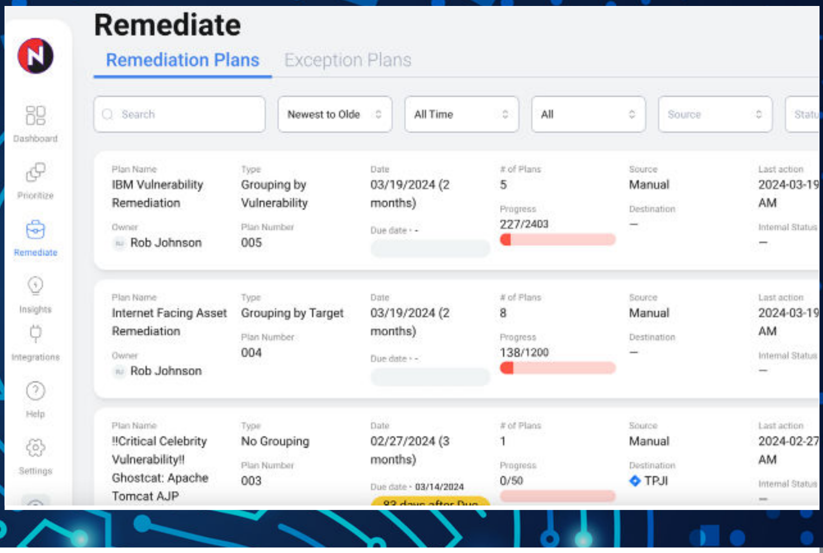
Solution Brief

NOPSEC

Align More. Expose Less

Best practices to align DevSecOps for strategic exposure management



Remediate

Remediation Plans | Exception Plans

Search | Newest to Olde | All Time | All | Source | Statu

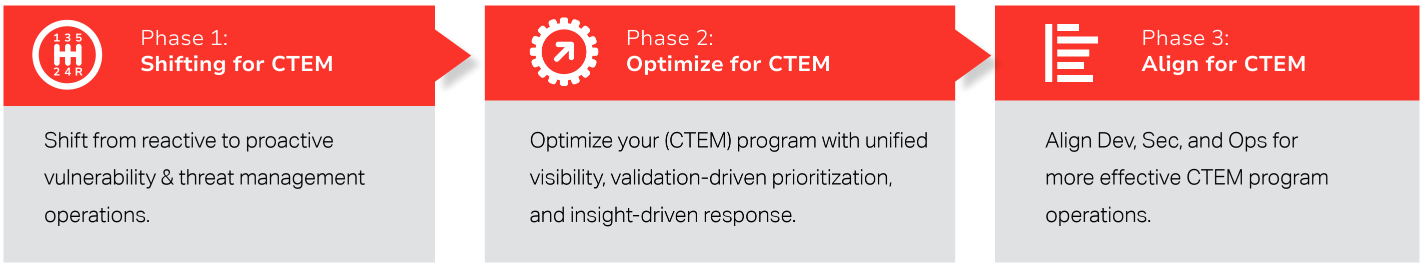
Plan Name	Type	Date	# of Plans	Source	Last action
IBM Vulnerability Remediation	Grouping by Vulnerability	03/19/2024 (2 months)	5	Manual	2024-03-19 AM
Owner: Rob Johnson	Plan Number: 005	Due date - -	Progress: 227/2403	Destination: —	Internal Status: —
Internet Facing Asset Remediation	Grouping by Target	03/19/2024 (2 months)	8	Manual	2024-03-19 AM
Owner: Rob Johnson	Plan Number: 004	Due date - -	Progress: 138/1200	Destination: —	Internal Status: —
!!Critical Celebrity Vulnerability!! Ghostcat: Apache Tomcat AJP	No Grouping	02/27/2024 (3 months)	1	Manual	2024-02-27 AM
	Plan Number: 003	Due date - 03/14/2024 93 days after Due	Progress: 0/50	Destination: TPJI	Internal Status: —

75%
Reduction in MTTR on highest risk vulnerabilities

As a CISO, you're spearheading a shift from the tactical "patch it, kill it, block it" mindset to a strategic continuous threat exposure management (CTEM) program, as defined by Gartner. However, transitioning from a theoretical CTEM program to operationalizing it in the real world is complex.

NopSec's Operationalizing for CTEM process is a phased approach that makes this transition possible, as shown in Figure 1. Aligning your security, IT, and app development teams is exceptionally challenging yet potentially the most rewarding. This alignment is critical when addressing real-time threats, such as a DAST scanner flagging a vulnerability in a vital repo, just as your risk team identifies a high-speed active exploit. Can your teams synchronize efforts to mitigate this risk effectively?

Aligning your DevSecOps teams around exposure management is crucial. At NopSec, we believe in a simple yet powerful mantra—Align More. Expose Less.— which encapsulates our approach to streamlined security efforts and effective team synchronization.



Phase 1:
Shifting for CTEM
Shift from reactive to proactive vulnerability & threat management operations.

Phase 2:
Optimize for CTEM
Optimize your (CTEM) program with unified visibility, validation-driven prioritization, and insight-driven response.

Phase 3:
Align for CTEM
Align Dev, Sec, and Ops for more effective CTEM program operations.

Figure 1 – Operationalizing for CTEM

Best practices to Align More, Expose Less

Derived from NopSec's years of offensive security experience, there are two essential and complementary best practices for aligning DevSecOps - establish universal DevSecOps prioritization and implement insight-driven workflows. These practices help your teams enhance communication, improve prioritization, and leverage the concepts of likelihood, impact, and velocity for strategic exposure management. [2]

> **"Effective communication of the risk to the organization to enable cross-team remediation actions is the main challenge in moving from threat to exposure management."** *Gartner*

1) Establish universal DevSecOps prioritization

Your teams require a unified prioritization strategy. This universal prioritization acts as a shared language, helping to determine if you're watching a tsunami from a safe distance or standing right in its path. After all, the higher the velocity, the shorter the fuse. Such context is essential for timely assessment and response.

Key tactics include:

- **Taming Data Overload:** Ensure team members have clear and actionable insights into vulnerabilities and exposures by using AI to eliminate data drowning. Machine learning algorithms can prioritize critical assets across your system by aggregating and normalizing data from multiple sources.
- **Injecting Deep Context:** Move beyond CVSS scores by linking threat actor tactics to vulnerabilities in your systems. This approach necessitates considering compensating controls and asset criticality to accurately judge a threat's impact and velocity.

[2] Gartner quote in text box: "Predicts 2023: Enterprises Must Expand From Threat to Exposure Management," Gartner, page 5, December 2022.

2) Implement insight-driven workflows

Equip your teams with insight-driven tools and workflows to make informed decisions about mitigating, blocking, or accepting risks. This shift from a tactical to a process-focused strategy—assessing, prioritizing, coordinating, and reporting—is vital for strategic exposure management.

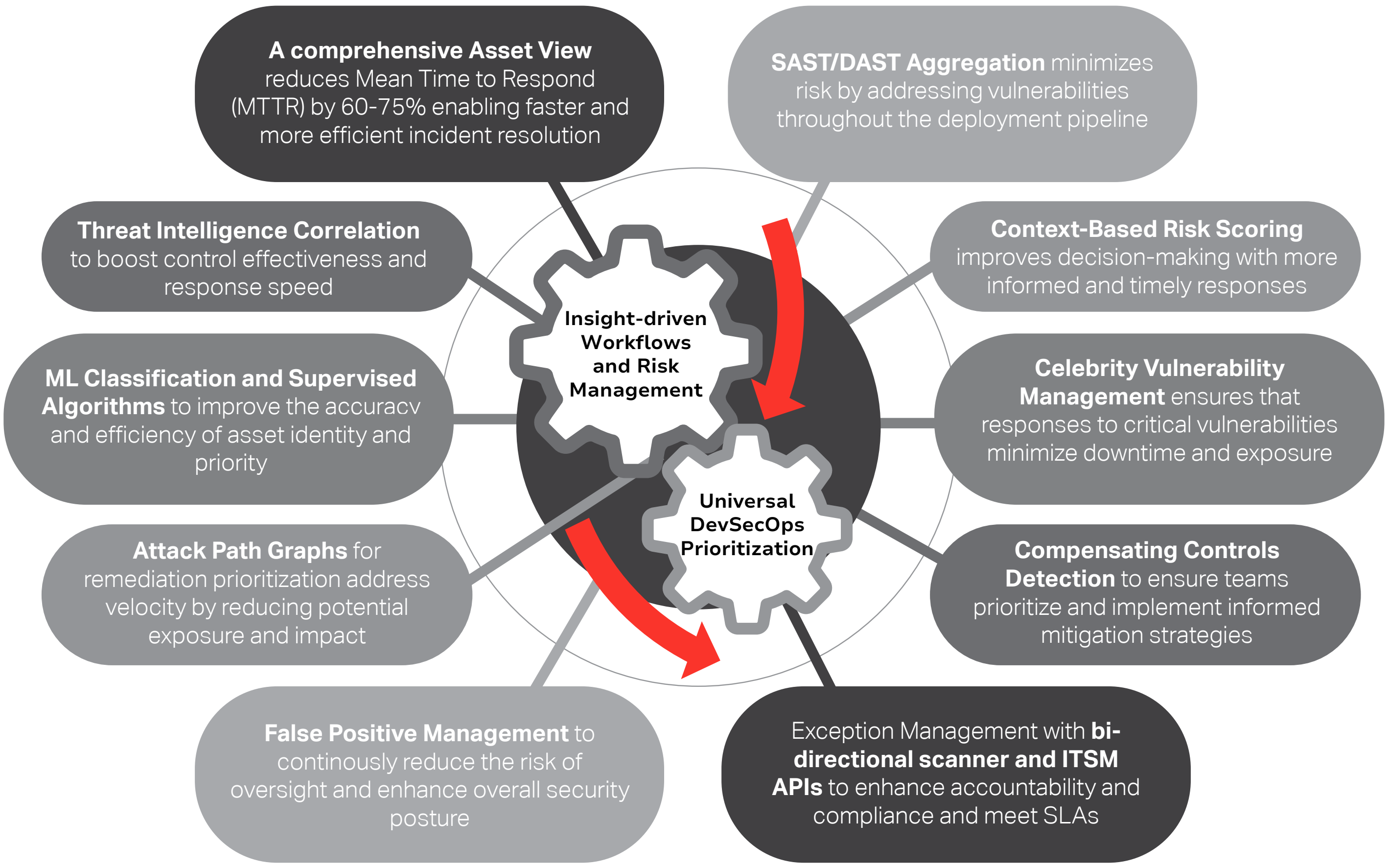
Key tactics include:

- **Analyze critical attack paths:** Illuminate critical dependencies across teams and platforms. Refine risk scores by considering existing controls and asset importance.
- **Integrate exposure management with ITSM and DevOps (CI/CD) processes:** Facilitate pre-deployment exposure identification and control implementation, ensuring controls are operational. Include plans for remediation exemptions to match risk appetite.
- **Adopt strategic metrics and dynamic assessments:** Move beyond tactical counts and CVSS scores. Instead, strategically monitor exposure and SLA compliance during risk analysis using a universal prioritization database (as shown in Table 1).

METRICS & REPORTING	TACTICAL		STRATEGIC
Security	• Vulnerabilities, Patches, IOCs, Threats	→	• Exposures, Exception Management, SLAs, TTPs
Development	• Vulnerabilities, Patches	→	• Exposures, Acceptance of Unpatched Vulnerabilities in Production
Operations	• Vulnerabilities, Patches, Time to Patch,	→	• Exposures, Compliance with SLAs,

How NopSec helps

Activate these best practices with NopSec at your side, transforming your SecDevOps teams from tactical vulnerability managers to strategic exposure experts. Our cutting-edge technology helps turbocharge your efforts across both practices, ensuring you align more and expose less!



Insight-driven Workflows and Risk Management

Universal DevSecOps Prioritization

A comprehensive Asset View reduces Mean Time to Respond (MTTR) by 60-75% enabling faster and more efficient incident resolution

SAST/DAST Aggregation minimizes risk by addressing vulnerabilities throughout the deployment pipeline

Threat Intelligence Correlation to boost control effectiveness and response speed

Context-Based Risk Scoring improves decision-making with more informed and timely responses

ML Classification and Supervised Algorithms to improve the accuracv and efficiency of asset identity and priority

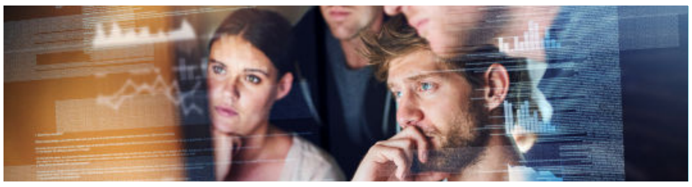
Celebrity Vulnerability Management ensures that responses to critical vulnerabilities minimize downtime and exposure

Attack Path Graphs for remediation prioritization address velocity by reducing potential exposure and impact

Compensating Controls Detection to ensure teams prioritize and implement informed mitigation strategies

False Positive Management to continously reduce the risk of oversight and enhance overall security posture

Exception Management with **bi-directional scanner and ITSM APIs** to enhance accountability and compliance and meet SLAs



Align your DevSecOps teams today

Transitioning from a tactical "patch it, kill it, block it" mindset to a strategic focus on assessing threats by their likelihood, impact, and velocity is achievable. Now, it's time for action, and that's where NopSec excels. Schedule a demo with our exposure management experts today to see this in action.

See the results of Operationalizing for CTEM

The results of NopSec's effectiveness speak for themselves. Don't take our word for it. Read about the first-hand experience this major media production company had after implementing NopSec and shifting to exposure management.