

RISK ENABLED GROWTH

EXECUTIVE SERIES

How?

create a 'risk optimized'
organization to achieve
strategic goals and
capitalize on growth
opportunities

online

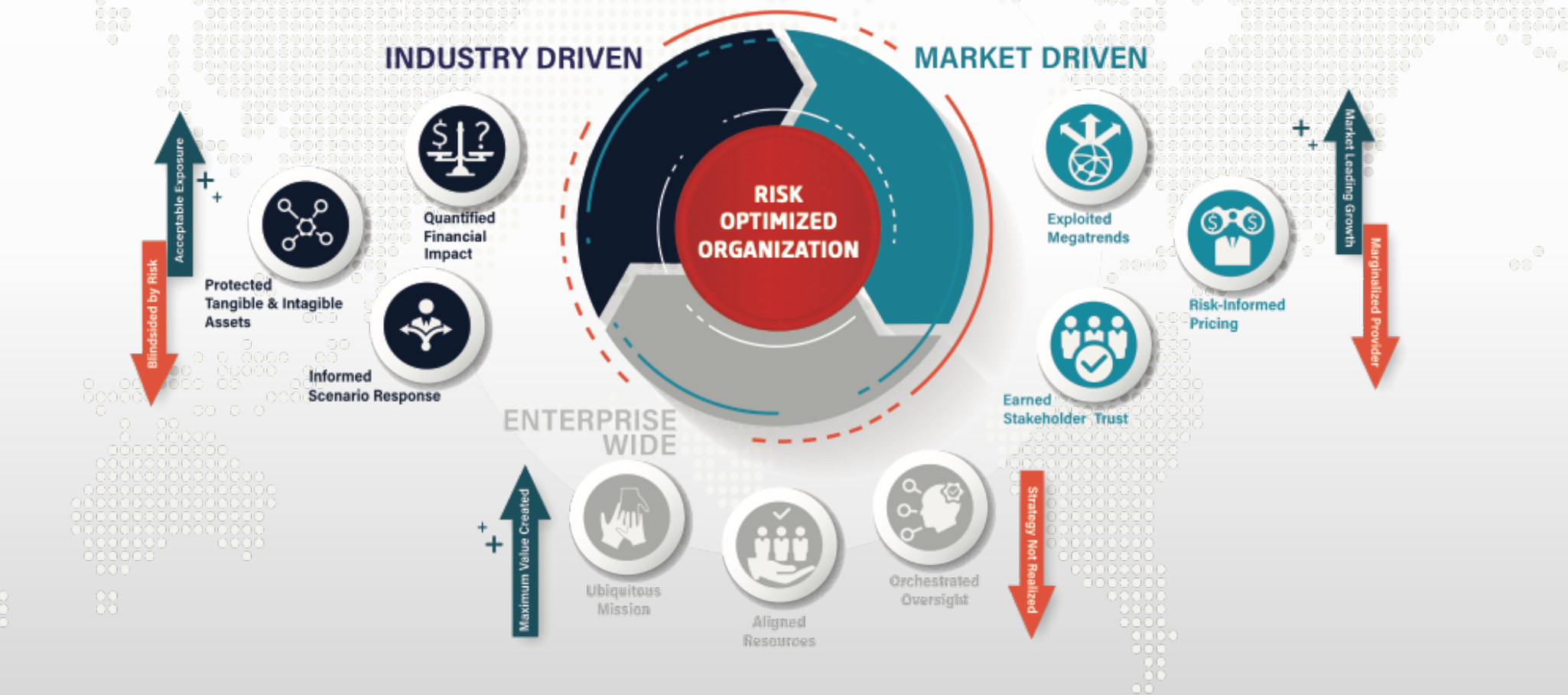


Tauruseer

RISKNEUTRAL

INTEGRATED RISK MANAGEMENT

Minimizing Deviation from Expected Outcomes is Highly Valued by Key Stakeholders





ENTERPRISE WIDE

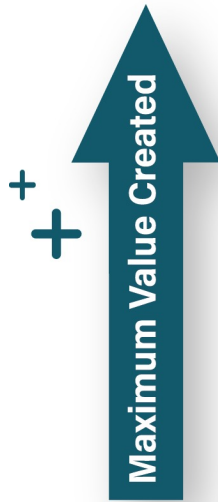
Ubiquitous mission



Aligned resources



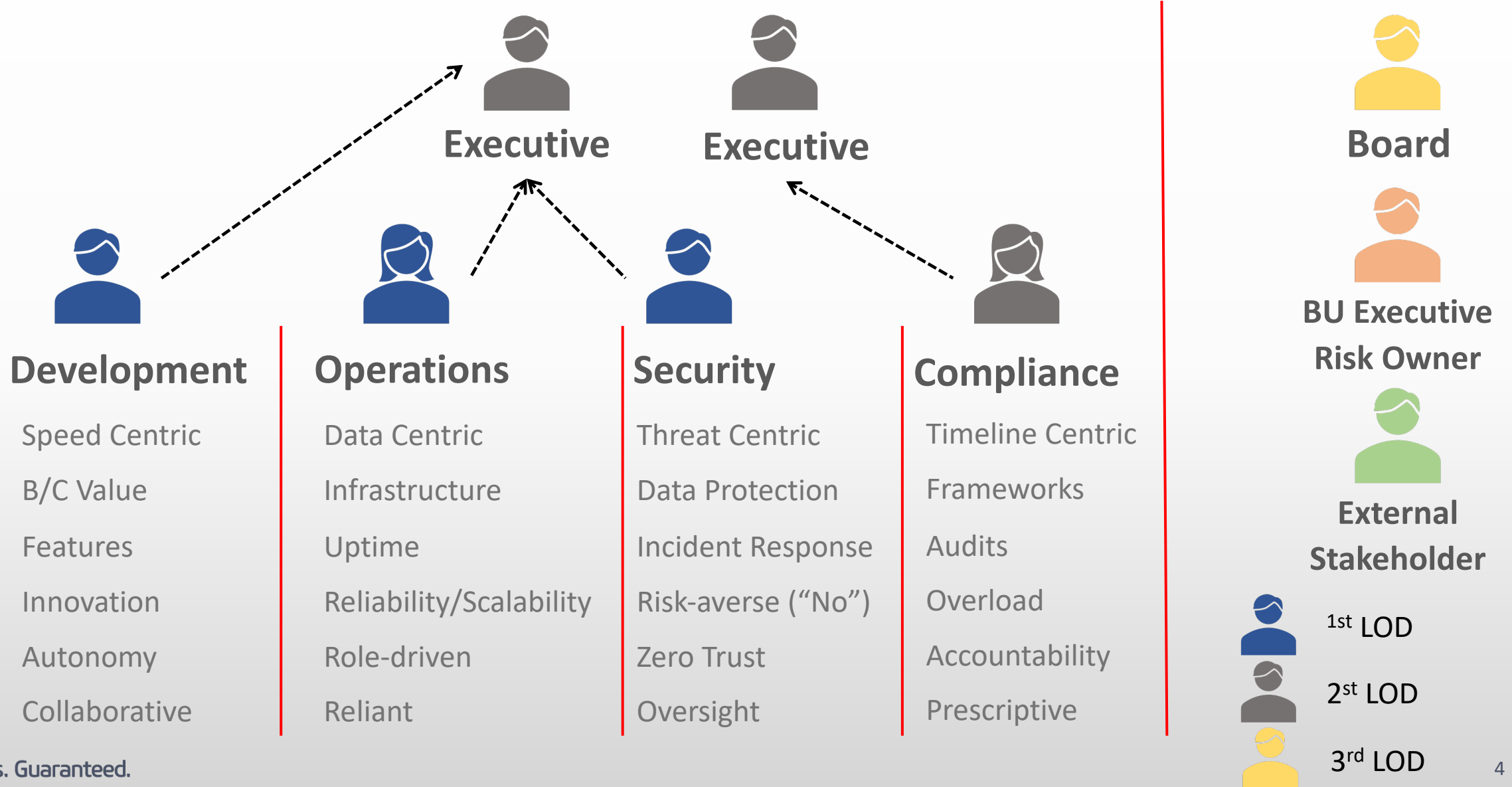
Orchestrated oversight



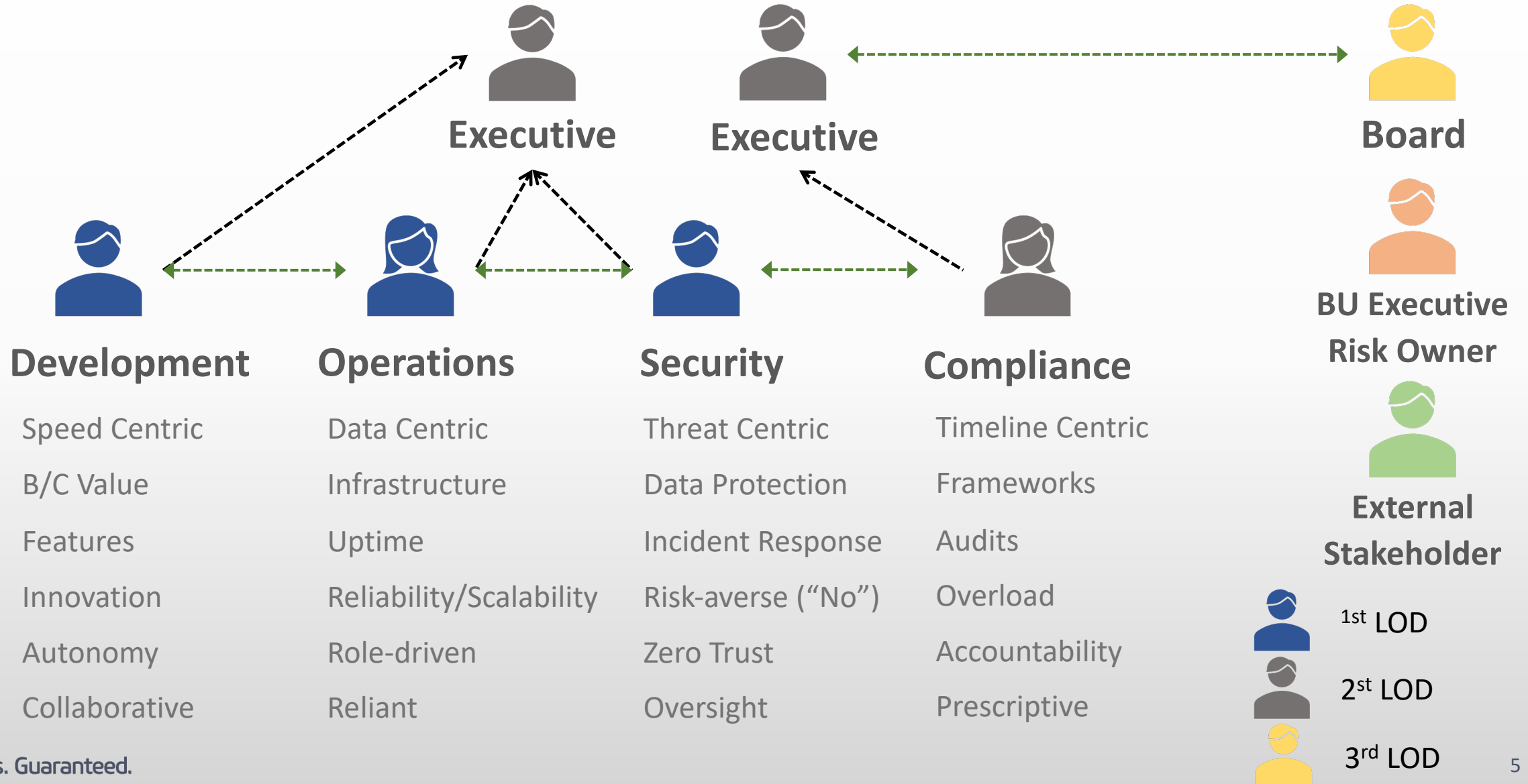
Board and C-Suite require adequate visibility to provide sound governance over current and emerging risks across all five core risk domains (Strategy, Operations, Finance, Compliance, and Reputation)



Challenges – Competing Objectives & Incentives (3LOD)



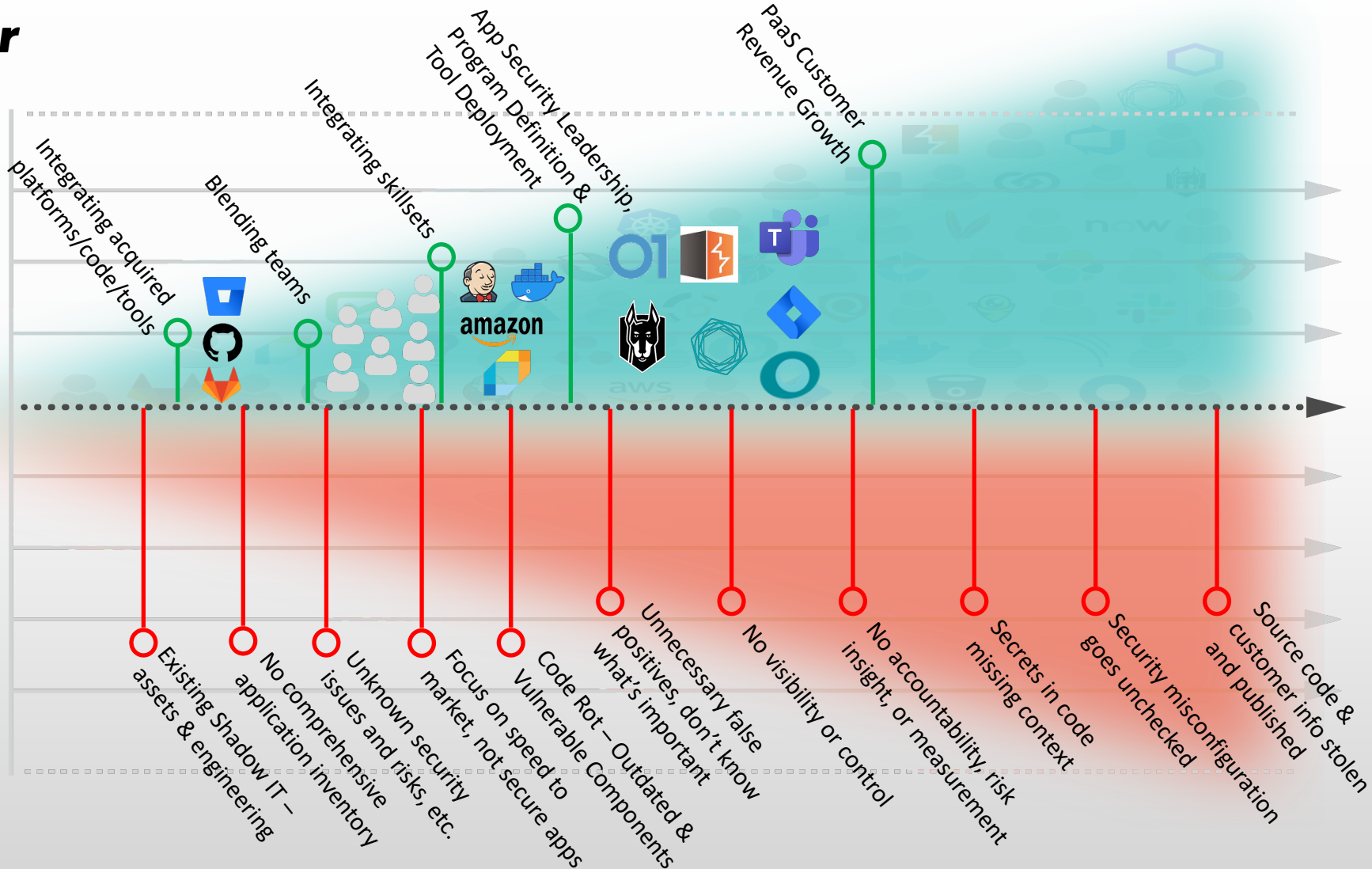
Challenges – Competing Objectives & Incentives (3LOD)



No Visibility, Control, Context with Point Solutions

Supporting corporate growth strategy

You can't manage what you can't see.



- Negative Impact
- Positive Impact
- Industry Impact

There are only TWO choices...

REACTIVE



Hacker-Led



Customer-Led



Stakeholder-Led

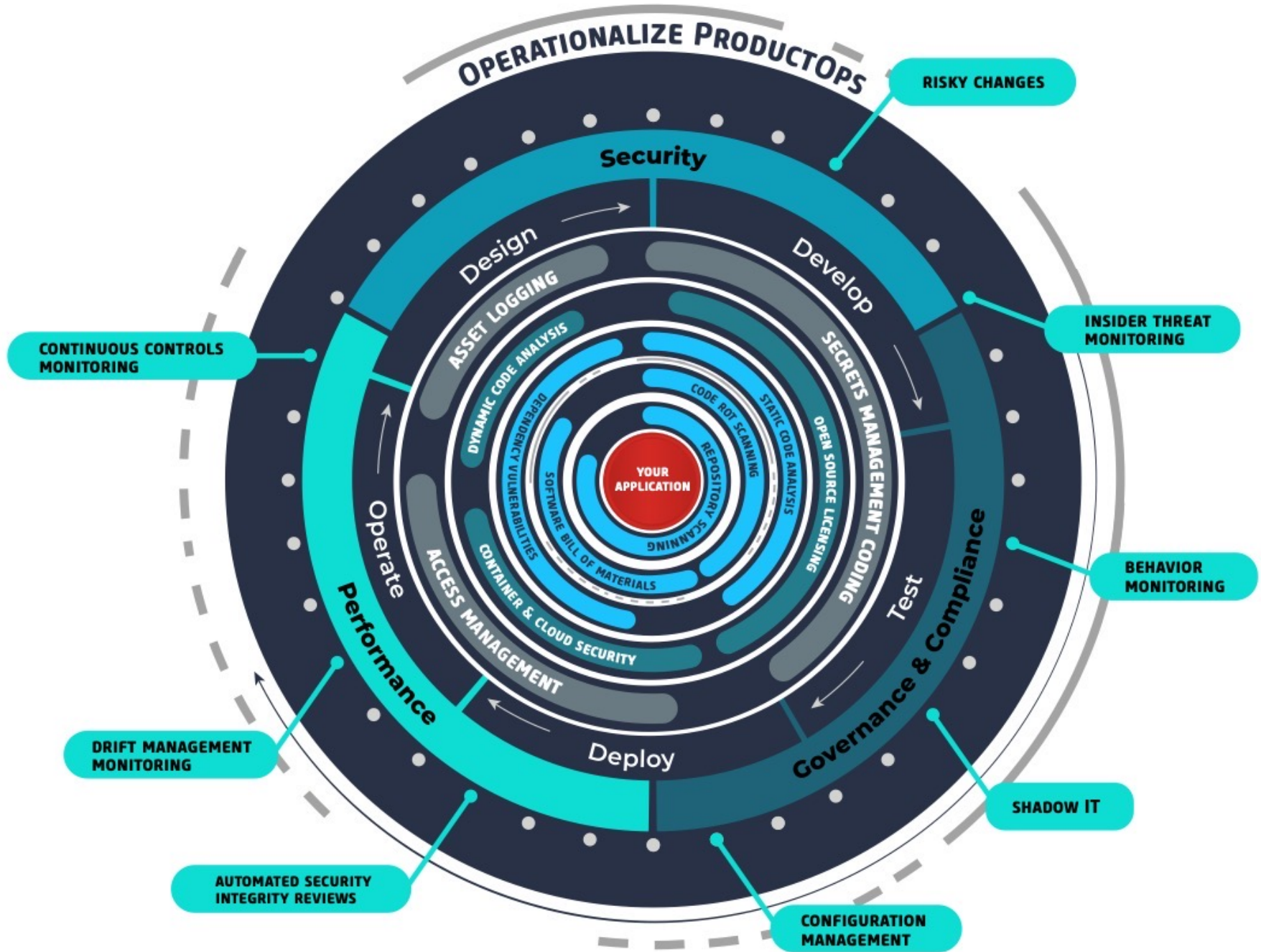


PROACTIVE



Board/Executive-Led





Cognition Construction

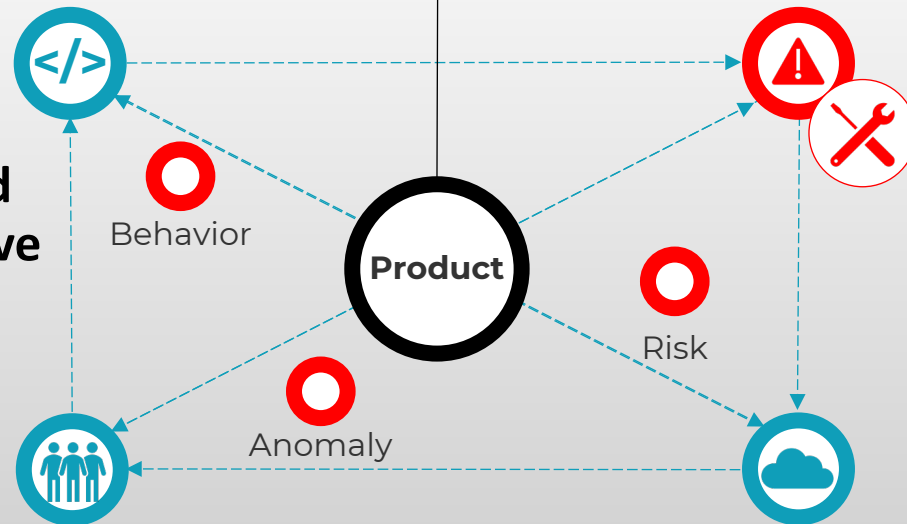
- Operationalizing risk management
 - Context and analytics at scale is the key to protecting growth
- SolarWinds, Amazon, Twitch, etc. wanted to know: what is the best predictor of long-term product security

The answer: automating an intelligent infrastructure to correlate people, process, technology, and behaviors

How do you figure this out?

Behavioral cohorting

Correlate anomalies, scenarios and high-risk combinations (pre-engineered measurements considering retrospective and real-time data)



Risky Behavior Detected

Commit Activity Without Work Item Activity

Misconfiguration Detected

No Longer Receiving Code Vulnerability Scanning Data

Threat Detected

Former Team Member Committed to Source Code Repository



Systemic risk treatment and continuous assurance

- Forms part of ubiquitous mission objectives within an organization to integrate a cognitive, risk-based culture
- Contributes towards aligning resources within an organization as far as assurance is concerned
- A mature risk management framework would generally define the criteria against which assets are measured.

- Prelude the next slides by establishing a baseline, using an industry prescriptive standard, for software development.
- The standard could not be directly associated with your organization, however the industry best practice ethos and methodologies are applicable to a vast amount of organizations
- PCI SSF (SLC)

Software Security Governance



Standards & Regulatory

- Senior leadership is required to establish formal responsibility for the security of software, authorize roles, assign responsibilities, and provide accountability within the development lifecycle (CO-1)
- Required to provide regular status updates to senior leadership on status, performance and changes to development initiatives at least annually or more regularly within significant changes to product.
(Anniversary/Periodic/Significant change) – contagion
- Ensure a software assurance program is established.
- Includes regular checkpoints, including use of reviews, scans, and automated tools

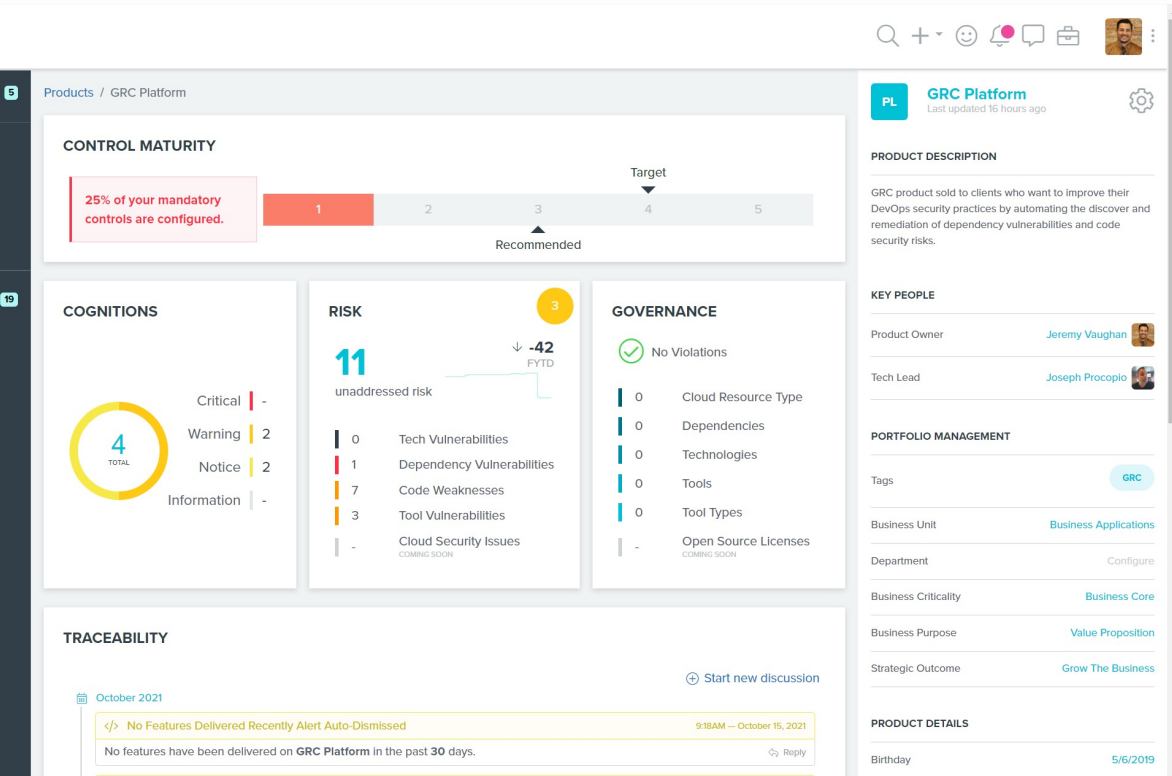
Platform Deliverables

- Product/App Inventory & Status/Traceability
- Risk Ownership / Performance
- Portfolio Management
- Heuristic Analysis (MITRE)
- Individual Contributor Metrics
- Configurations & Controls Monitoring
- Workflow Orchestration
- Cognition Alerting
 - Statistical Analysis / Trend Differentiations*
 - Anomalies



RO

Tauruseer roles and responsibilities and workflow approval process.



CONTROL MATURITY

25% of your mandatory controls are configured.

Target: 4 (Recommended)

COGNITIONS

4 TOTAL

- Critical: 0
- Warning: 2
- Notice: 2
- Information: 0

RISK

11 unaddressed risk

-42 FYTD

- 0 Tech Vulnerabilities
- 1 Dependency Vulnerabilities
- 7 Code Weaknesses
- 3 Tool Vulnerabilities
- 0 Cloud Security Issues (COMING SOON)

GOVERNANCE

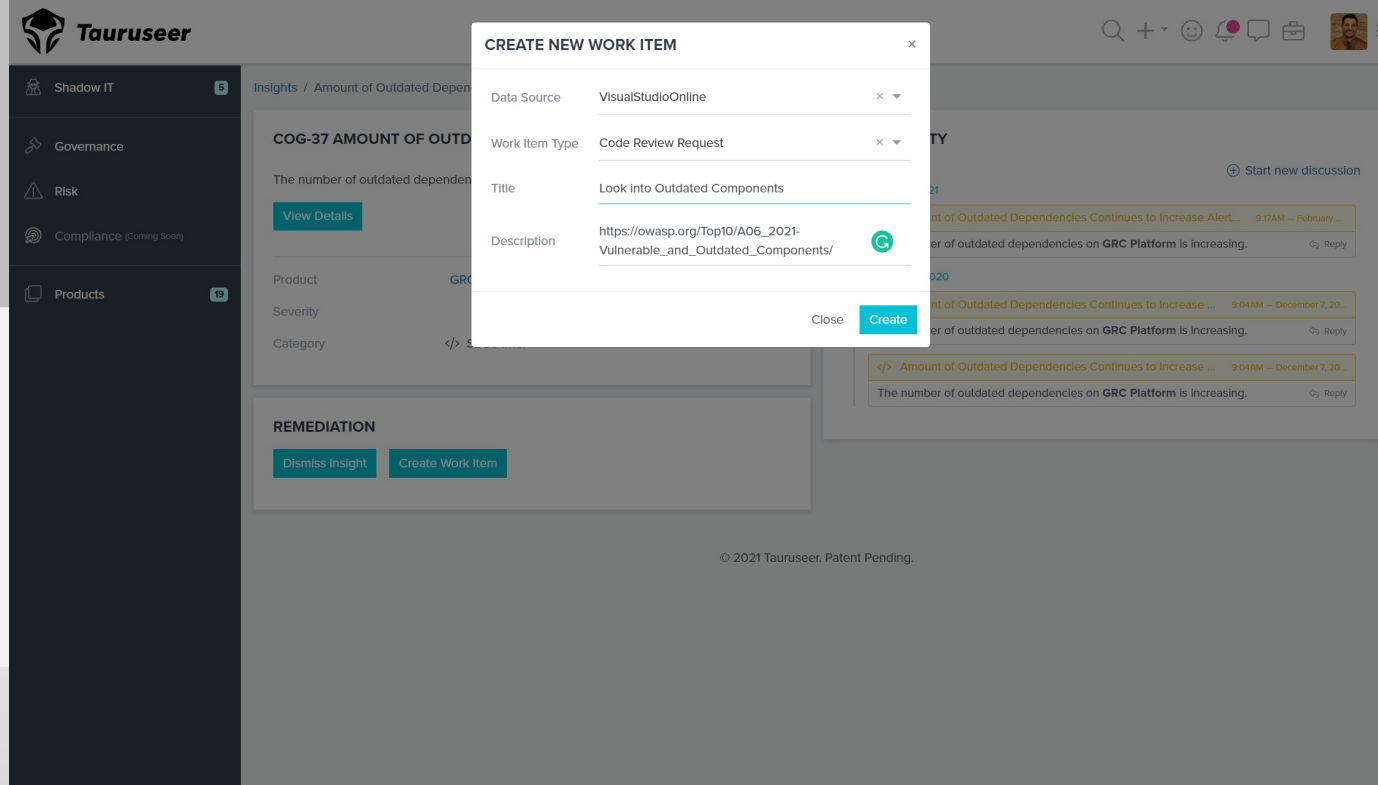
No Violations

- 0 Cloud Resource Type
- 0 Dependencies
- 0 Technologies
- 0 Tools
- 0 Tool Types
- 0 Open Source Licenses (COMING SOON)

TRACEABILITY

October 2021

No features have been delivered on GRC Platform in the past 30 days.



TAURUSEER

Shadow IT

Governance

Risk

Compliance (Coming Soon)

Products

INSIGHTS / Amount of Outdated Dependencies

COG-37 AMOUNT OF OUTDATED DEPENDENCIES CONTINUES TO INCREASE ALERT

The number of outdated dependencies on GRC Platform is increasing.

View Details

Product: GRC Platform

Severity: High

Category: Vulnerability

REMEDATION

Dismiss Insight

Create Work Item

CREATE NEW WORK ITEM

- Data Source: VisualStudioOnline
- Work Item Type: Code Review Request
- Title: Look into Outdated Components
- Description: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Close Create

© 2021 Tauruseer, Patent Pending.

Secure Software Engineering



Standards & Regulatory

- All critical assets are required to be defined
- Perpetual identification and addressing of threats and vulnerabilities is required as a BAU process (remediation turnaround timelines)
 - Within code
 - Against interfaces
 - Defined scenarios
- Third Party and open-source components require inclusion into vulnerability management and ongoing monitoring for vulnerabilities.
- Enforceable remediation is a core component of any systemic risk treatment program

Platform Deliverables

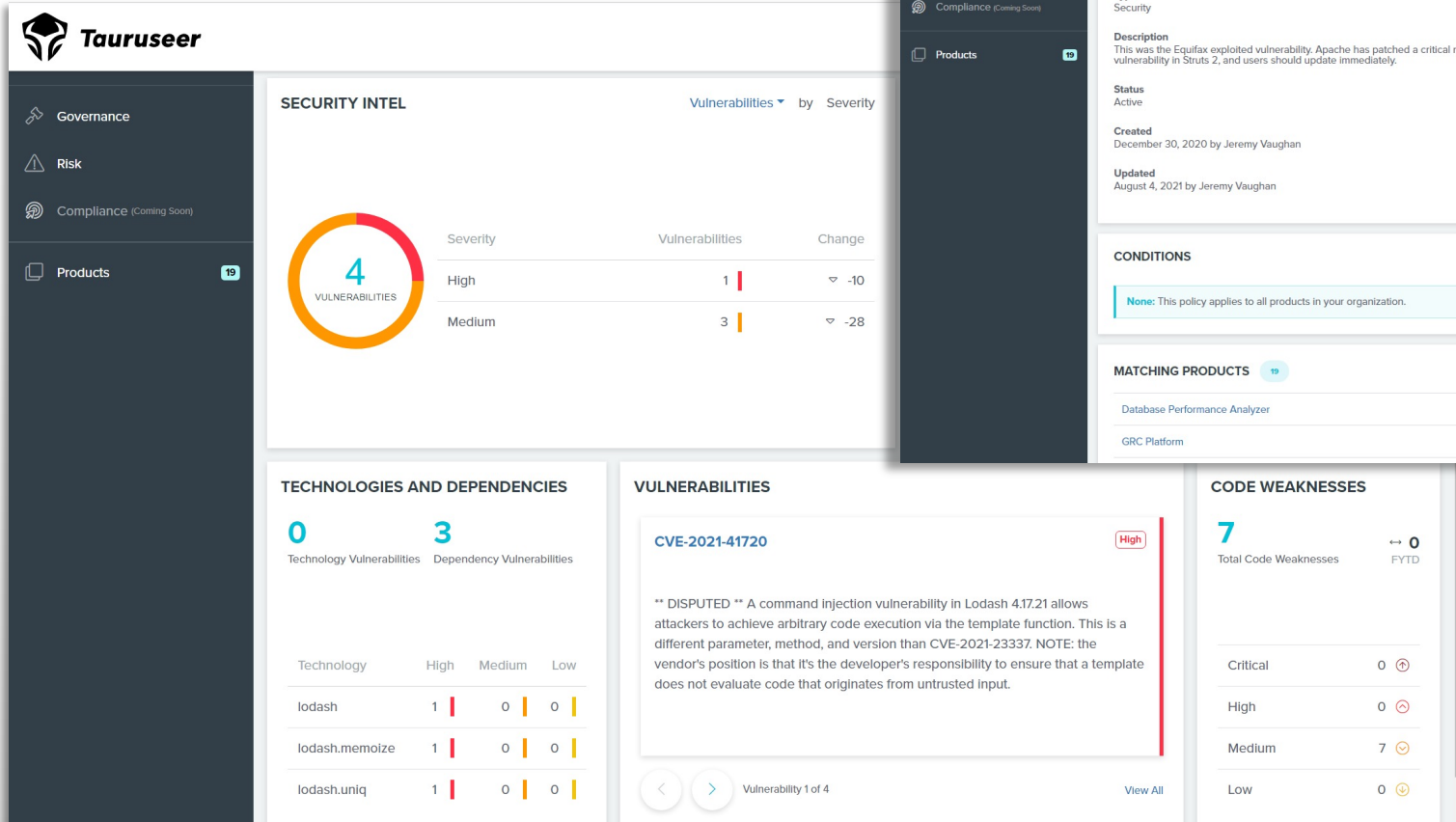
- Orchestrated oversight
- Insider Threat
- Shadow IT & Shadow Engineering
- Software Bill of Materials
- Open-Source / Dependency Vulnerabilities
- Tech, Tool & Cloud Vulnerabilities
- Code Weaknesses
- Policy Enforcement

- Cognition Alerting
 - Statistical Analysis / Trend Differentiations*
 - Anomalies



SO

Tauruseer vulnerability and drift management.



SECURITY INTEL Vulnerabilities by Severity

Severity	Vulnerabilities	Change
High	1	-10
Medium	3	-28

TECHNOLOGIES AND DEPENDENCIES

0 Technology Vulnerabilities | 3 Dependency Vulnerabilities

Technology	High	Medium	Low
lodash	1	0	0
lodash.memoize	1	0	0
lodash.uniq	1	0	0

VULNERABILITIES

CVE-2021-41720 High

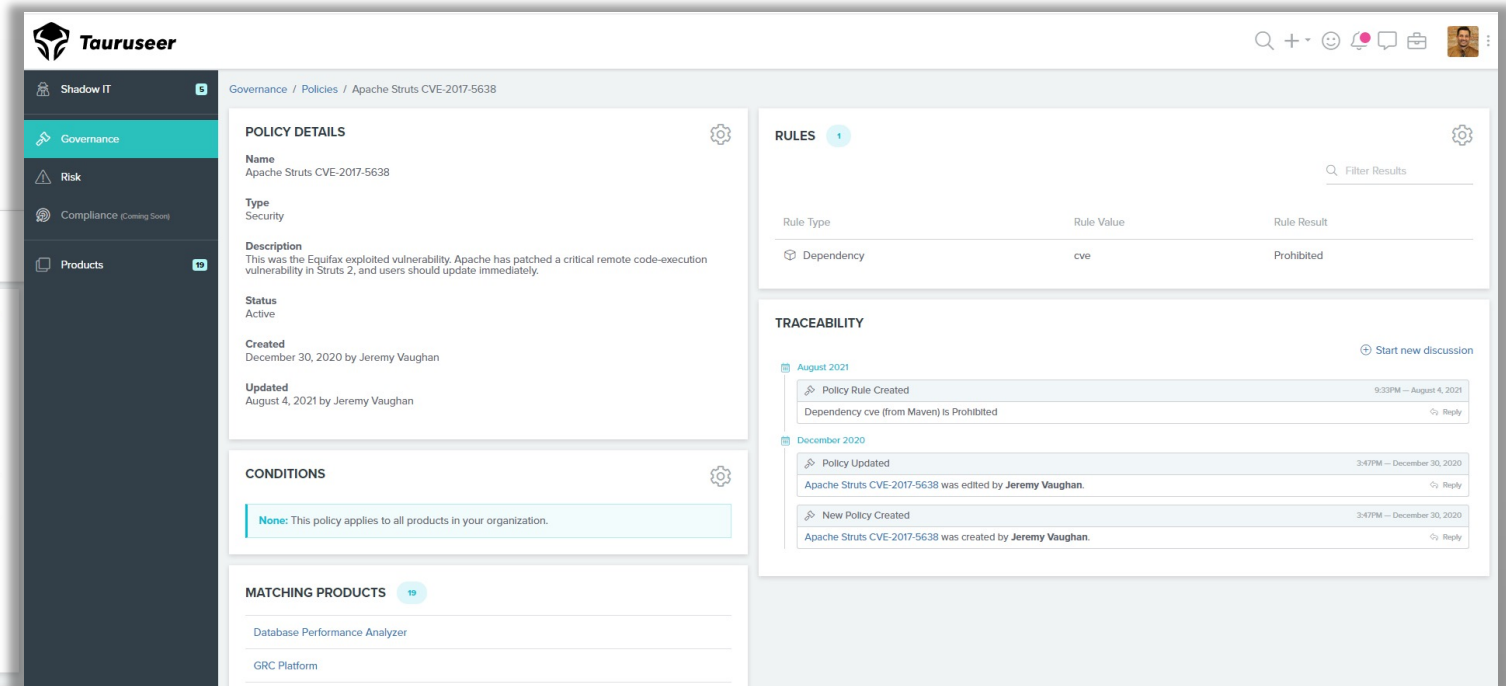
**** DISPUTED **** A command injection vulnerability in Lodash 4.17.21 allows attackers to achieve arbitrary code execution via the template function. This is a different parameter, method, and version than CVE-2021-23337. NOTE: the vendor's position is that it's the developer's responsibility to ensure that a template does not evaluate code that originates from untrusted input.

Vulnerability 1 of 4 [View All](#)

CODE WEAKNESSES

7 Total Code Weaknesses ↔ 0 FYTD

Critical	0
High	0
Medium	7
Low	0



Tauruseer Governance / Policies / Apache Struts CVE-2017-5638

POLICY DETAILS

Name: Apache Struts CVE-2017-5638

Type: Security

Description: This was the Equifax exploited vulnerability. Apache has patched a critical remote code-execution vulnerability in Struts 2, and users should update immediately.

Status: Active

Created: December 30, 2020 by Jeremy Vaughan

Updated: August 4, 2021 by Jeremy Vaughan

CONDITIONS

None: This policy applies to all products in your organization.

MATCHING PRODUCTS 19

- Database Performance Analyzer
- GRC Platform

RULES 1

Rule Type	Rule Value	Rule Result
Dependency	cve	Prohibited

TRACEABILITY Start new discussion

- August 2021**
 - Policy Rule Created 9:33PM — August 4, 2021
 - Dependency cve (from Maven) is Prohibited [Reply](#)
- December 2020**
 - Policy Updated 3:47PM — December 30, 2020
 - Apache Struts CVE-2017-5638 was edited by **Jeremy Vaughan**. [Reply](#)
 - New Policy Created 3:47PM — December 30, 2020
 - Apache Struts CVE-2017-5638 was created by **Jeremy Vaughan**. [Reply](#)

Secure Software & Data Management



Standards & Regulatory

- Formalized and measurable change management process
- Software code repository integrity
- Software deployment integrity
- Retention and disposal of sensitive information retained for valid reasons

Platform Deliverables

- Process Adherence Monitoring & Alerting
- Git & CI/CD Security Integrity
- Product/App Lifecycle Alerting
- Architectural Drift or Code Rot
- Continuous Assurance

- Cognition Alerting
 - Statistical Analysis / Trend Differentiations*
 - Anomalies

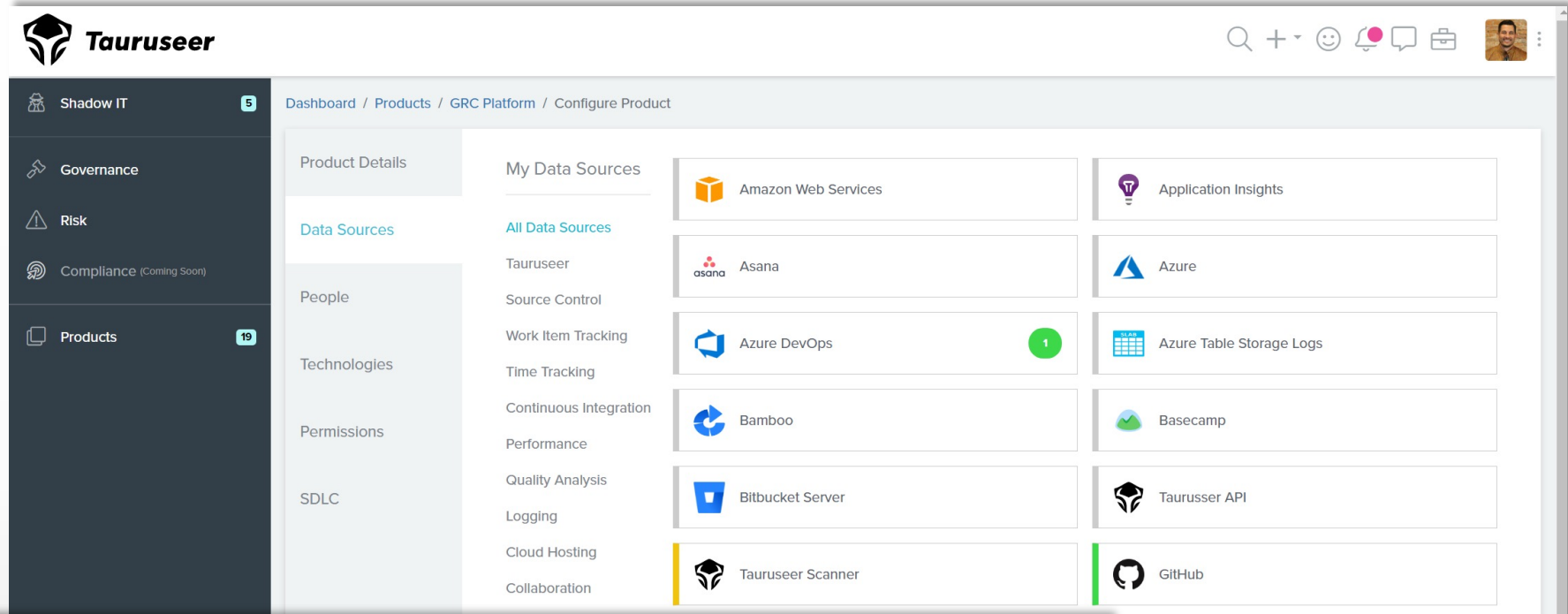


OO



RO

Risk management is a team sport, "everybody in the pool!"



Dashboard / Products / GRC Platform / Configure Product

Product Details

Data Sources

People

Technologies

Permissions

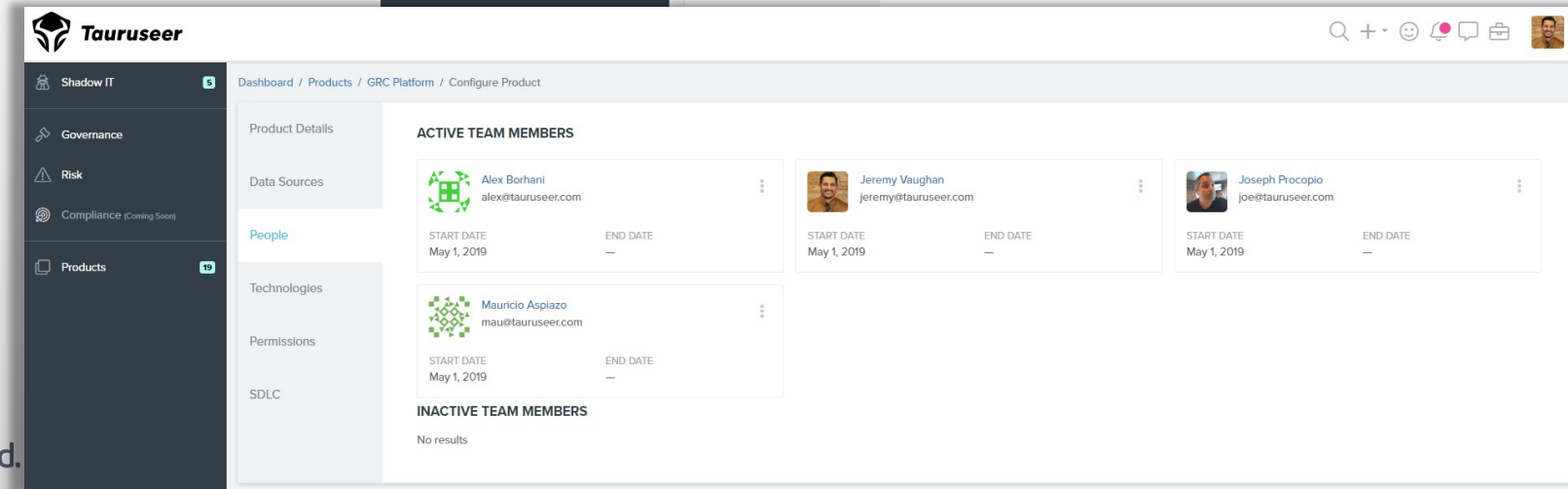
SDLC

My Data Sources

All Data Sources

- Tauruseer
- Source Control
- Work Item Tracking
- Time Tracking
- Continuous Integration
- Performance
- Quality Analysis
- Logging
- Cloud Hosting
- Collaboration

- Amazon Web Services
- Asana
- Azure DevOps
- Bamboo
- Bitbucket Server
- Tauruseer Scanner
- Application Insights
- Azure
- Azure Table Storage Logs
- Basecamp
- Taurusser API
- GitHub
- Harvest
- JIRA
- SonarQube
- Team Foundation Server



Dashboard / Products / GRC Platform / Configure Product

Product Details

Data Sources

People

Technologies

Permissions

SDLC

ACTIVE TEAM MEMBERS

Profile	START DATE	END DATE
Alex Borhani alex@tauruseer.com	May 1, 2019	—
Jeremy Vaughan jeremy@tauruseer.com	May 1, 2019	—
Joseph Procopio joe@tauruseer.com	May 1, 2019	—

INACTIVE TEAM MEMBERS

No results

Security Communications – Optimize business value



Standards & Regulatory

- Implementation Guide – living document
- Communication Channels and information dispersion process for updates, threats, risk mitigation.
- Communication to stakeholders
- Earning stakeholder trust requires an omnichannel communication process and methodology

Platform Deliverables

- Telemetry & KPIs for Specific Stakeholders
- “App Groupings” or Portfolio Management
 - Internal IT / Product Teams
- SLA (third-party/vendor risk management)
 - Customer Groupings & Measurement
- External Audit collaboration
 - Read-only access
- Cognition Alerting
 - Statistical Analysis / Trend Differentiations*
 - Anomalies



RO



SO



SH

Compliance and Security becomes a valuable by-product

1. Streamlines and automates manual efforts involved to report on compliance controls and retain perpetual documentation and process workflow information for compliance validation evidentiary items (Orchestration)
2. Set up guardrails to make sure development stays within the lines and promotes organizational operationalizing of risk management policy
3. Ensures organizations are compliant and operating and within the bounds of defined risk appetite tolerances by Continuously monitor actions/behaviors/performance (KPI/KRI)
4. Create transparent, continuously updated information to facilitate effective governance



INTEGRATED RISK MANAGEMENT

Minimizing Deviation from Expected Outcomes is Highly Valued by Key Stakeholders

INDUSTRY DRIVEN

MARKET DRIVEN

RISK OPTIMIZED ORGANIZATION



RISK ENABLED GROWTH

EXECUTIVE SERIES

Stay Tuned for our 2022 Series

to create a 'risk-optimized' organization to achieve strategic goals and capitalize on growth opportunities

online



Tauruseer

RISKNEUTRAL



THANK YOU

Enjoy the rest of your day.

Stay tuned for our 2022 series!