Winning the Battle Against Vulnerabilities & Unauthorized File Changes

Simon Gaiser – CISSP – Cyber Threat and Vulnerability Specialist

Simon Gaiser – CISSP

Cyber Threat & Vulnerability Specialist, Transurban

- Extensive experience in vulnerability management across sectors
- Including transportation, energy, and education
- Strong foundation in IT
- Native of South Africa, moved to Melbourne, Australia in 1988
- Married with four children

Overview of Transurban

1999

CityLink opened in 1999

22

Operate 22 roads, across 3 countries

Top 20

Top 20 ASX-listed company

446,000

Hours saved every workday

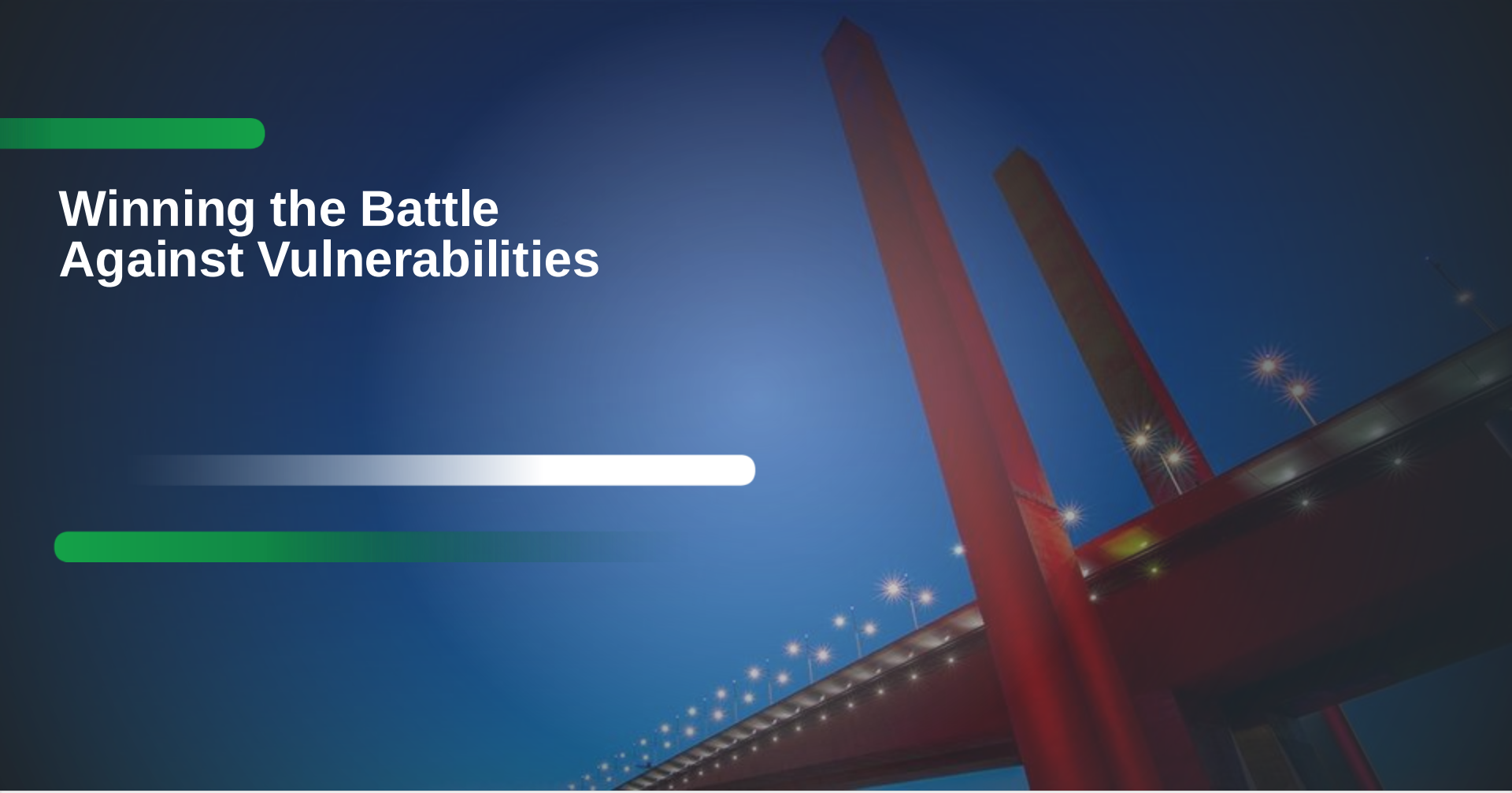
+4,100

Employees

10.8M

Customers across Australia and North America

Winning the Battle Against Vulnerabilities



Qualys Detection Score Enhanced Exploitable Rating

Qualys Detection Score

- CVSS Base Score
- Malware
- CISA Known Exploited Vulnerability (KEV)
- Trending Risk
- Real-Time Threat Indicators (RTIs)
- Threat Actors
- Exploit Code Maturity

Winning the Battle Against Vulnerabilities

Enhanced ratings prioritize actively exploitable vulnerabilities first

Lowering Transurban's cyber security risk

Reducing the risk of exposure or loss from a data breach

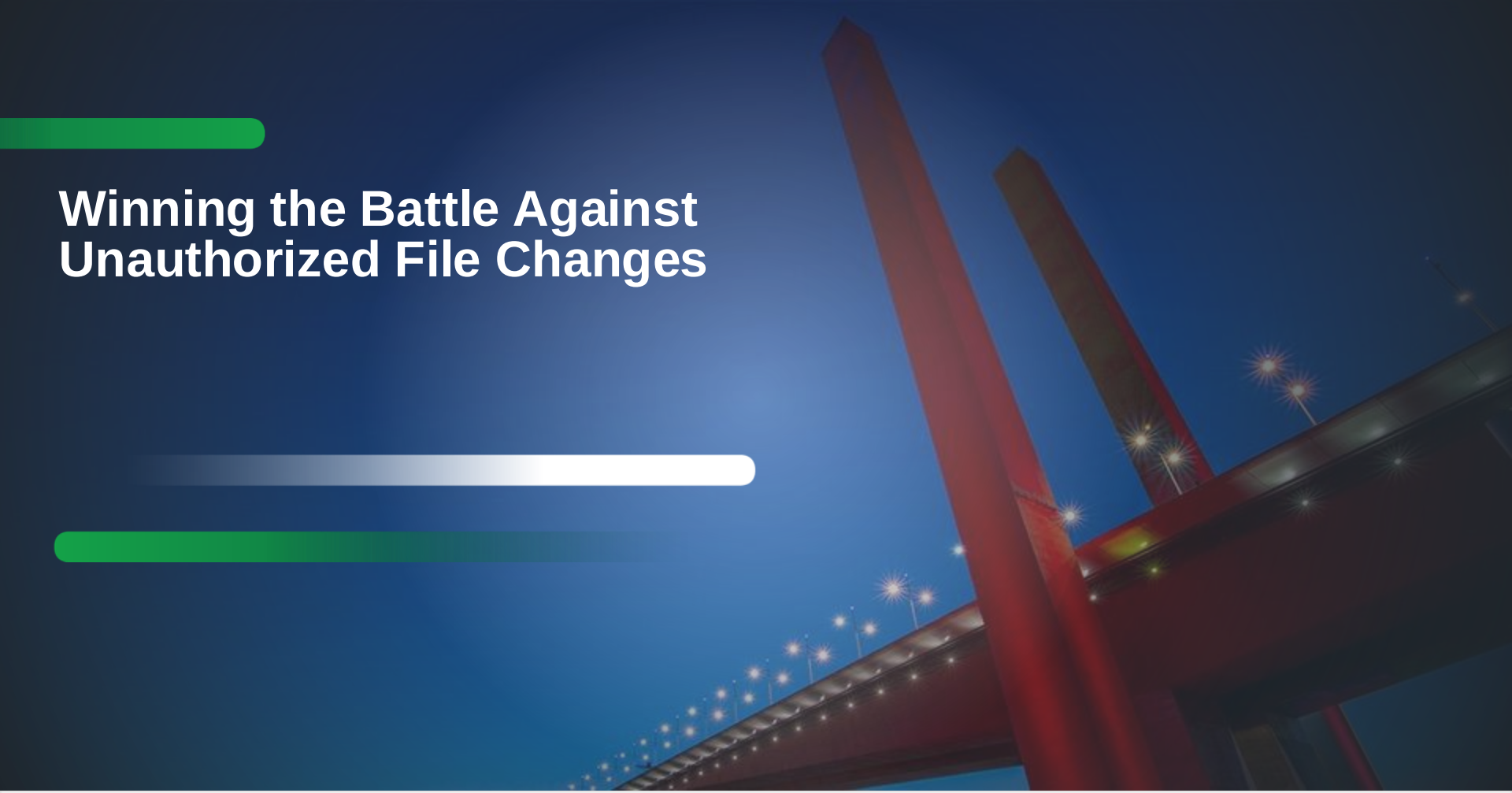
VMDR Outcomes

High/Critical decrease from 66% to 23%

Medium decrease from 27% to 17%

Low increase from 6% to 59%

Winning the Battle Against Unauthorized File Changes



About PCI

Organizations that handle credit card transactions,

like **Transurban,** are required to comply with the Payment Card Industry (PCI Security Standards Council) Standards.

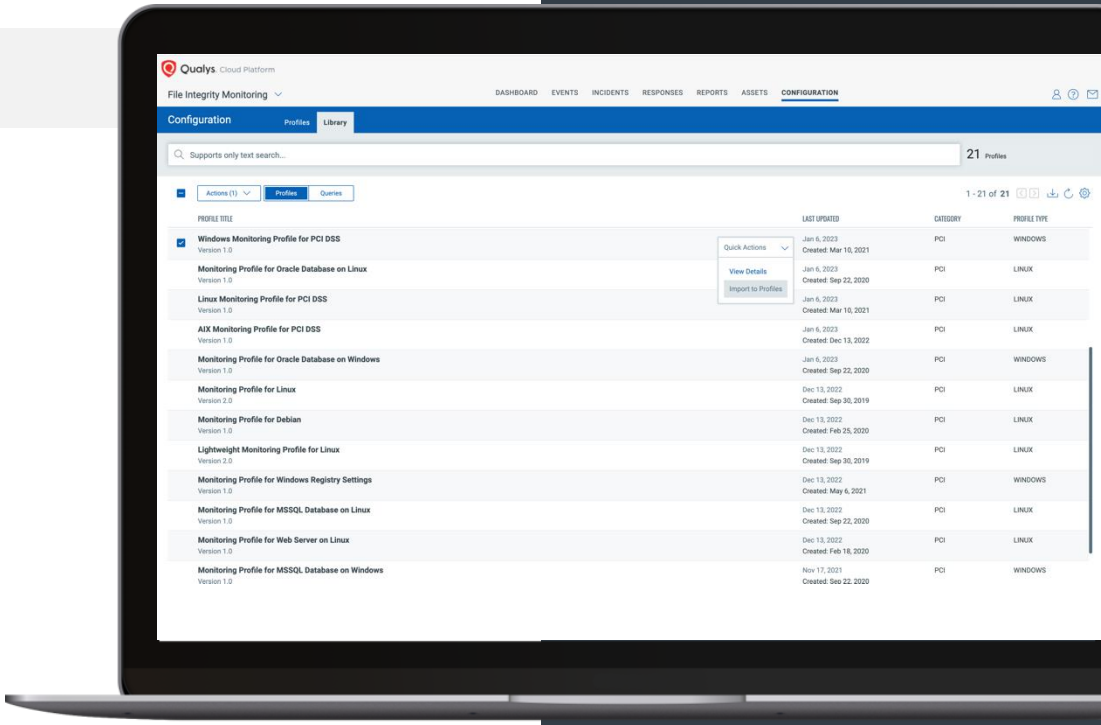
PCI DSS 4.0

Requires organizations to detect and respond to unauthorized changes in critical system files, configuration files, or content files, which is crucial for maintaining the security of cardholder data.

Eliminate Compliance Risk: Complete Coverage for PCI DSS 4.0 FIM

Requirements

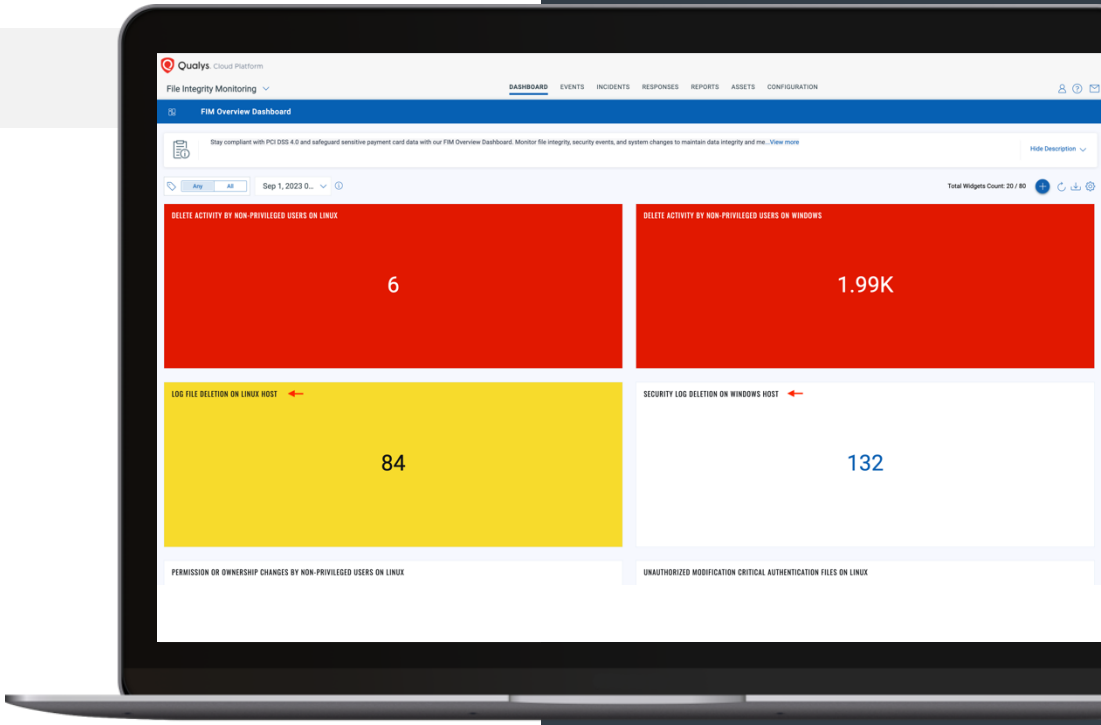
- **10.2.1** Audit logs are enabled and active for all system components and cardholder data.
- **10.2.2** Audit logs record the comprehensive details for each auditable event.
- **10.3.4** FIM to ensure that existing log data cannot be changed without generating alerts.
- **10.4.1.1 New Requirement:** Automated mechanisms are used to perform audit log reviews.
- **10.7.2 New Requirement:** Failures of critical security control systems, such as change-detection mechanisms, are detected, alerted, and addressed promptly.



Eliminate Compliance Risk: Complete Coverage for PCI DSS 4.0 FIM

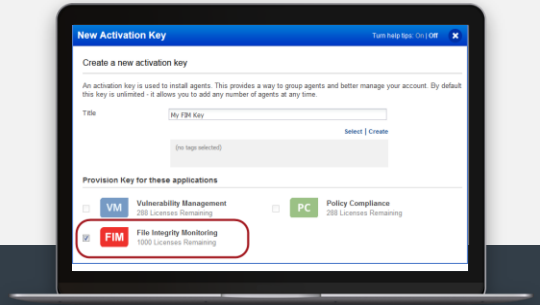
Requirements

- **7.2.4** Ensure user accounts and access remain appropriate based on job function.
- **10.5.1** Data retention for **at least 12 months,** with at least the most recent three months immediately available for analysis.
- **11.5.2** A change-detection mechanism (FIM) is deployed.
- **12.10.5** The security incident response plan includes monitoring and responding to alerts from Change-detection mechanisms for critical files.
- **A3.5.1** A methodology is implemented to promptly identify attack patterns and undesirable behavior across systems.

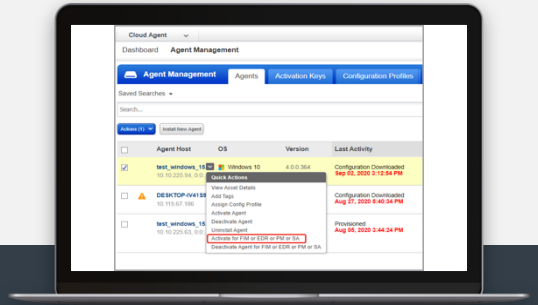


Qualys FIM Implementation at Transurban

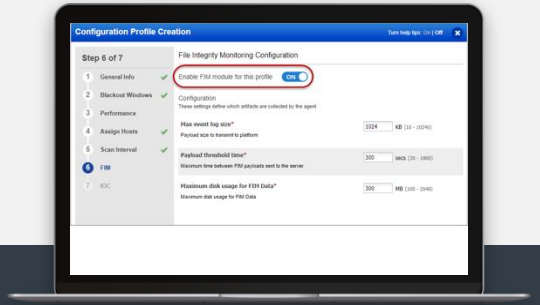
Install Cloud Agents & Activate File Integrity Monitoring



Enable the FIM Module on a Host with the Qualys Agent Already Installed



Activate FIM in a CA Configuration Profile



Transurban Implementation: Agent -> Splunk -> ServiceNow Incident

01	02	03	04	05	06	07	08
Agent deployed	FIM enabled for agent	Profiles applied	Events Correlated to Incidents	Integration with Splunk	Splunk Phantom creates incident in ServiceTU	Cyber Defence respond to incident	Dashboards for reporting

Winning the War Against Unauthorized File Changes

The Case for Qualys File Integrity Monitoring (FIM)

Qualys.
File Integrity Monitoring

- Simplified PCI DSS Compliance and readiness for PCI DSS 4.0
- FIM is available with Qualys agent, along with VM, PC, Patch, EDR
- Operational cost reduction
- Fast and easy to deploy: One-click activation.
- Administrative overhead reduction
- Effective noise cancellation and native integration with SIEM
- Vendor rationalization and consolidation

File Integrity Monitoring

Ready for PCI DSS 4.0

Comprehensive FIM Solution: Agent-based and agentless deployment options. Coverage for Servers, Endpoints, Network devices, **Containers** and more.

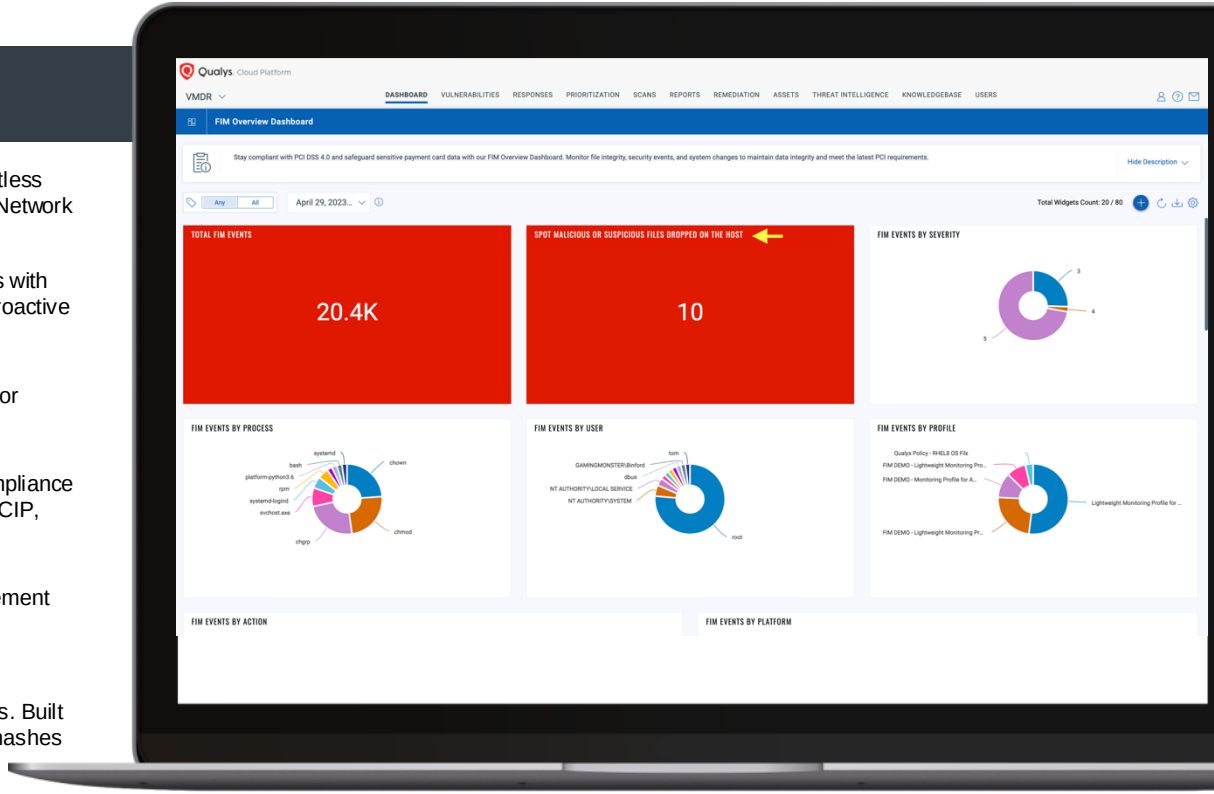
File Access Monitoring (FAM): Empowers SOC teams with real-time alerts for access to sensitive data, ensuring proactive threat response

Save Analyst Time: Ready-to-use, fine-tuned profiles for compliance frameworks, streamlining setup

Reduce Compliance Risk: Comply with regulatory compliance frameworks such as PCI DSS 4.0, HIPAA 2023, NERC CIP, GDPR, CCPA and NIST CSF 2.0, NIS2

Stay Audit Ready: Built-in automated Incident Management and Compliance Reporting

Minimized Alert Fatigue with Noise Cancelling FIM: Eliminate 90%+ of noise for trusted users and processes. Built in Threat Intelligence to detect malicious or suspicious hashes




Transurban
Questions?
Simon Gaiser