2025 NORTH AMERICA COMMUNITY MEETING

Cloud Security & Vulnerability Management

Convergence of Robust Cloud Security Practices and a Mature Vulnerability Management Program

PCI Security Standards Council

Kevin Simmonds

CISSP

Partner / Principal

PricewaterhouseCoopers (PwC)

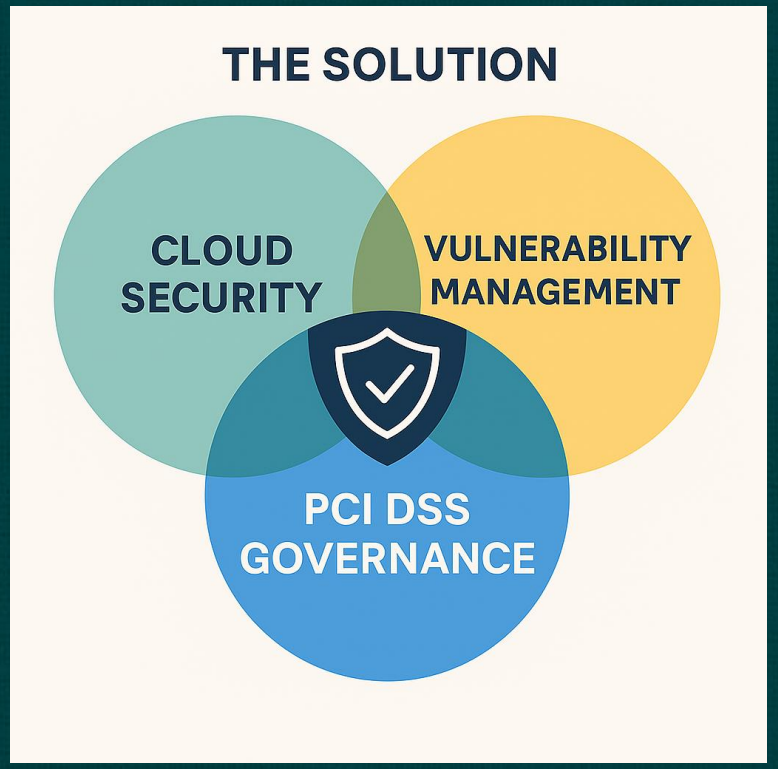
Kevin.Simmonds@pwc.com

pwc

PCI Security Standards Council

Problem Statement and Desired Outcome

How do we ensure our Vulnerability Management (VM) program is operating effectively, not overlooking cloud assets/environments, fortifying the organization, and designed to achieve PCI compliance?



PCI Security Standards Council

Common challenges organizations face…

Cloud Operations

- Nonexistent or outdated cloud security controls framework
- Neglecting security controls during the design stage
- Immature or absence of a DevSecOps model
- No Cloud Native Application Protection Platform (CNAPP)

Vulnerability Management Program

- Primarily focused on traditional infrastructure (e.g., cloud-native assets omitted)
- Inconsistently ingesting or review of vulnerabilities from other sources
- Cloud security knowledge gap

PCI DSS Governance

- Unknow control owner for cloud assets and/or environments
- Inconsistent tracking of scanning and remediation SLAs across technology / environments

Cloud Security

PCI Security Standards Council

Where should you focus along the journey

People, Process, and Technology

People:

- Ensure you have / identify the right resources to create effective collaboration across the cloud team(s), Information Security department, and PCI Compliance team

Process:

- Design practical processes to achieve the desired outcomes across team - - having additional headcount and acquiring new tools is not enough

Technology:

- Identify which solutions are best for your organization to create efficiencies and support defined processes

Leading Cloud Security Practices to Consider*

Cloud Security Controls Framework

- Ensure controls for all applicable Cloud Service Providers (CSPs) are included
- Provide mapping to PCI DSS reqs. and other applicable frameworks
- Provide specific config details

Operationalize Cloud Security Solutions

- Leverage a CNAPP or comparable solutions to identify configuration gaps and PCI non-compliance
- Automating compliance checks via CNAPP, CSPM, or IaC tools, via periodic scanning

Security Automation and DevSecOps Integration

- Integrate security checks into CI/CD pipelines (e.g., IaC scans, container scanning).
- Automate responses to common alerts (e.g., quarantining resources, revoking keys).

Data Protection and Encryption

- Encrypt data at rest and in transit using strong encryption (e.g., AES-256, TLS 1.2+).
- Manage encryption keys securely (e.g., AWS KMS, Azure Key Vault).

* This is not an exhaustive list

PCI Security Standards Council

CNAPP: Supporting compliance in the cloud

A **CNAPP** is a unified security solution that integrates multiple cloud-native security functions, including Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), Cloud Infrastructure Entitlement Management (CIEM), Vulnerability Management, and Compliance Monitoring.

CNAPP Capability	PCI DSS Requirement(s)
Asset Inventory	Req. 2.4, 2.5.1
Posture Management	Req. 2.2.1, 5.2.2
Vulnerability Mgmt	Req. 6.3.1, 11.3.1.2
IAM Governance	Req. 7.1, 7.2
Logging & Monitoring	Req. 10.2, 10.4.1.1
Compliance Reporting	Req. 12.1, 12.5.2

PCI Security Standards Council

Vulnerability Management

PCI Security Standards Council

Leading VM Practices for Cloud*

VM must evolve beyond traditional on-premise scanning to handle ephemeral, distributed, and cloud-native workloads

1. **Continuous and Context-Aware Scanning**
   - Continuous discovery and scanning of cloud assets, including ephemeral resources like containers and serverless functions.
   - Context-aware scanning that prioritizes vulnerabilities based on: (1) Internet exposure, (2) Asset criticality, (3) Workload privilege levels, and (4) Cloud account or subnet segmentation.
2. **Risk-Based Prioritization**
   - Dynamic risk scoring that combines CVSS, exploitability, asset value, and cloud-specific context.
3. **Shift Left: Vulnerability Scanning in CI/CD Pipelines**
   - Scanning container images, IaC templates, and dependencies as part of CI/CD pipelines before deployment.
   - Enforcement gates to block builds with high-severity CVEs or misconfigurations.
4. **Asset-Centric VM in Multi-Cloud Environments**
   - Ability to scan workloads deployed across AWS, Azure, and GCP from a single platform.

* This is not an exhaustive list

PCI Security Standards Council

Leading VM Practices for Cloud* (cont.)

5. **Integrated Remediation Workflows**
    - Automated ticket generation in Jira, ServiceNow, or Slack based on severity and context.
    - Auto-remediation or guided fixes for common findings (e.g., updating base container images, removing insecure packages).
6. **Compliance-Ready Reporting and Evidence Collection**
    - Real-time dashboards and compliance reporting mapped to frameworks like PCI DSS.
    - Automated evidence collection to streamline audits (e.g., proof of patching, scan logs, exception approvals).
7. **Vulnerability Management for Serverless and Managed Services**
    - Runtime behavior analysis of serverless functions.
    - Dependency and permission analysis to flag vulnerable packages and over-permissive roles (e.g., AWS Lambda running outdated SDKs with AdministratorAccess).
8. **Use of AI/ML for Anomaly Detection in Vulnerability Trends**
    - Detect unusual spikes in vulnerability exposure.
    - Suggest remediation paths based on environment-specific learning.

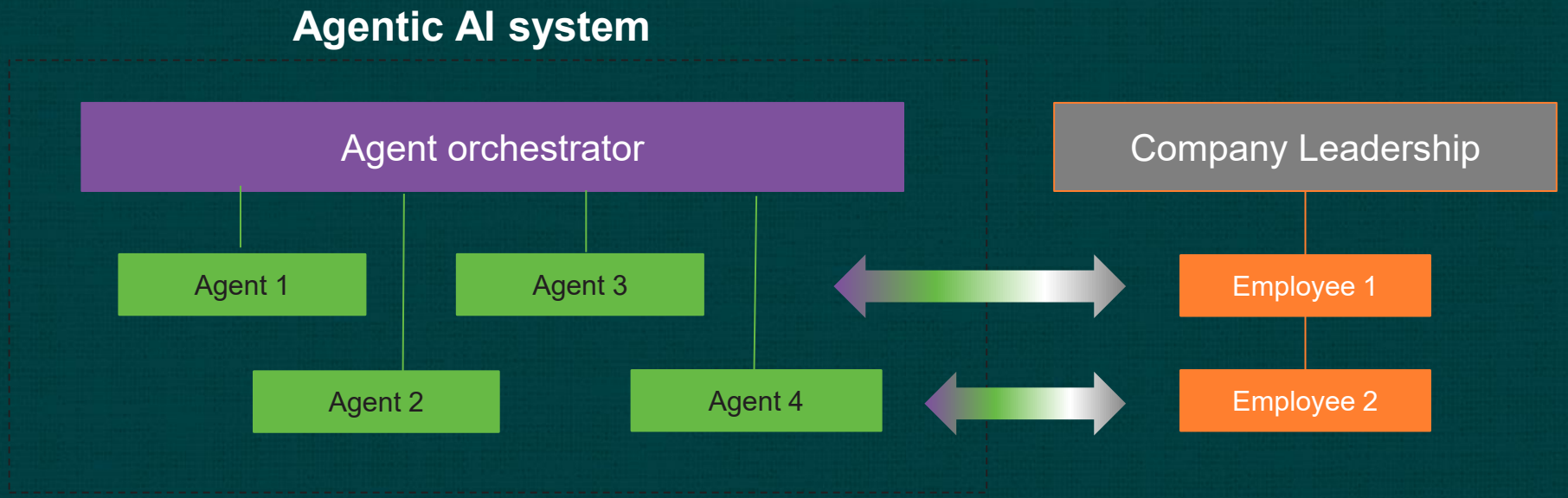
* This is not an exhaustive list

Agentic AI for VM

PCI Security Standards Council

What is Agentic AI?

Agentic AI systems are designed to autonomously make decisions and pursue complex goals with limited supervision.

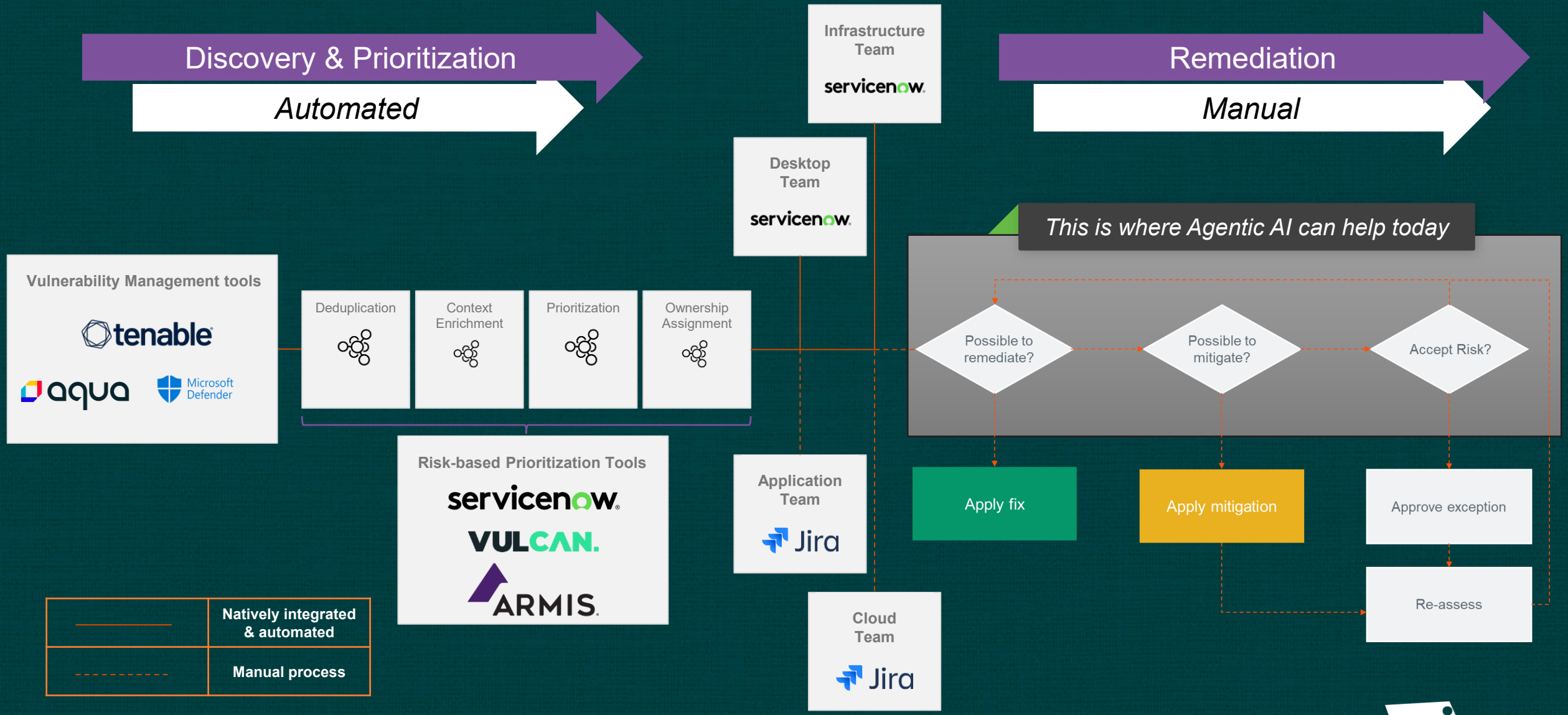


An *agentic AI system* tackles high level goals, with a level of autonomy and flexibility, using an 'agent orchestrator' and individual 'agents'

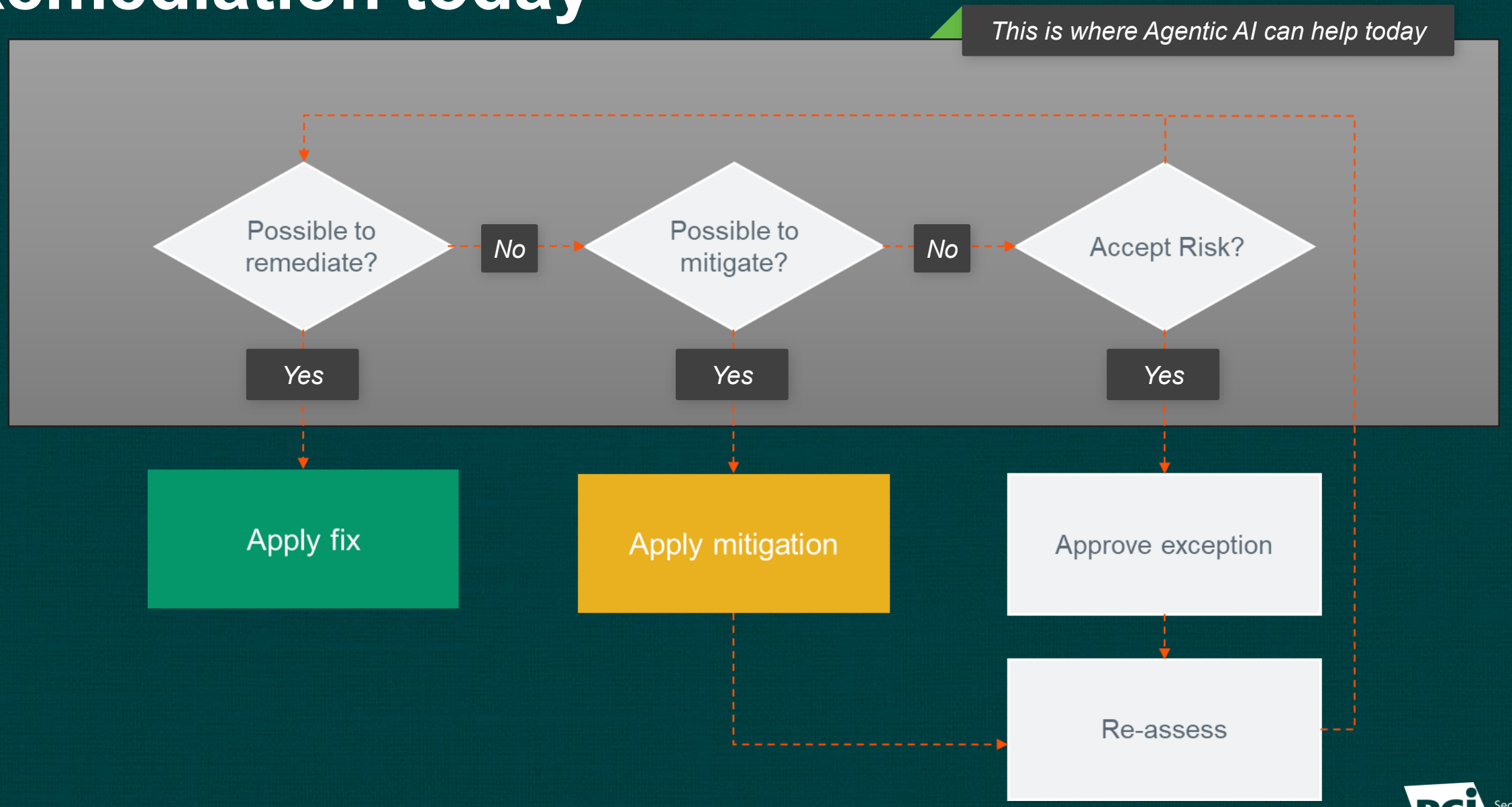
The *agent orchestrator* interacts with humans and co-ordinates the activity of multiple individual *agents*, ensuring they work efficiently to tackle the system's overall goals

An *AI agent* performs a defined task with a degree of autonomy, and acts within specified guardrails to maintain control and alignment

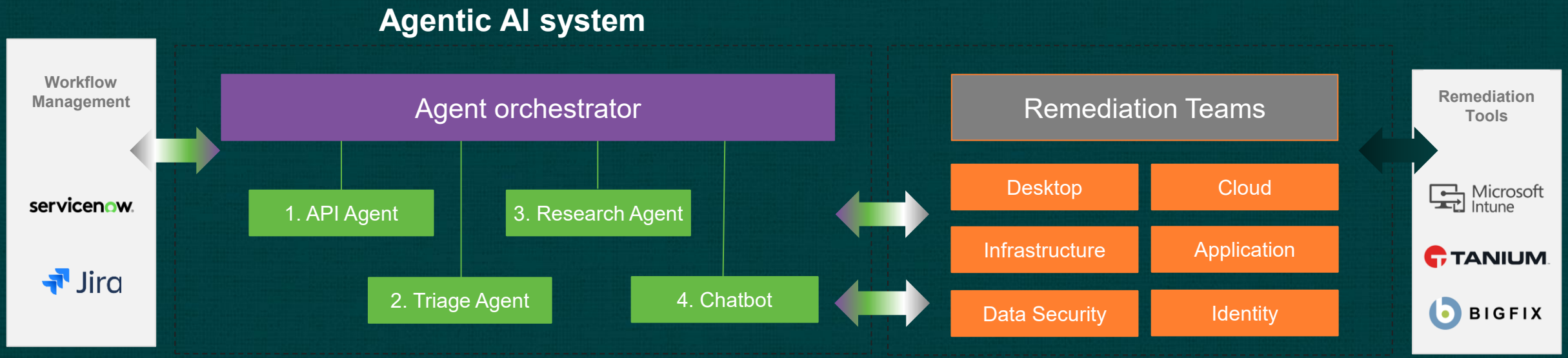
Remediation today



Remediation today



How does Agentic AI help?



1. API Agent

Allows the Agentic AI system to talk to ServiceNow, Jira, and more. The API agent can search within ServiceNow to find the owner, system, and application information.

2. Triage Agent

Watches for new Vulnerability Tickets to be created in ServiceNow and Jira. Works with the Research Agent to analyze the finding and provides contextually relevant, tactical remediation guidance.

3. Research Agent

Researches findings online using the latest data from software vendors and publicly available threat intelligence sources to verify which exposures are low priority, and which are urgent.

4. Chatbot

A friendly and helpful support bot that interacts directly with the remediation teams and helps them re-assign tickets, raise exceptions, or submit change requests to fix the exposure.

The Convergence

PCI Security Standards Council

Cloud Security + VM + PCI Governance = ….

- Maintain a strong cloud security **control framework** and cloud security requirements
- Track and drive remediation **consistently across cloud assets**

+

- Combine cloud scanner alerts (e.g., CNAPP) and VM scan results into a **compliance-aligned dashboard**
- **Leverage AI** to enhance analysis, communication, and remediation of gaps

=

- **Clearer expectations** for control owners
- **Better integration** with SecOps and related processes
- **Reduced** audit readiness efforts and annual cost

PCI Security Standards Council

Thank you!

Kevin Simmonds
kevin.simmonds@pwc.com

PCI Security Standards Council