



# ***Strengthening Detection & Response with Censys***

A discussion on empower security teams to enhance visibility, reduce response times, and fortify their security operations with

Shunta Sharod Sanders, Global Federal Lead; Pre-sales Engineer at Censys

# Agenda

1

**Problems facing Cybersecurity teams today**

2

**What's the Answer?**

3

**Introduction to Attack Surface Management**

4

**Utilizing Censys ASM**

# Current Cybersecurity Landscape Problems



Exploits



Threat Actors



Budget Restraints





# Zero Days

**TFW YOUR DEATH STAR  
GETS BLOWN UP**

**BECAUSE OF A  
ZERO-DAY EXPLOIT.**

## Easy Credential Leaks

“New Zero-Day Vulnerability in Windows Themes Threatens NTLM Security”

## Unspecified Third-Party Bugs

“CISA Adds ScienceLogic SLI Vulnerability to Exploited Catalog After Active Zero-Day Attack”

## Malicious Code Attacks

FortiGate admins report active exploitation 0-day.  
Vendor isn't talking.

# Shadow IT



## COST

Shadow IT precludes the benefits of volume, potentially costing the total business more in resources, time and labor

## RISK

Unskilled individuals engaging in shadow IT might not have the expertise needed to properly configure & secure resources

## INCONSISTENCY

Different departments implement shadow IT differently, leading to inconsistencies in resource procurement, configuration and use

## CONTROL

IT teams cannot see shadow IT resources, which means they cannot manage, organize, control, or support them

# Cybersecurity Tool Sprawl



"We tend to continue to plug holes as we find weaknesses, and what we end up with is quite a bit of overlap," - CIO at a nonprofit

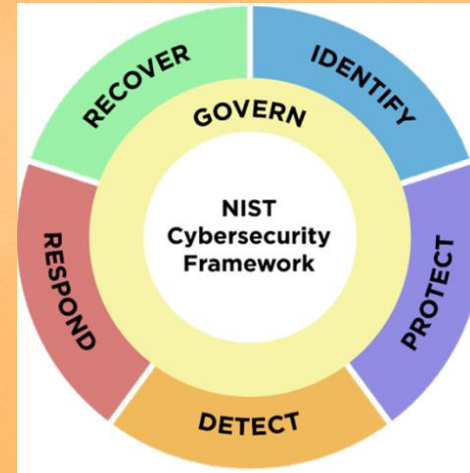
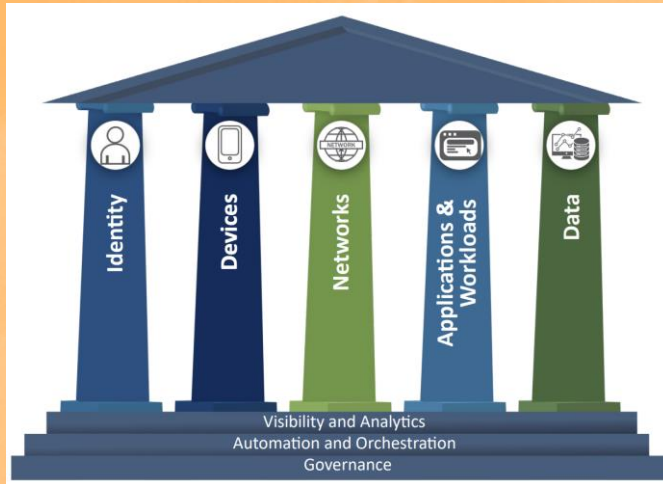
"Because these tools are very sophisticated and each of them are covering a separate aspect of the cybersecurity landscape, I think the biggest risk is to not understand if they're configured correctly to protect the organization in an efficient matter," - a cofounder and CTO at a data security solutions company

!

"There's a lot of risk just because tools usually touch data," - a field CISO at a cybersecurity company

# What's the Answer?

- **Assessments:** Assess current environment, resources, and solutions.
- **Collaboration:** Breakdown stovepipes within the organization foster communication.
- **Frameworks:** Implement industry best practices, frameworks, and best of breed solutions.



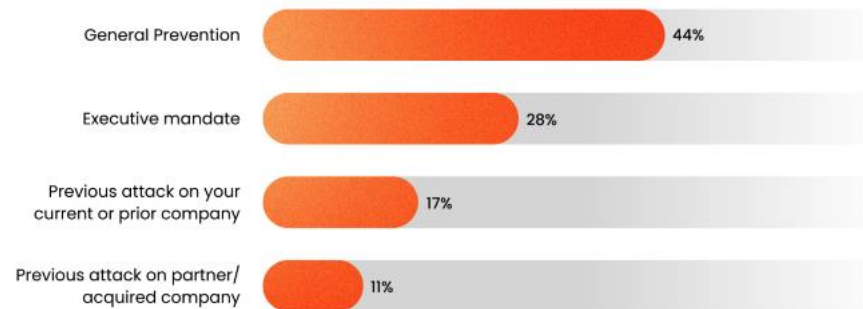


# ASM: What is it, and how does it fit in my security stack?

ASM comprises six major elements that facilitate ongoing discovery through extensive data source and risk scoring

1. Asset Discovery
2. Unified Global Inventory
3. Cloud Governance
4. Risk Detection and Remediation
5. Post-Announcement M&A Risk Assessment
6. Subsidiary Risk Assessment

## Primary reason for employing an ASM solution



Source: Paradoxes, Inc Attack Surface Management Study, August 2022 (n50)



# Responding to Cyber Security Risk Threat: A Step-by-Step Guide Using Censys ASM

## Alert Notification

Receive an immediate alert about a vulnerability or exploit advisory.

## Asset Discovery

Scan the organization's environment using Censys ASM to identify exposed VPN servers.

## Threat Investigation

Investigate potentially vulnerable systems using detailed asset information from Censys ASM.

## Vulnerability Prioritization

Prioritize vulnerable assets based on factors like criticality, location, and exposure.

## Mitigation


Coordinate the patching or isolation of exposed systems to reduce risk.


## Reporting


Generate a comprehensive report on identified threats and mitigation actions for key stakeholders.


# Step I – Identify the Risk (Alerts & Notifications)


## ALERTING INTEGRATIONS


**Email**  
Send messages to your email when Censys detects a new issue.


**Teams | Microsoft**  
Send messages to a selected channel in Microsoft Teams when Censys detects a new issue. [Set Up](#)

**Slack**  
Send messages to a selected channel in Slack when Censys detects a new issue. [Set Up](#)

**WebEx | Cisco**  
Integrate with your team's communication platform to receive risk and host event notifications in real time, reducing the remediation timeframe.

**Rapid Response Email**  
Send Rapid Response messages to your email when Censys detects a new Risk. [Set Up](#)

**Webhook Connection**  
As new risks are found in your attack surface, send a webhook containing a JSON payload to a URL of your choosing. [Set Up](#)



### Save this Query?

**Name**

Max characters 200 33 / 200

**Syntax**

```
((risks.severity: `Critical`) and risks.categories = `.*Software Vulnerability.*`) and type = `HOST`
```

☒ Save as Alert

[Cancel](#) [Save & Set up Alert](#)

Certificates		0 Storage Buckets	
	Risks		Source
	1 5 3		Censys
	3		
	1 1 3		Censys
	3		

# Step II – Analyzing the Risk

## RISK DETAILS

Risk ID	387
IP Address	34.121.235.0
Port	5432
Service	POSTGRES
Transport	TCP
URI	postgres://34.121.235.0:5432
First Seen	FEB 24, 2022   09:29 AM UTC
Last Seen	SEP 18, 2024   08:35 AM UTC
Categories	EXPOSURE
	Service or Interface

## SCAN DATA

Protocol	Port	
FTPS	21	< 1 > of 18
View as <span>Table</span> <span>JSON</span>		
Attribute	Value	
ftp.authTlsResponse	MjMOIEFVVVEggVExTIE9LLgOK	
ftp.banner	220----- Welcome to Pure-FTPd [privsep] [TLS] ----- 220-You are user number 1 of 100 allowed. 220-Local time is now 20:15. Server port: 21. 220-This is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 10 minutes of inactivity.	
ftp.implicitTls	false	
ftp.statusCode	220	
ftp.statusMeaning	Service ready for new user.	
ftp.tls.certificate.ct.entries.cloudflare_nimbus_2024.index	186553705	

# Step II – Analyzing the Risk

## RECENT HOST ACTIVITY

< Back / Recent Host Activity

Go to Logbook →

○ POSTGRES Service Exposed added to 34.121.235.0

Aug 3, 2024 08:09 PM UTC ^

	Date	Risks
New Value	Aug 3, 2024 08:09 PM UTC	Risk: POSTGRES Service Exposed (Severity critical).
Old Value	Aug 1, 2024 05:58 PM UTC	--

○ No Trusted Path Certificate added to 34.121.235.0

Aug 3, 2024 08:09 PM UTC ▾

○ Certificate added to 34.121.235.0 on port 5432 / POSTGRES

Aug 3, 2024 08:08 PM UTC ▾

○ POSTGRES added to 34.121.235.0

Aug 3, 2024 08:08 PM UTC ▾

○ 34.121.235.0 on port 5432 added Postgresql \*

Aug 3, 2024 08:08 PM UTC ▾

○ 34.121.235.0 on port 5432 added Linux \*

Aug 3, 2024 08:08 PM UTC ▾

○ Port 5432 added to 34.121.235.0

Aug 3, 2024 08:08 PM UTC ▾



### Azure Sentinel | Microsoft

Connect your host and risk events with your existing alert, correlation, and incident workflows for improved efficiency.

Set Up



### Splunk

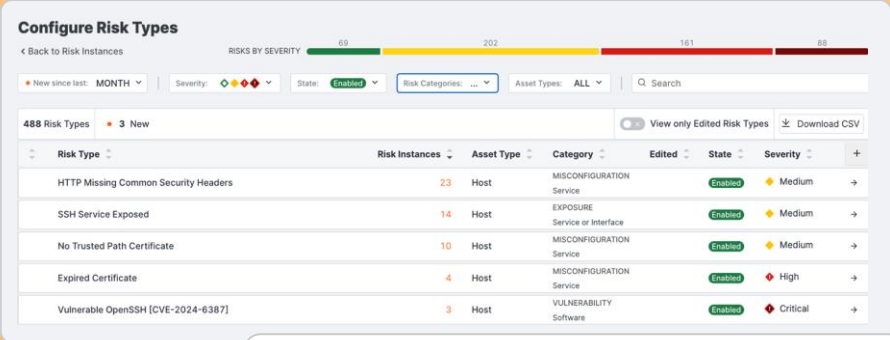
Configure your system to connect attack surface data with your security and analytics applications for enhanced insights.

App Download ↗

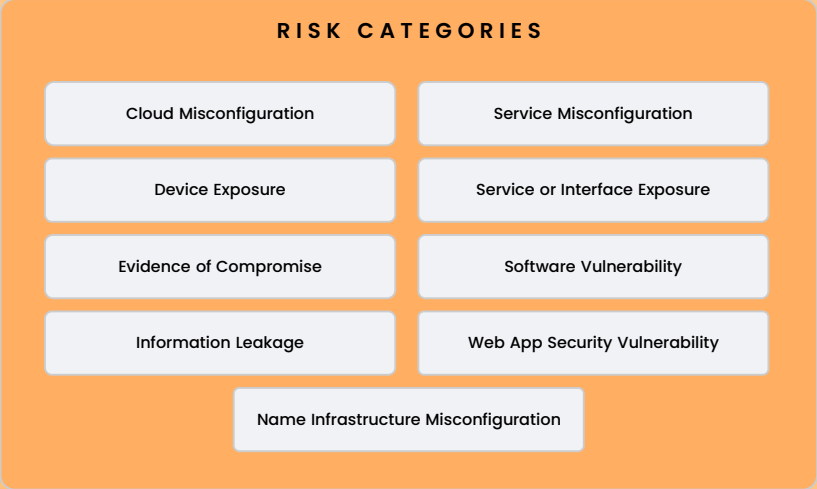


# Step III – Prioritize Risks

## Different Risk Views



Top Risk Types			Risks By Category	Risks By Severity	Riskiest Assets
SEVERITY	RISK TYPE	RISK INSTANCE COUNT			
Critical	Vulnerable OpenSSH [CV...		2		
Critical	POSTGRES Service Expos...		1		
High	Expired Certificate		3		
High	Exposed MOVEit Transfer...		2		
High	Vulnerable OpenSSH [CV...		1		



# Step IV – Treat the Risks

## Remediation Recommendations

### Primary

Restrict access to this service using firewall rules, VPN segmentation, or VPC segmentation to make it inaccessible from the Internet.

### Secondary

Use one-way hashing encryption methods for columns that don't need to be unencrypted, like passwords. Restrict all non-required management ports.

## ITSM Platforms



### JIRA

Automate the process of creating and updating tickets in Jira based on identified issues in Censys.

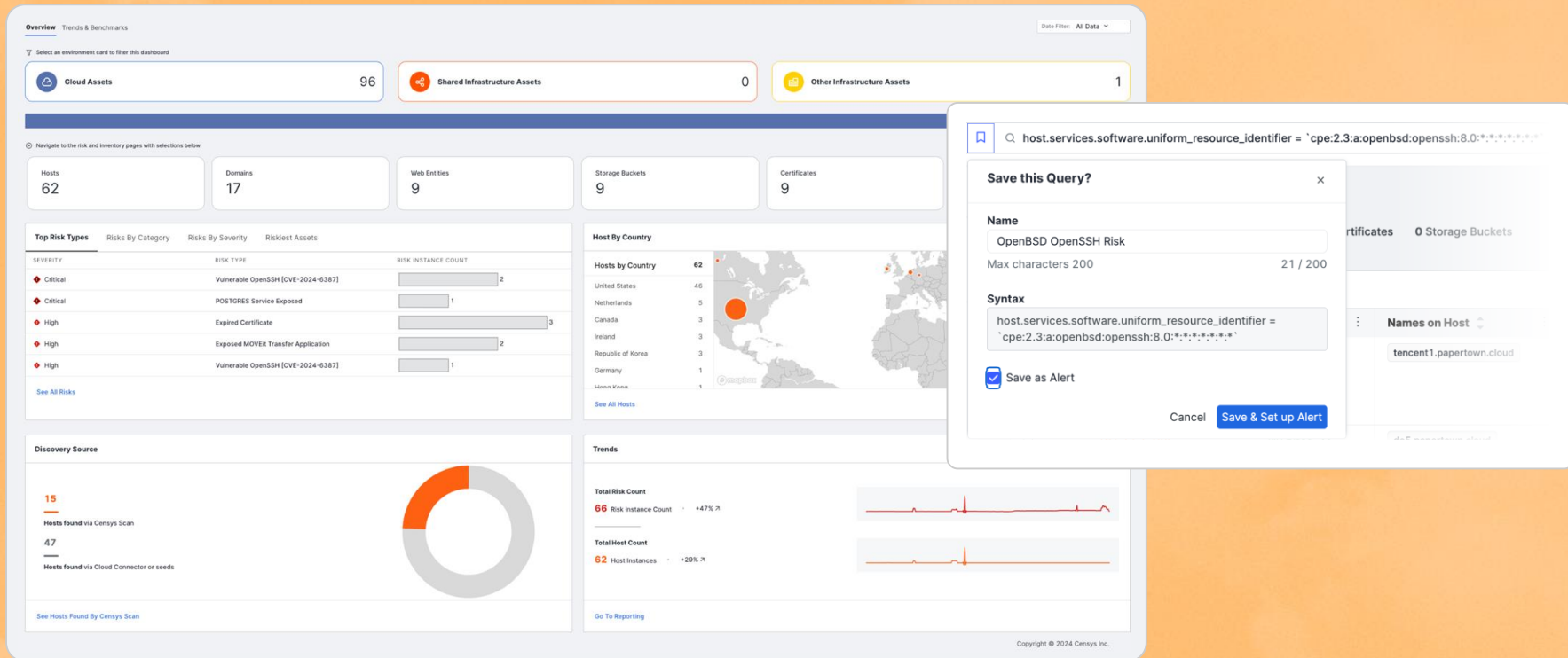
[Set Up](#)

### ServiceNow ITSM

Automate the process of creating and updating tickets in ServiceNow based on identified issues in Censys.

[Set Up](#)

# Step V – Monitor the Risks



# Benefits of an ASM

Cybersecurity professionals employ a blend of solutions to protect their organizations. The most common solutions used are Vulnerability Management, Cloud Security Posture Management (CSPM), Cloud Access Security Broker (CASB), and Attack Surface Management.

**35%**

of attacks are carried out through software vulnerability exploits.

**33%**

through supply chain and third-party breaches

**32%**

through web application exploits



"The first thing that comes to mind when I hear Attack Surface Management is a comprehensive solution that analyzes existing vulnerabilities and enables mitigation efforts."

– CISO, HEALTH CARE





# Thank You

Connect with us at  
[www.censys.com](https://www.censys.com)