RiskRecon Overview

June 10, 2020

Texas Department of Information Resources

Transforming How
Texas Government
Serves Texans

Introductions

- Matt Kelly, Texas Department of Information Resources
- Dave Manning, RiskRecon
- Raine Drosdick, RSA Professional Services

RiskRecon Onboarding Overview

Dave Manning

Customer Success Advisor

riskrecon

mastercard

Some questions you may want answers to

riskrecon
mastercard

Some Questions

- What is my risk exposure today?
- Is my risk exposure getting better or worse?
- Do I encrypt sensitive data in transit?
- Do I manage software vulnerabilities well?

Where are the answers?

riskrecon
mastercard

riskrecon
mastercard

What kind of data do you need to understand risk?

Risk [Risk]

Noun 1. **The probable frequency and magnitude of an undesirable outcome.**

Understanding risk requires knowing issue severity and asset value.

riskrecon

mastercard

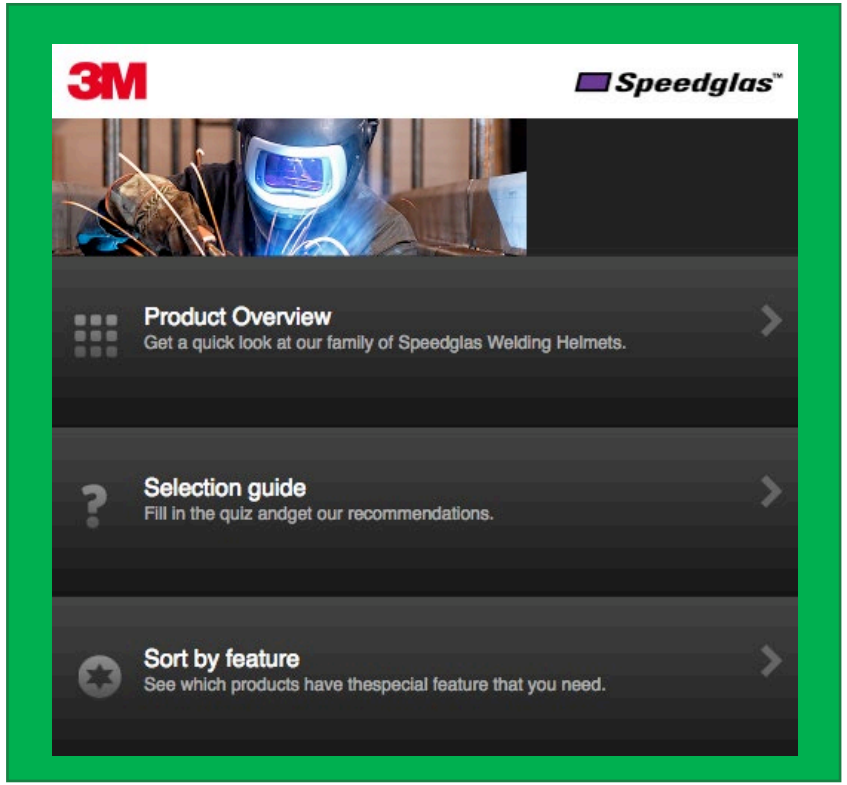
Asset value is critical to determining risk

Example: 2 systems with same critical unpatched software issue:

1 system is sensitive email gateway

VS

1 system is marketing brochure site

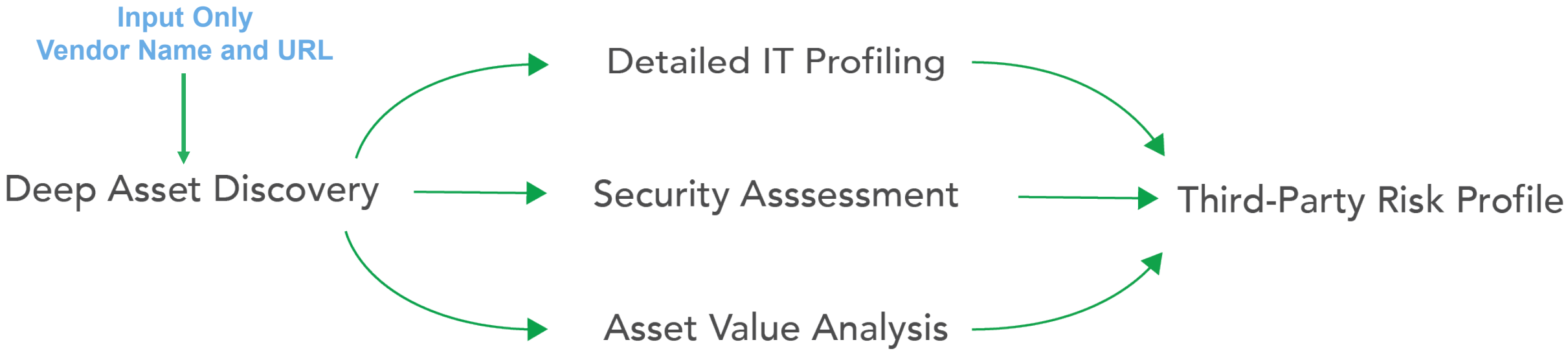


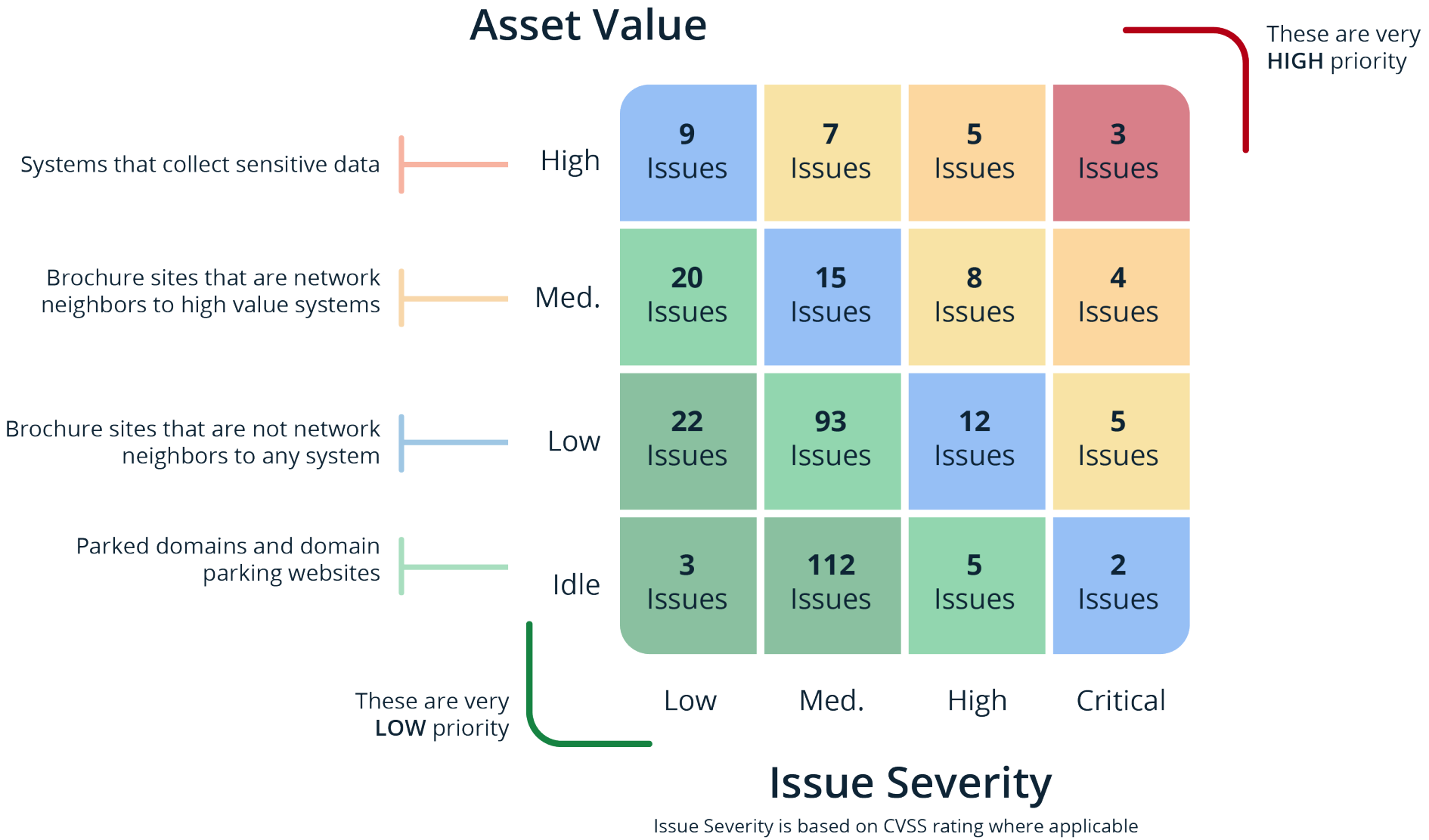
Same issue, but risks are very different

riskrecon

riskrecon mastercard

RiskRecon builds risk profiles by analyzing each third-party's publicly-accessible Internet surface





riskrecon
mastercard

State Implementation

Matt Kelly

RiskRecon Overview

- Provides security metrics on public-facing assets across 10 security domains.
- Identifies vulnerabilities and recommends remediation responses.
- Integration with Archer IT Security Vulnerability Management use case.
  - Issues Management
  - Vulnerability Ticketing
- Licensed for 300 companies
  - Limiting RiskRecon accounts to ISO
  - Including common vendors in monitoring
  - Vendor suggestion form: https://www.surveygizmo.com/s3/5620263/RiskRecon-Vendor-Suggestions

State Implementation

- Mapped identified assets to organization profiles via MS-ISAC VMP program scan results, existing RiskRecon state of Texas domains/hosts, DIR Registrar records, etc.
- Profiles can be tuned – add/remove domains and hosts. Send requests to support@riskrecon.com
- Starting with designated ISO – additional users and user administration on RiskRecon side handled by support@riskrecon.com
- Moving to production in SPECTRIM – new workspace (IT Security Vulnerability Management) will be available for Information Security Group members.
- General users will have visibility into only assigned tickets.
- Scan results are for the benefit of your organization, DIR is not incorporating scan results into maturity scores, security plans, etc.

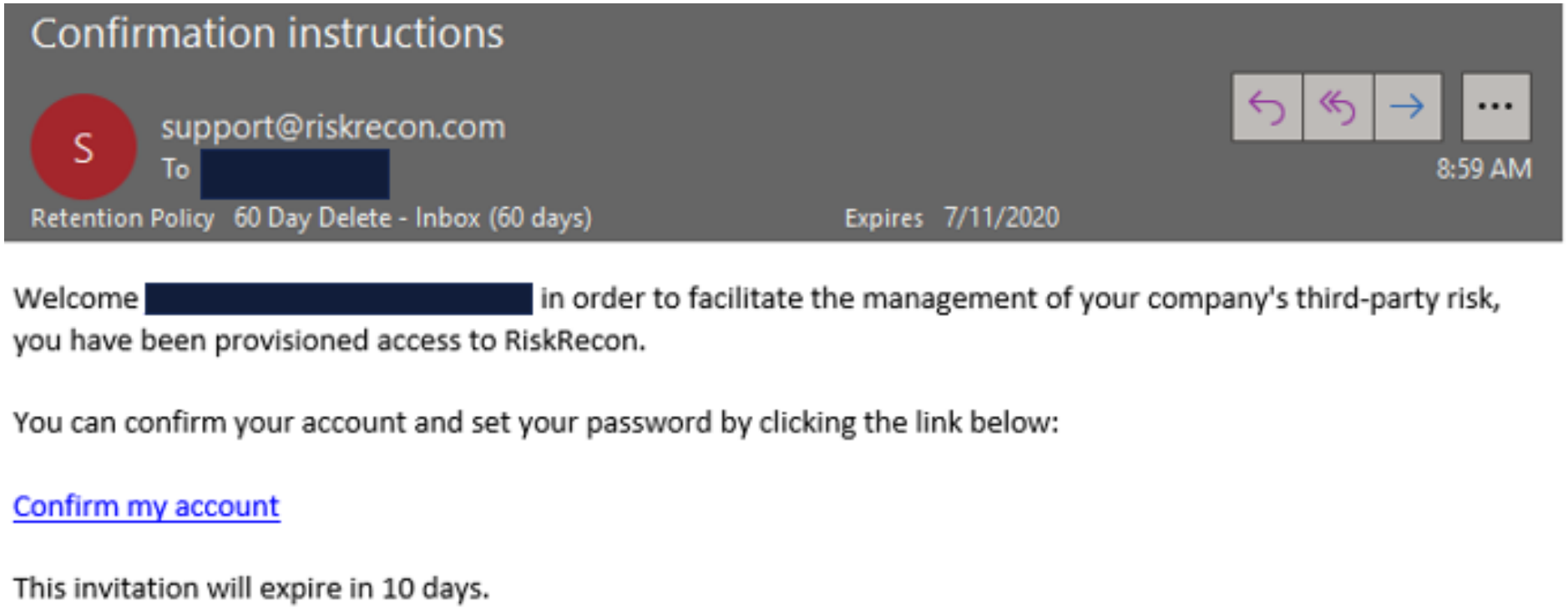
RiskRecon Does...

- Deep mining of domain registration databases
- Deep mining of network registration databases
- Analysis of Internet DNS IP to hostname resolution logs
- DNS queries
- Lightly browse web sites, obeying robots.txt instructions
- Analytics of publicly accessible code, content, configurations
- Monitoring and analysis of commercial and open-source IP reputation feeds
- Mining the internet for relevant information such as indicators of data loss events
- Analyze Internet port scan data sourced from a commercial provider

RiskRecon Does Not...

- Tamper with parameters
- Inject code
- Conduct cross-site scripting
- Conduct SQL injection
- Attempt to bypass authentication
- Execute memory overflow tests
- Fill out form fields
- Guess credentials
- Execute vulnerability exploits
- Attempt to bypass security controls

Account Confirmation Email



Confirmation instructions

S

support@riskrecon.com

To [redacted]

8:59 AM

Retention Policy 60 Day Delete - Inbox (60 days) Expires 7/11/2020

Welcome [redacted] in order to facilitate the management of your company's third-party risk, you have been provisioned access to RiskRecon.

You can confirm your account and set your password by clicking the link below:

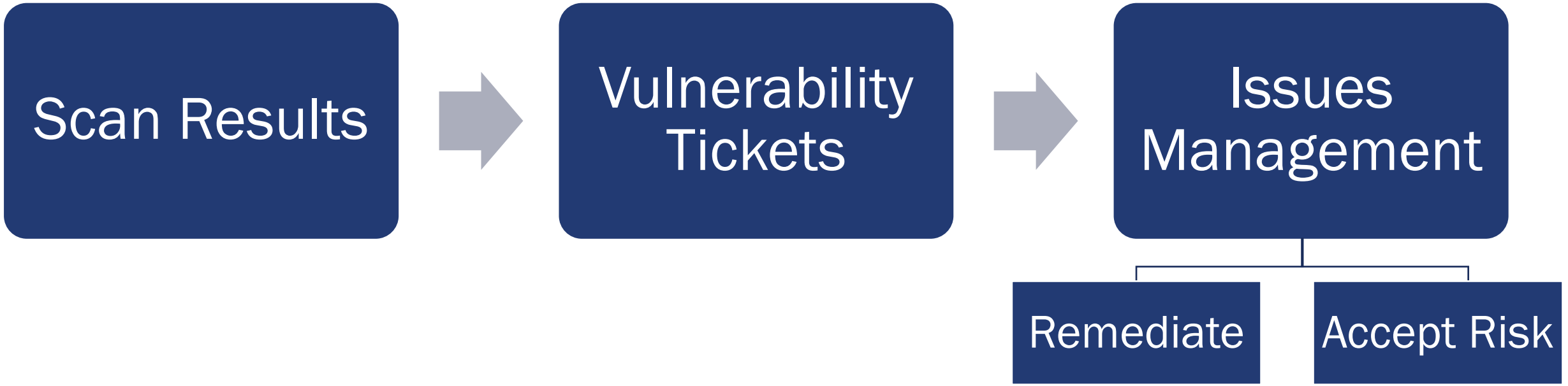
Confirm my account

This invitation will expire in 10 days.

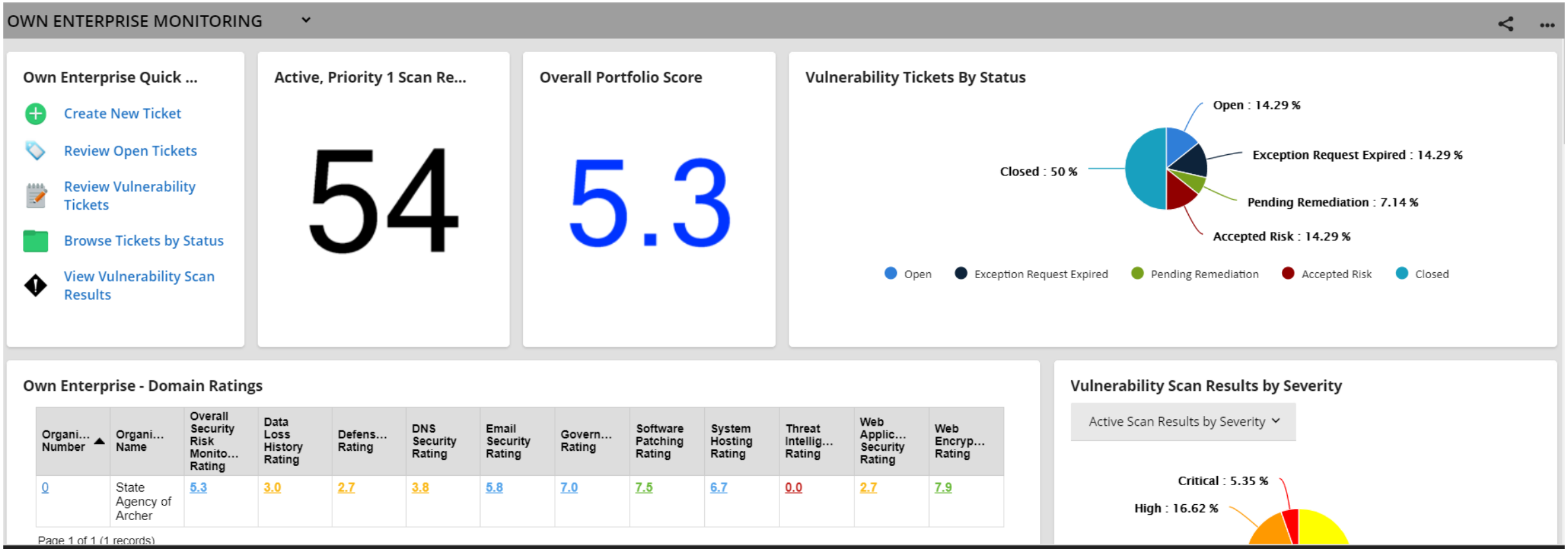
SPECTRIM Integration

Raine Drosdick

SPECTRIM Workflow



Own Enterprise Monitoring



Vulnerability Scan Results

Title:	Software Patching-Application Server Patching-PHP 5.2.x	**VSR Overall Status:**	Active
Organization:	0	**Scan Status:**	Active
Organization Name:	State Agency of Archer	**Related Ticket Status:**	
Severity:	Critical	**First Found Date:**	1/29/2019 7:01 PM
Severity Override:		**Last Found Date:**	5/2/2020 1:20 AM
Assigned To:		**Closed Date:**	
		Days Open:	487 Days

▼ SECURITY RISK MONITORING SCAN RESULTS

Security Domain:	Software Patching	**Security Criteria:**	Application Server Patching
Priority:	1	**False Positive:**	False
Security Risk Monitoring Severity:	Critical		To gain access to the Security Risk Monitoring portal, please email grc@dir.texas.gov.
Finding Type:	PHP	**Scan Result Link:**	View all Software Patching findings
Issue:	PHP 5.2.x	**Finding Notes:**	
Finding Context:	The software is end of life and has known security vulnerabilities.		

▼ DEVICE DETAILS

Number of Times Vulnerability Occurred:	1	**Asset Value:**	High
Hostname:		**Hosting Type:**	Internal
Domain Name:		**Hosting Provider:**	state of texas
IPv4:			
Has Authentication?:	Yes	**Data Characteristics:**	Password User Name

Vulnerability Tickets

GENERAL INFORMATION

Ticket Number: 302703
Ticket Name: App Server Patch for PHP 5.4
Organization: 0
External Ticket Number:
Ticket Due Date: 3/27/2020
Ticket Description: Upgrade these servers to the latest version of PHP.

Ticket Status: Closed
All Associated VSR Closed, Verified, or Accepted Risk: No
Organization Name: State Agency of Archer
Days Open: 48
Opened Date: 2/24/2020 2:47 PM
Closed Date: 4/13/2020 11:52 AM

▼ STAKEHOLDERS

Ticket Owner: *TEST, IRM
Business Stakeholders (Additional Access):

Vulnerability Analyst: *TEST, ISO / Incident

▼ RESPONSE SUMMARY

Ticket Response: Remediate Risk (Simple Remediation)
Remediation Status: Complete

Response Status: Remediation Complete
Verifiable by Scanner?: Yes

▼ SIMPLE REMEDIATION DETAILS

Is a Patch Available?: Yes
Expected Simple Remediation Date: 3/23/2020 12:00 PM
Remediation Plan Details: this is what im going to do...

Simple Remediation Completed Date: 3/25/2020 5:00 PM

Questions

GRC@dir.texas.gov

Thank You

dir.texas.gov

#DIRisIT

@TexasDIR

DIR

Texas Department of Information Resources

Transforming How
Texas Government
Serves Texans