Noise Cancelling FIM

Lavish Jhamb
Senior Product Manager, Compliance Solutions

How many of you use Qualys Cloud Agents?

How many of you know that existing these existing agents can do File Integrity Monitoring (FIM) and File Access Monitoring(FAM)?

Success Formula

For Your File Integrity Monitoring Program

01 **Experience seamless onboarding with** ready-to-use set up for PCI 4.0

02 **Fine-tuned FIM solution** with automated noise cancellation

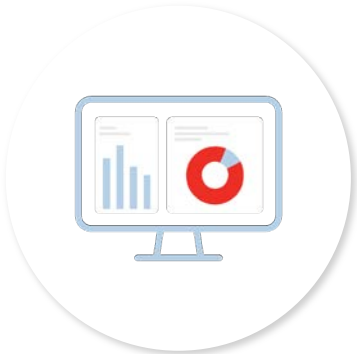
03 **Most comprehensive FIM coverage** for servers, endpoints, network devices and containers

Outcomes

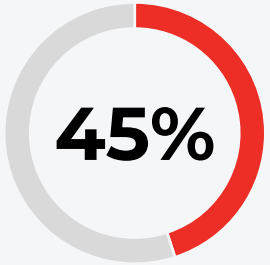
Significant reduction in operational costs for managing FIM

Zero issues in meeting PCI 4.0 FIM Requirements

Why FIM is a Must-have?

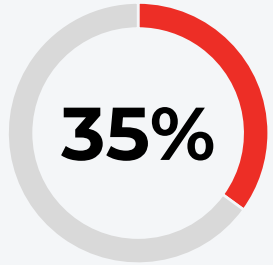


File Integrity Monitoring



Ransomware attacks involve **changes to user files**

Advanced Persistent Threats (APT) **use registry changes for persistence**

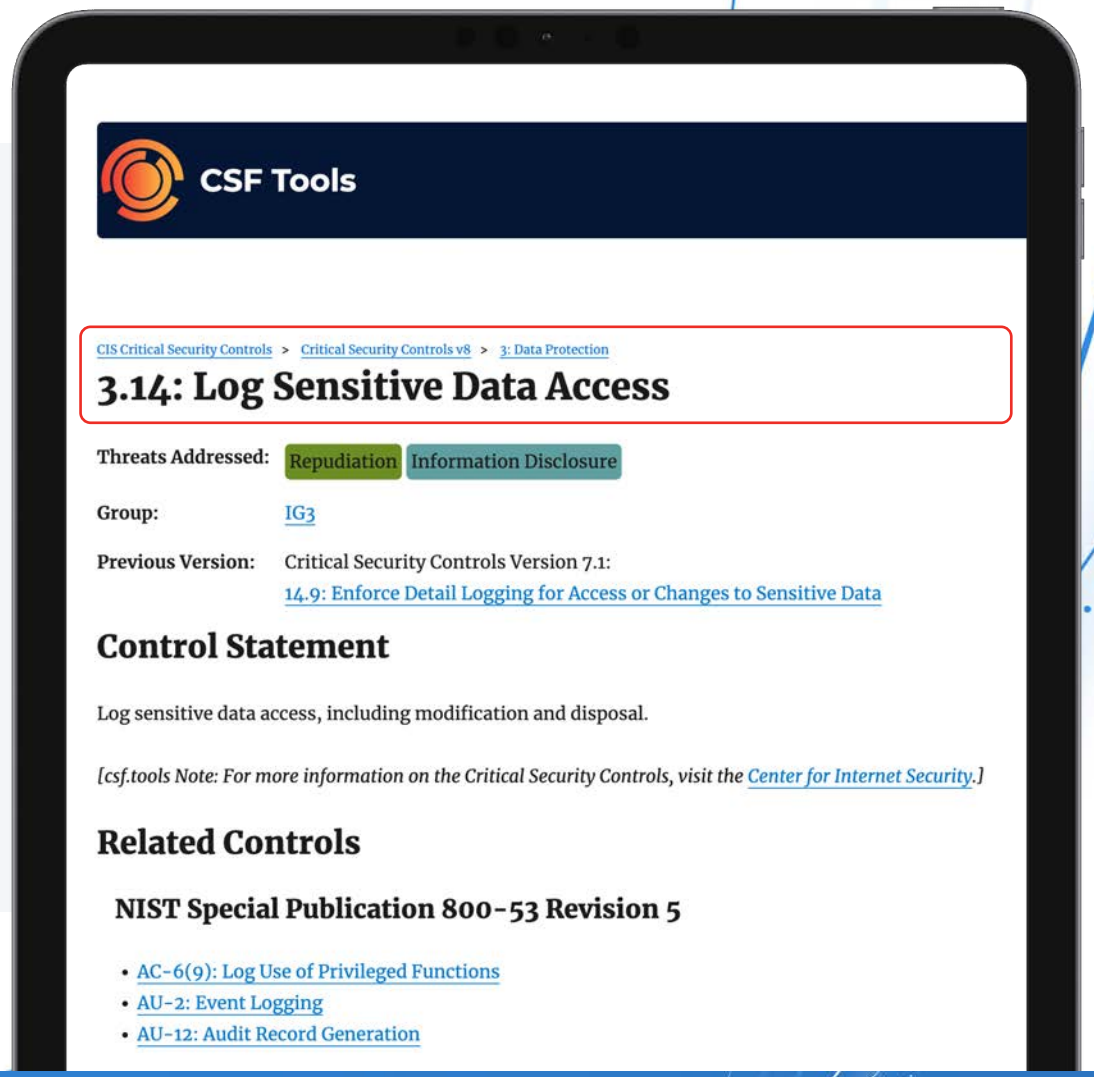


Rootkits modify **registry keys to evade detection**

Security Agencies Recommend FIM

"Implement a configuration change control process to detect unauthorized modifications"

"Compare against expected configuration changes and patching plans to verify that the changes are authorized"



verizon

Verizon 2024 Payment Security Report marks FIM as one of The 20 Biggest Control Gaps

Cost of non-compliance - Business comes to a halt

Source: Verizon 2024 Payment Security Report -Bottom-20 lists

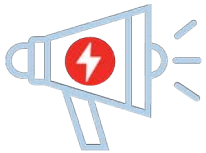
Challenges with FIM Deployments

Not the Right Sensor

Sensors responsible for FIM are found using **self-signed certificates**

Fail to Cover Blind Spots

FIM on Network Devices, Container-based FIM, File Access Monitoring (FAM)



Alert Fatigue

Inability to distinguish between legitimate changes from patches and updates and potentially malicious activity

Challenges with Traditional FIM Solutions

Unauthorized File Access

Unable to detect unauthorized access attempts

User Impersonation

Cannot identify user impersonation during file changes

Lack of Threat Intelligence

Cannot detect malicious hashes dropped in critical locations

Usability

Extremely difficult to use and manage

Detecting White Noise

Inability to distinguish between legitimate changes from patches and updates and potentially malicious activity

The Solution and Its Capabilities

Qualys

One Platform for Most Comprehensive FIM Coverage

Scanner Appliance

Agentless FIM

Scan-based FIM on network devices

Detect configuration changes in network devices such as routers, switches, and firewalls.

Cloud Agent

Agent-based FIM

Real time monitoring for servers and endpoints

Real time File Access Monitoring (FAM)

Threat detection

Container Sensor

Container Runtime Security

Real time FIM on containers

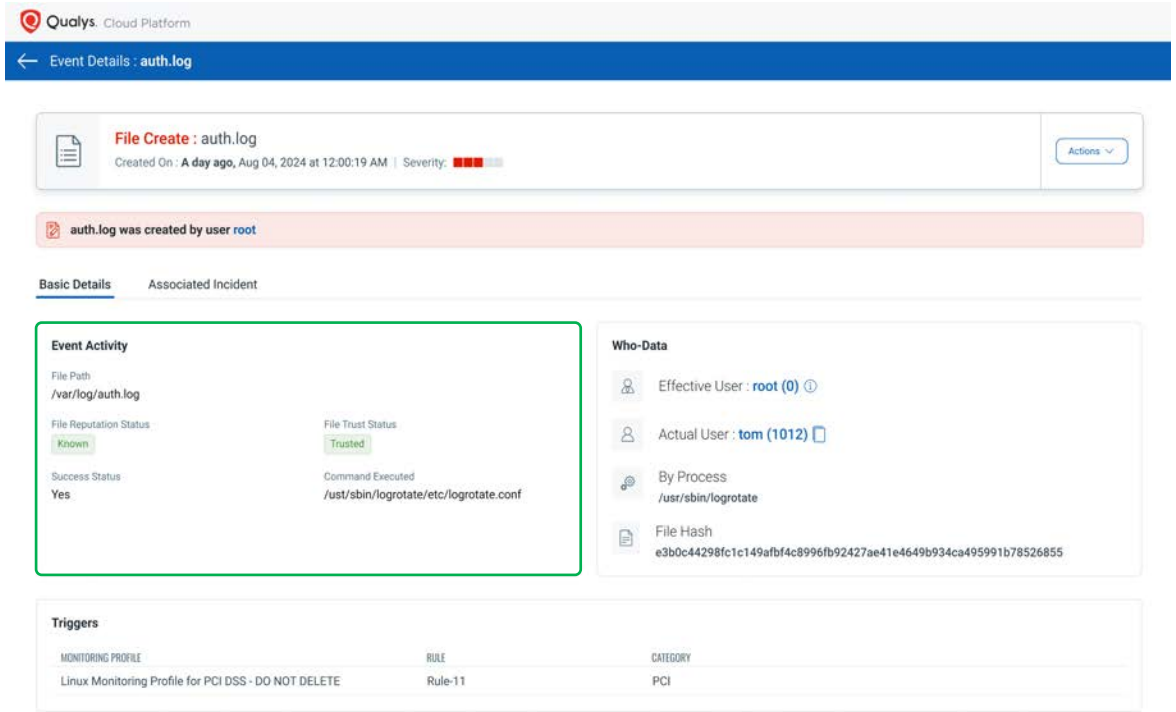
Track unauthorized access to critical files on containers

Qualys FIM

Noise Cancellation

Trust Status - Automated reconciliation of change events from known vendor updates and patches

User and Process based event suppression: Eliminate 90%+ of false positives by excluding FIM events generated by known good users and processes



File Access Monitoring (FAM)

15% **Of unauthorized access attempts targeted highly sensitive.**

Linux

13.1M
Total Unauthorized Access Attempts

2.22M
Highly Sensitive Files

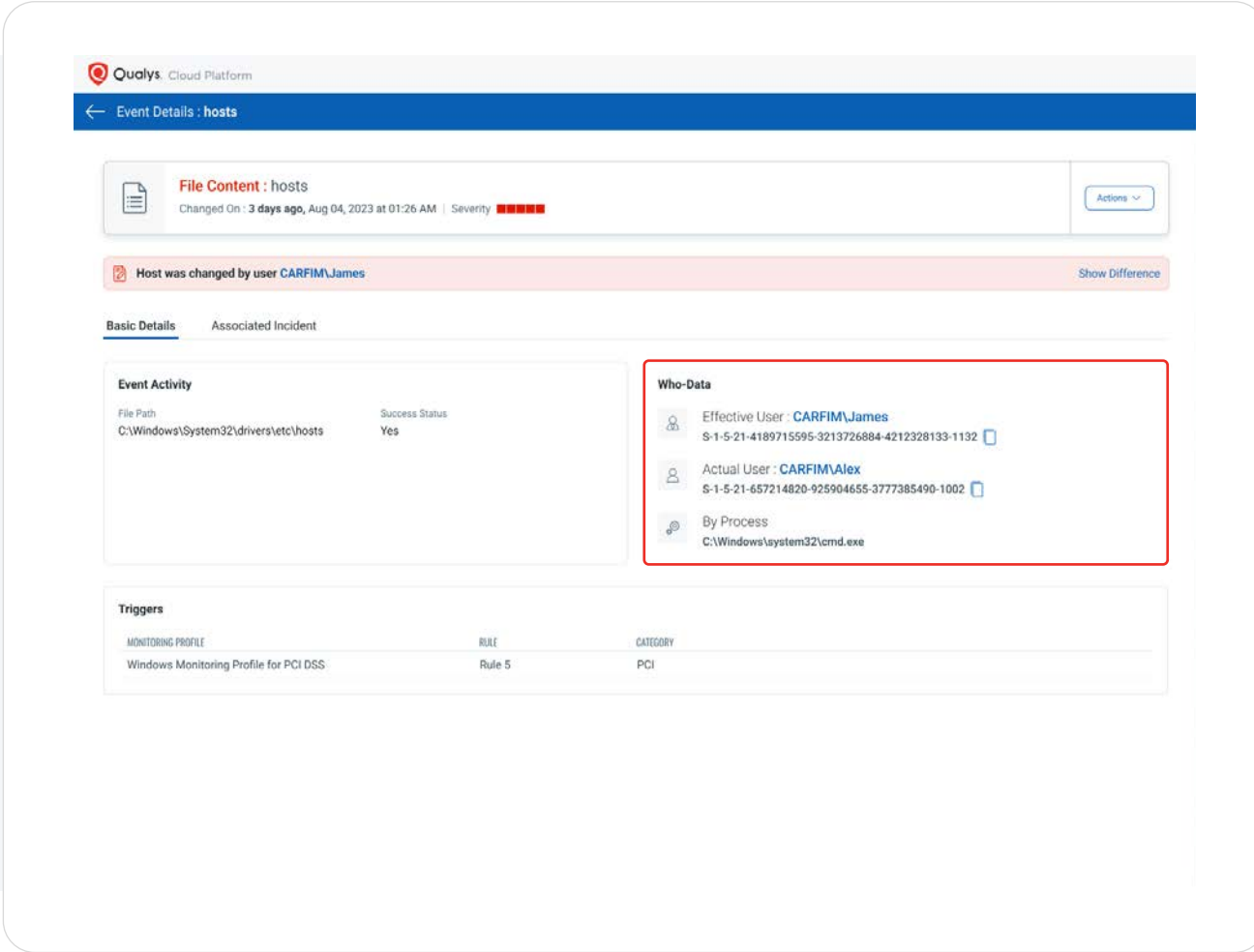
Windows

14.6M
Total Unauthorized Access Attempts

2M
Highly Sensitive Files

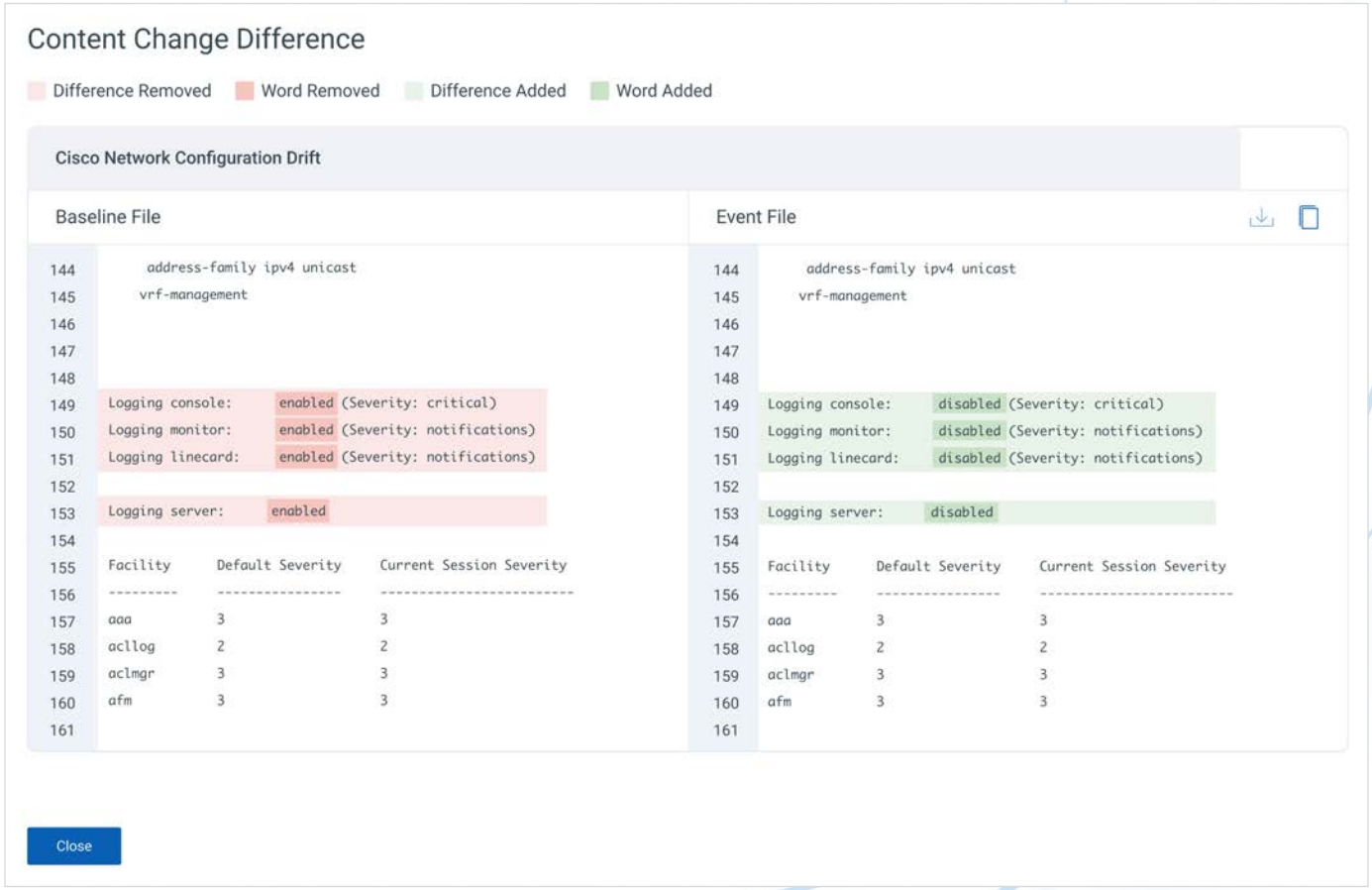
Identify User Impersonation

Detects when a user impersonates another to gain unauthorized access



Detect High Risk Activities on Your Network Devices

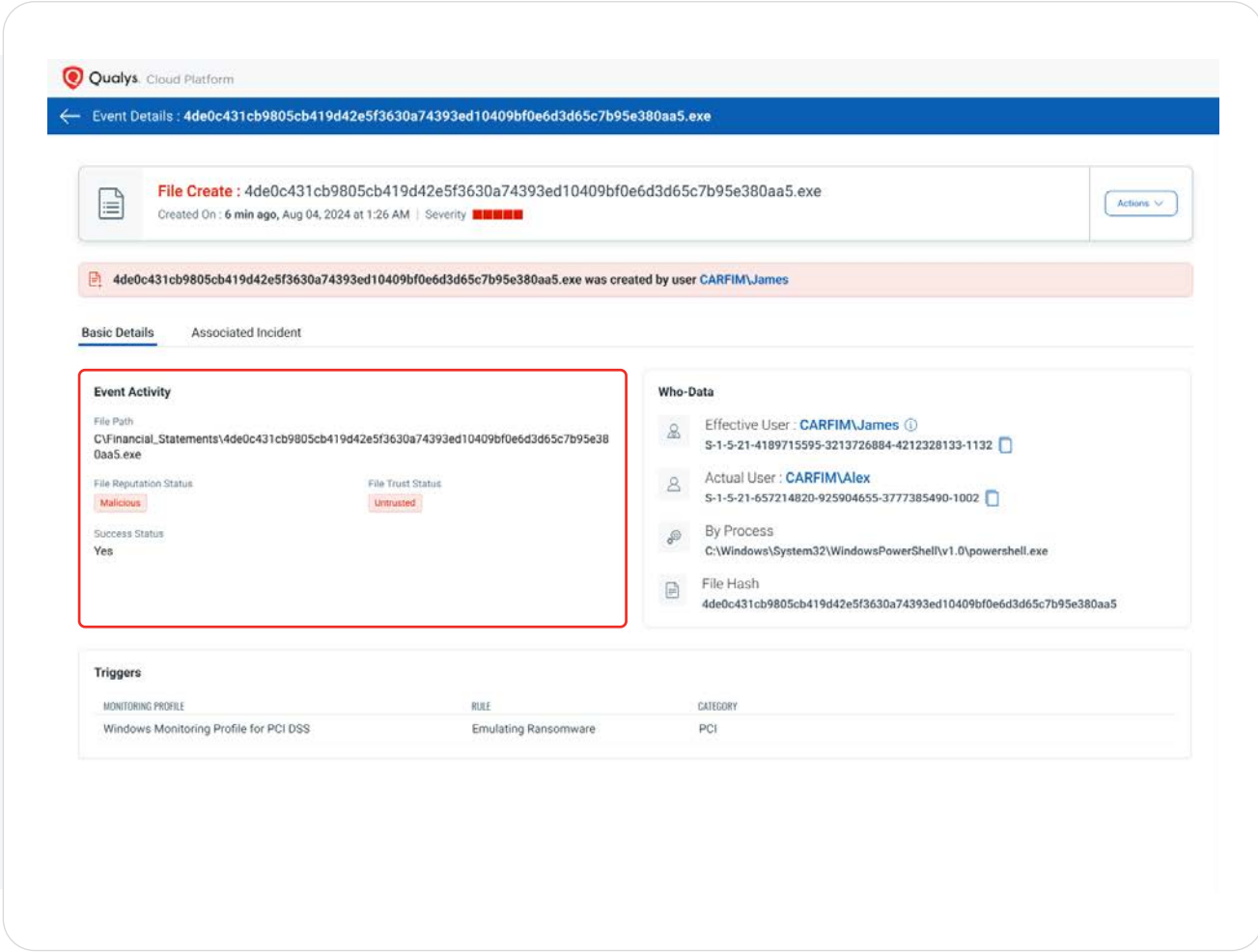
- Modification of access restrictions
- Modification of authentication or authorization mechanisms
- **Modification of logging procedures**
- Modification of the boot process
- Creation of new VLANs, tunnels or virtual interfaces
- Allowing outbound connections from a network device
- Enabling shell access



Integrated Threat Intelligence

Built-in threat intelligence enriches file reputation status for binaries and portable executable files

Quickly identify malicious or suspicious hashes in monitored locations



What You'll See in the Demo

- Easy onboarding
- Real-time alerts for Sensitive data access on containers
- User impersonation detection
- FIM on network devices
- Malicious hash detection
- Automated noise cancellation
- Automated FIM Report for PCI 4.0

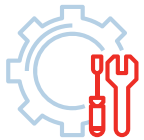
Demo

Qualys

Key Takeaways

Qualys FIM Highlights

No more manual reports



No more siloed tools

No more fire drills during Audits

No more being in Continuous Audit mode

PCI DSS 4.0 Ready

Latest Updates and Roadmap

Latest Updates

File Access Monitoring (FAM) to detect unauthorized access to sensitive data

FIM on containers

User impersonation detection

FIM on network devices

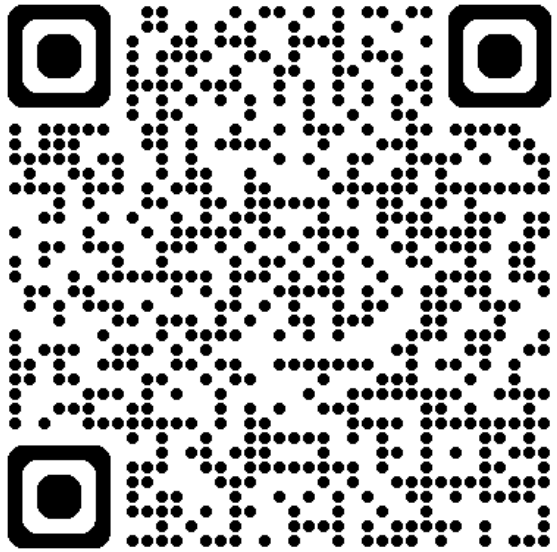
Roadmap

- Fully automated workflow for on-boarding FIM
- Automated noise cancellation
- Response capabilities in FIM – ability to execute commands or scripts on associated hosts in response to FIM events, enabling immediate action and remediation.
- Audit Trails in FIM to track FIM Profile modifications
- FIM Executive Summary Report

Transurban

Simon Gaiser – CISSP

Cyber Threat & Vulnerability Specialist, Transurban



Start Your 30-Day Free Trial of **Qualys FIM** and get executive FIM report for PCI 4.0

Qualys®