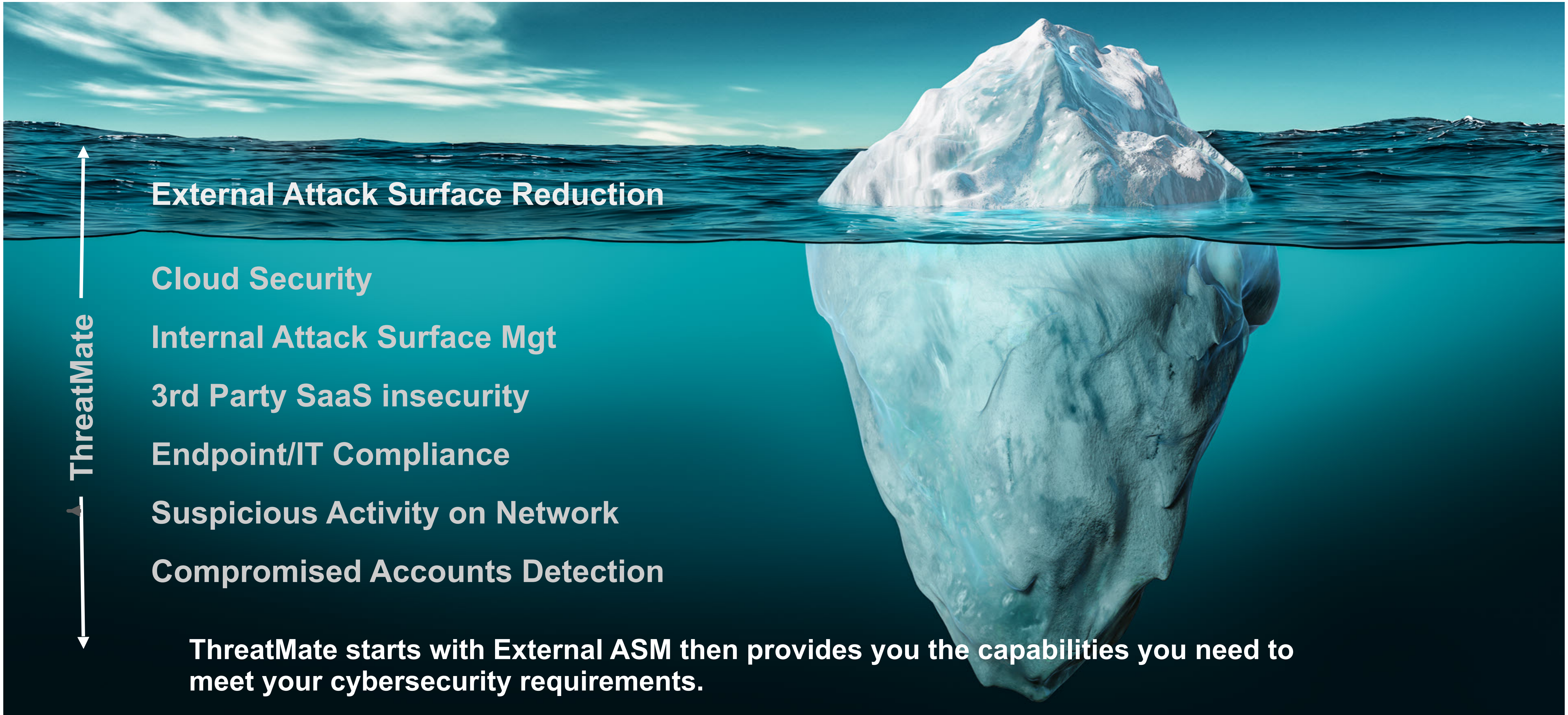
ThreatMate Discovers & Analyzes Your Attack Surface for Vulnerabilities

External Attack Surface (for adversaries) include:

- Second & third level domains (eg www.example1.com, customer1.example1.com…)
- Cloud footprint (AWS, GCP, Azure)
- Customer-facing SaaS instances
- 3rd Party SaaS (CRM, Github, HR, Payroll systems)



The External Attack Surface is the Tip of the Iceberg



ThreatMate

External Attack Surface Reduction

Cloud Security

Internal Attack Surface Mgt

3rd Party SaaS insecurity

Endpoint/IT Compliance

Suspicious Activity on Network

Compromised Accounts Detection

ThreatMate starts with External ASM then provides you the capabilities you need to meet your cybersecurity requirements.

Inquisitive Security

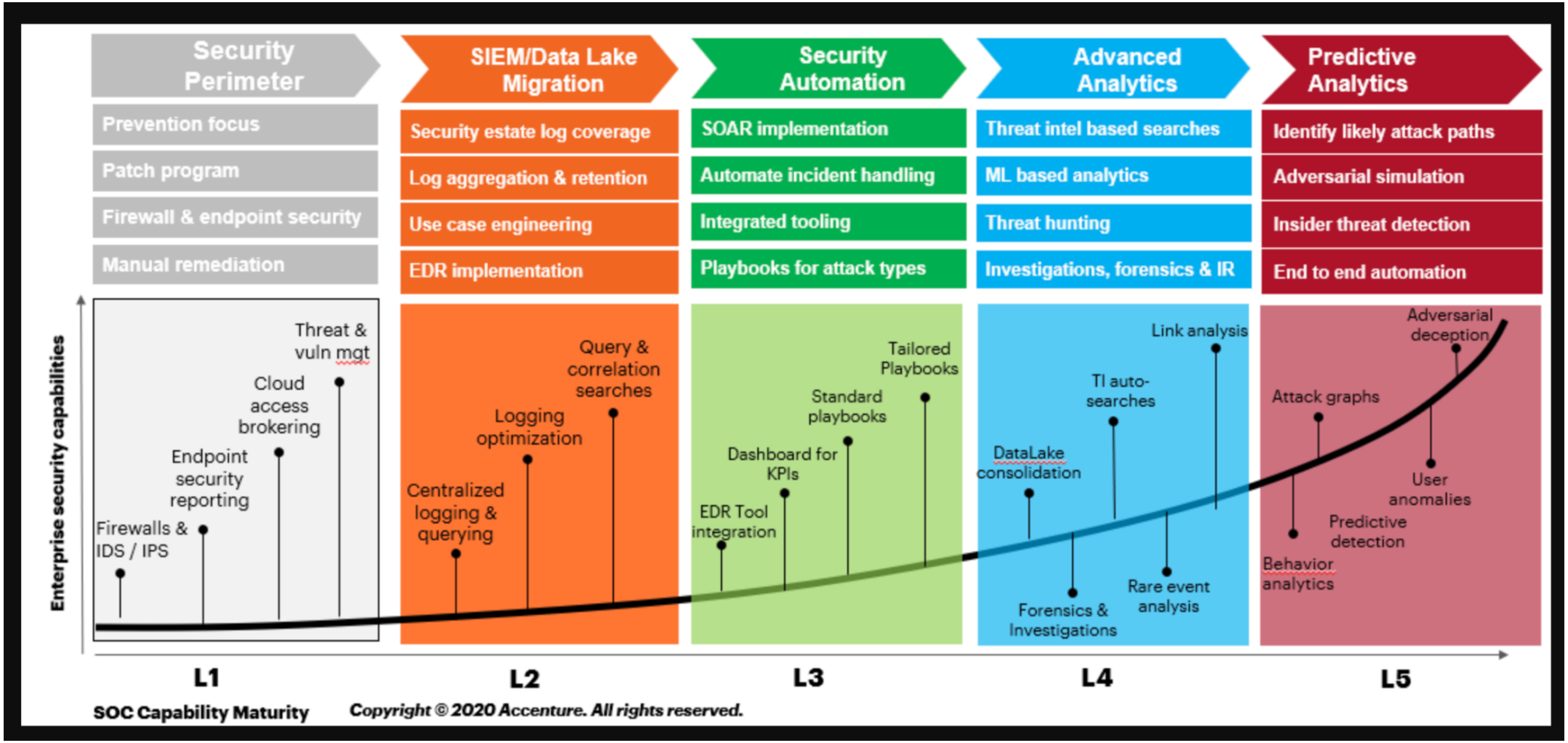
Ask critical questions that are required for Compliance, Cyber Risk Insurance surveys, 3rd party Vendor Surveys

Categories of Risk	Example Questions
Asset Discover/Identification	What new devices have connected to my network in the past week?
Cloud Security	Do I have open storage buckets or other security misconfigurations?
Compliance	Are my devices using Security best practices? Has anything changed since yesterday?
IT Policy	Which of my users do not have MFA enabled?
3rd Party Vendor Compliance	Is my MSP/ecommerce vendor/etc. keeping me secure?
Suspicious Activity	Which machines have initiated network connections directly with another machine on the same subnet? Which have scanned the subnet?
Vulnerability Management	Which browsers are not at their current versions?

Example “Bare Bones” Security Stack for Meeting Compliance

Category	Example Vendor Stack
Pen Testing	Cobalt/ThreatMate
External Attack Surface Mgt	Detectify/Cycognito/ThreatMate
Firewall	PANW/Fortinet
Vulnerability Mgmt	Rapid7/Tenable/ThreatMate
Compliance Agent	Hexnode/StrongDM/ThreatMate
Managed Endpoint Detection & Response (EDR/ MDR)	Crowdstrike/SentinelOne
Multi-Factor Authentication	Microsoft Azure
Cloud Security	Aqua Security/ThreatMate
Compliance automation	Vanta/Drata
SIEM	Splunk/Chronicle

Prior Work in SOC Maturity Models



Security Perimeter	SIEM/Data Lake Migration	Security Automation	Advanced Analytics	Predictive Analytics
Prevention focus	Security estate log coverage	SOAR implementation	Threat intel based searches	Identify likely attack paths
Patch program	Log aggregation & retention	Automate incident handling	ML based analytics	Adversarial simulation
Firewall & endpoint security	Use case engineering	Integrated tooling	Threat hunting	Insider threat detection
Manual remediation	EDR implementation	Playbooks for attack types	Investigations, forensics & IR	End to end automation

Copyright © 2020 Accenture. All rights reserved.

How Much is Enough Security?

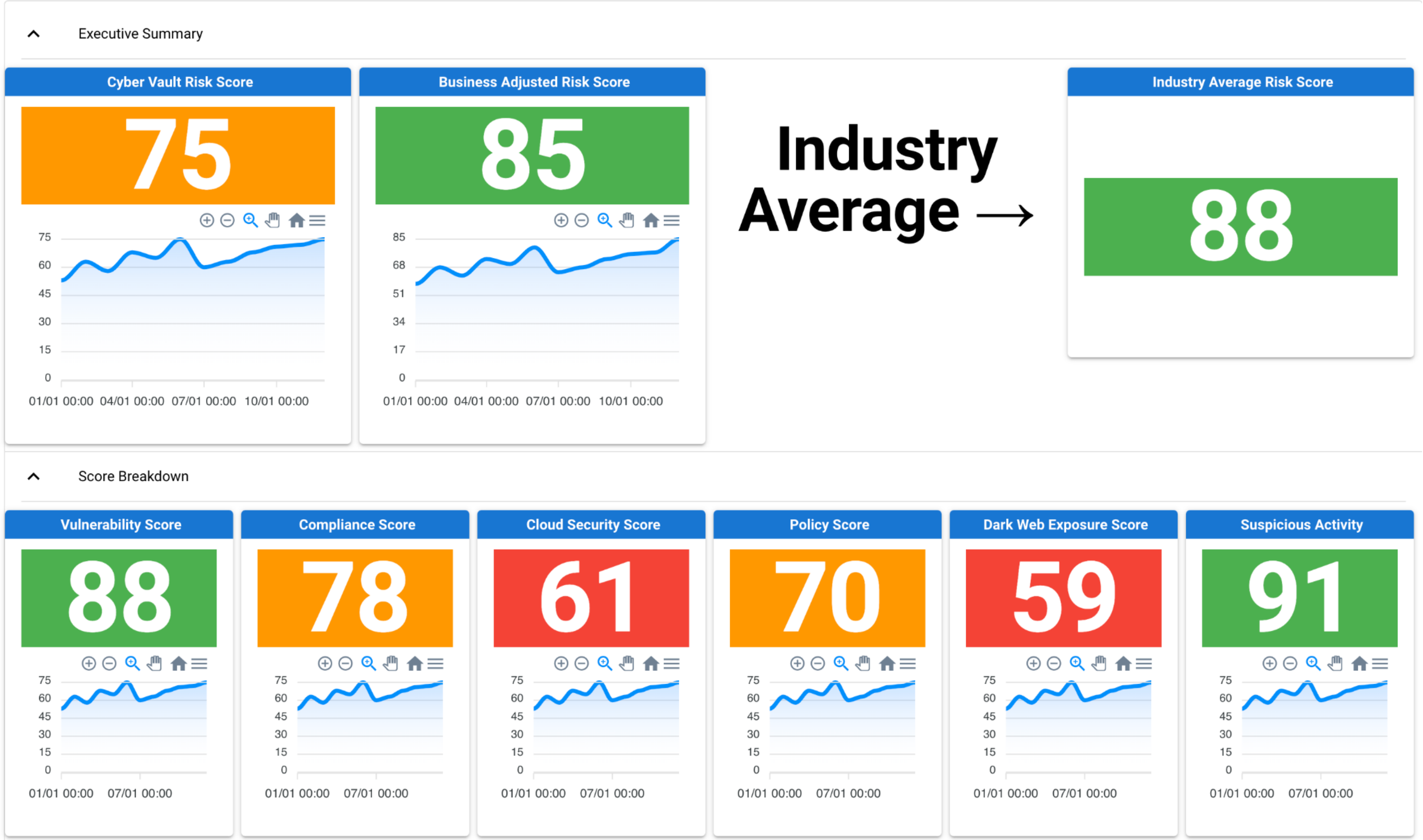
Most Security Professionals Struggle to Answer:

- How secure is my network?
- How much is enough spend in cybersecurity?
- Am I likely to suffer a Ransomware attack?
- What is my MTTD, MTTR, exposure time, Vuln Mgt Health?
- How do I compare to my peers & competitors?

In spite of standards, frameworks, and programs, quantifiable security is hard to come by.

At ThreatMate, we provide continuous assessment of security across your security exposures, then quantitatively measure your progress in improving security.

Risk Dashboard



Executive Summary

Cyber Vault Risk Score

75

Business Adjusted Risk Score

85

Industry Average →

Industry Average Risk Score

88

Score Breakdown

Vulnerability Score

88

Compliance Score

78

Cloud Security Score

61

Policy Score

70

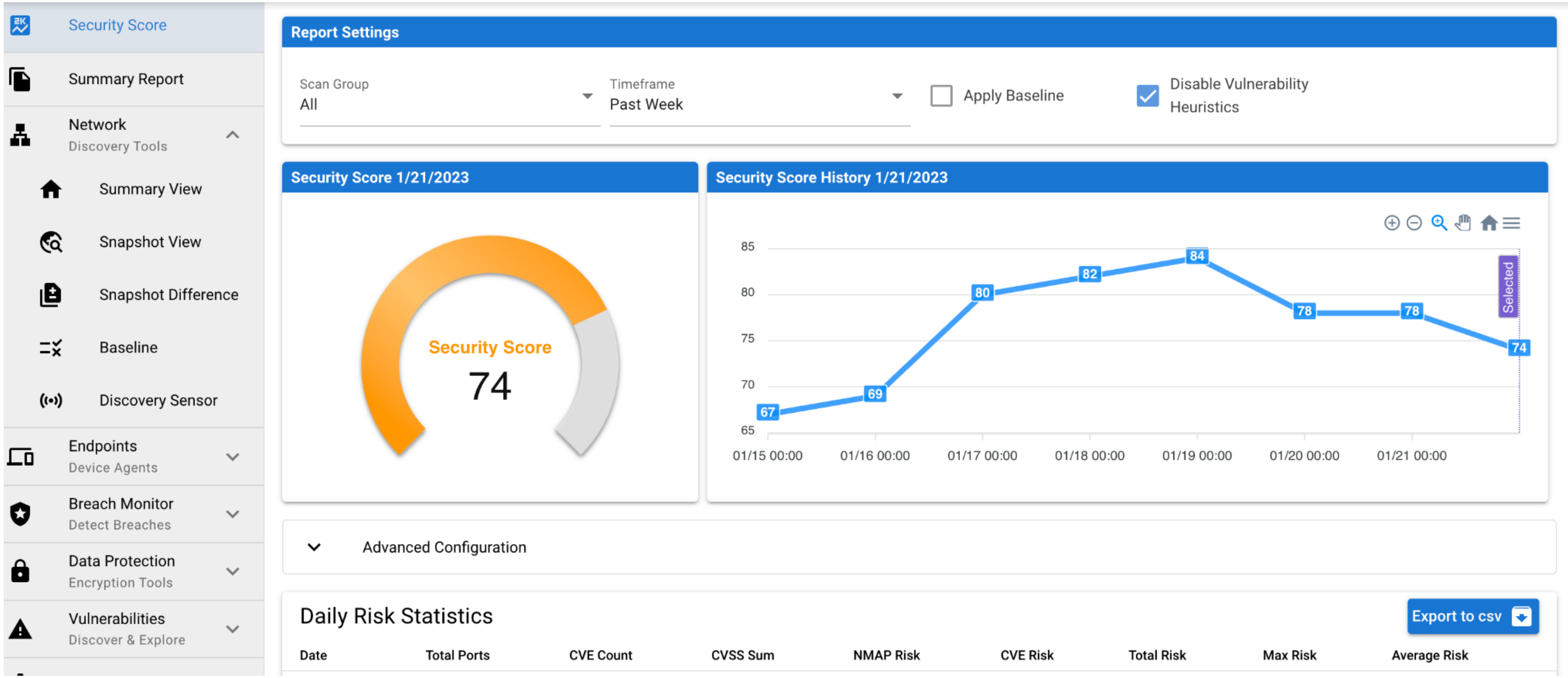
Dark Web Exposure Score

59

Suspicious Activity

91

Progress Dashboard



Report Settings

Scan Group: All

Timeframe: Past Week

□ Apply Baseline

☑ Disable Vulnerability Heuristics

Security Score 1/21/2023

Security Score 74

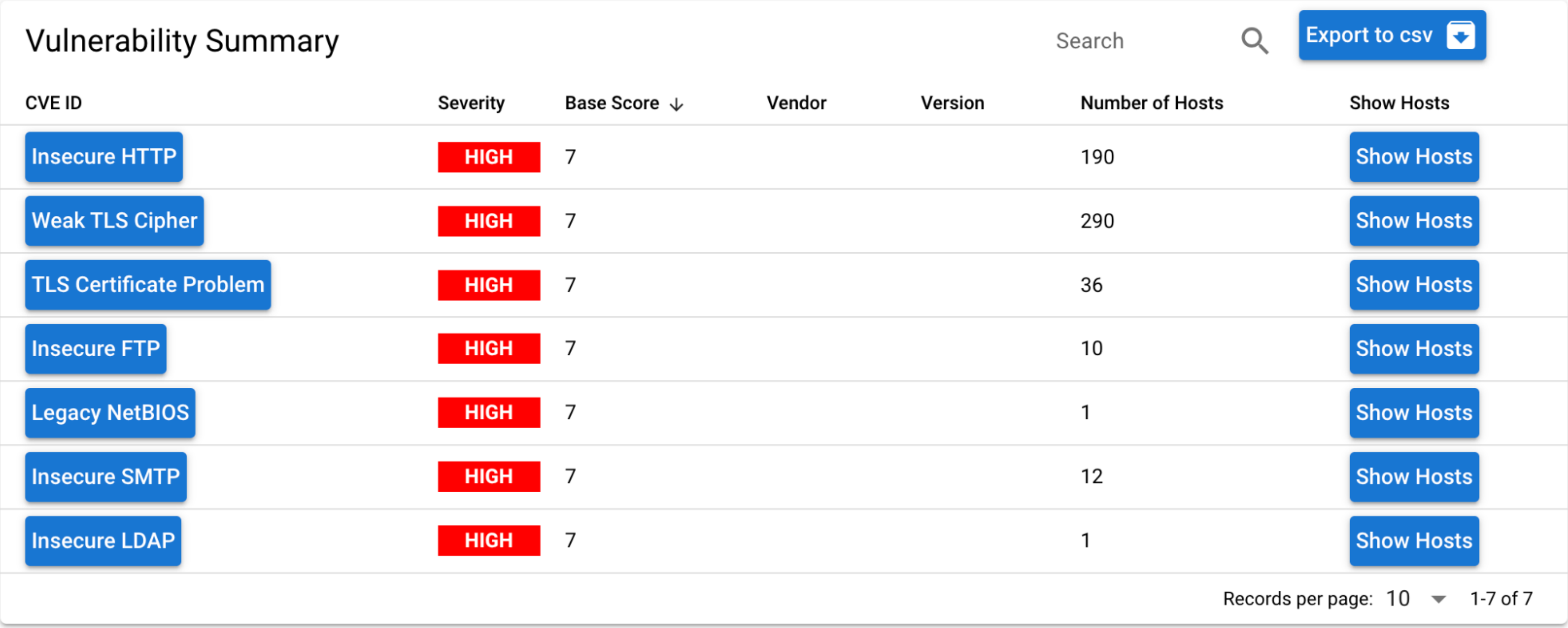
Security Score History 1/21/2023

Advanced Configuration

Daily Risk Statistics

Date	Total Ports	CVE Count	CVSS Sum	NMAP Risk	CVE Risk	Total Risk	Max Risk	Average Risk

Identified Issues

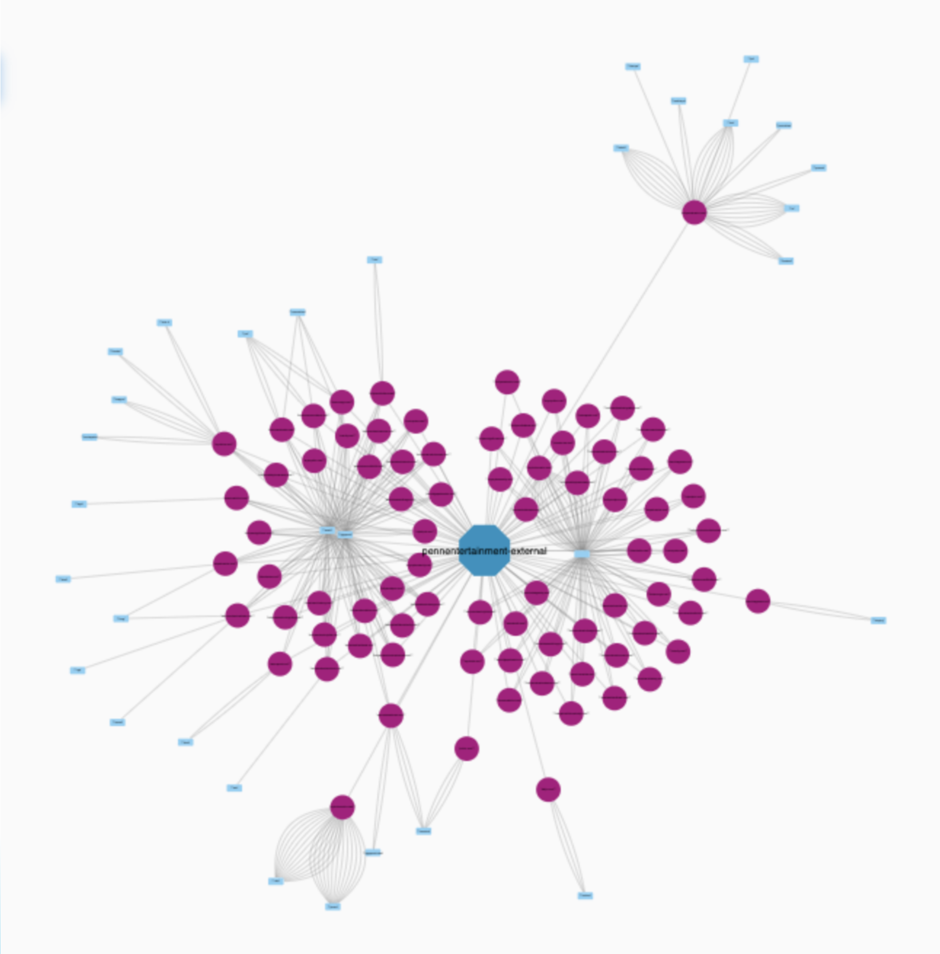


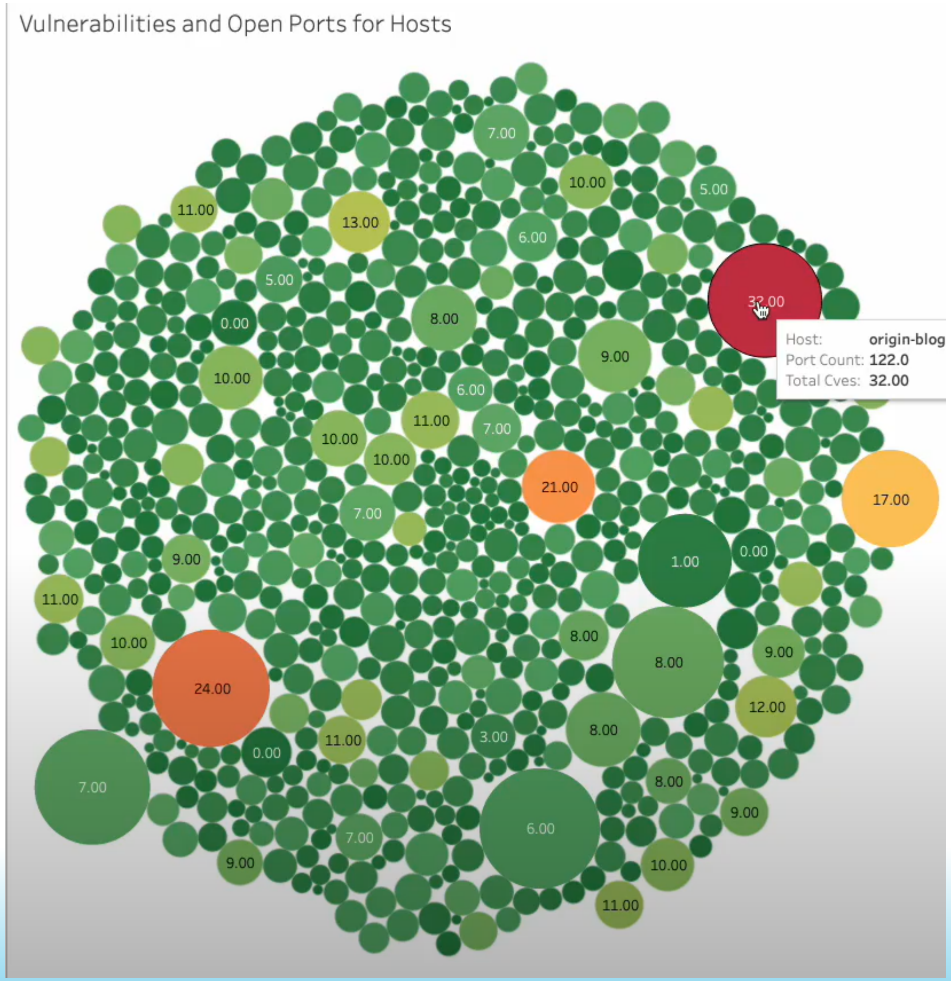
Vulnerability Summary

CVE ID	Severity	Base Score ↓	Vendor	Version	Number of Hosts	Show Hosts
Insecure HTTP	HIGH	7			190	Show Hosts
Weak TLS Cipher	HIGH	7			290	Show Hosts
TLS Certificate Problem	HIGH	7			36	Show Hosts
Insecure FTP	HIGH	7			10	Show Hosts
Legacy NetBIOS	HIGH	7			1	Show Hosts
Insecure SMTP	HIGH	7			12	Show Hosts
Insecure LDAP	HIGH	7			1	Show Hosts

Records per page: 10 ▾ 1-7 of 7

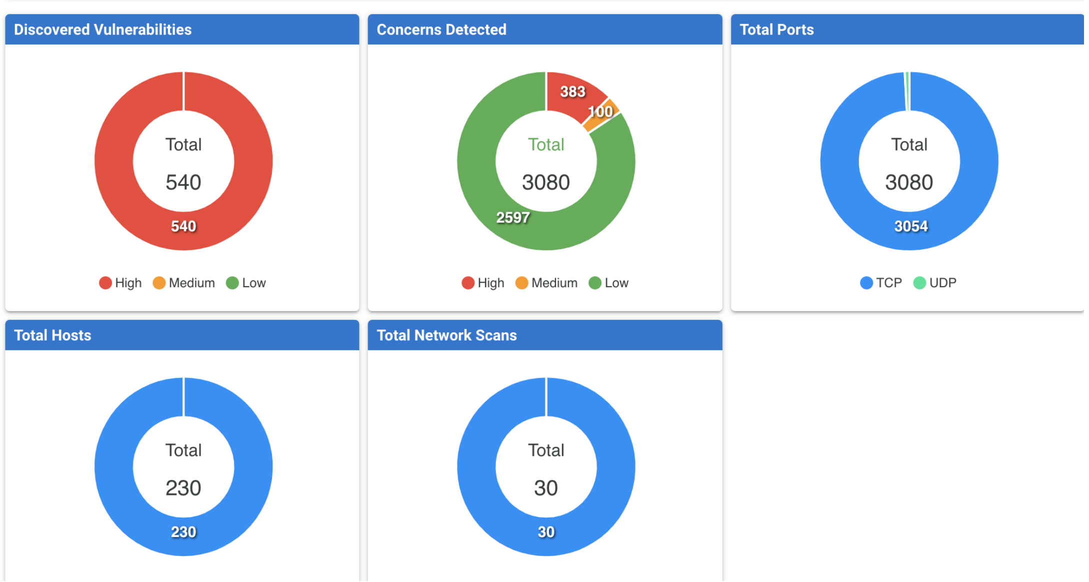
Visualizing Large-Scale Data Sets to Identify Weaknesses




Vulnerabilities and Open Ports for Hosts

Host: origin-blog
Port Count: 122.0
Total Cves: 32.00

From Ratings to Resiliency



- ThreatMate rates each risk area with weighted risks and identifies the risk contribution from each identified issue
- Ratings gamify security work & rewards improved resiliency while capturing measures of performance (eg exposure time, MTTD, MTTR)
- Integrations with Jira and SNOW (ITSM) permit SecOps teams to create user stories, tickets, resolve issues & increase resiliency

Let’s Collectively Figure Out the Best Measures of Risk

Quantitative cybersecurity is the best way to understand if your SOC program is working

Allows you to focus fixed resources in areas that need it and measure performance

Holds everyone accountable

Industry is already moving in this direction

Let’s get in front of it!

Discussion

IT NATION™ SECURE

Don't forget to fill out your

SESSION SURVEY