Palo Alto Prisma Cloud and Tamnoon

Adding Deep Context to CNAPP Alerts For Easy Prioritization, Remediation, and Proactive Protection.

The Challenge

Cloud-Native Application Protection Platforms (CNAPPs) excel at detecting misconfigurations that can lead to potential vulnerabilities and surface risks in cloud environments that would normally go undetected. However, by their very nature, solutions with such comprehensive visibility generate a high volume of alerts.

While this ensures that no risk goes unnoticed, it can also overwhelm cloud security teams who must sift through these alerts to determine which issues require immediate attention. For example, similar misconfigurations across multiple resources may be flagged with identical criticality ratings, even though their real-world impact can vary based on the asset's role, exposure, or data sensitivity. This results in security teams dedicating significant time to addressing less impactful issues while critical vulnerabilities remain unresolved.

To bridge this gap, organizations need solutions that adapt and are tailored to their specific architecture and business priorities, ensuring remediation efforts effectively address their critical infrastructure.

Our Integrated Solution

Tamnoon integrates seamlessly with **Palo Alto Prisma Cloud** to combine the visibility of Prisma Cloud with the context, expert remediation advice, and proactive protection from Tamnoon against cloud vulnerabilities.

- **Prisma Cloud's** agentless scanning provides teams immediate visibility into all workloads and cloud services, identifying vulnerabilities and misconfigurations across cloud environments.
- **Tamnoon** enriches Prisma Cloud alerts by incorporating contextual information such as the type of resource, its environment, its exposure, encryption status, the criticality of the vulnerability, and the resource owner, thus ensuring that critical misconfigurations and risks are addressed first. In addition, Tamnoon offers simple, easy-to-follow remediation advice and playbooks, as well as blocking major, recurring misconfigurations from happening again.

This hybrid approach bridges the gap between detection and action, allowing teams to prioritize and remediate cloud security risks efficiently and effectively. Tamnoon's collaboration with Prisma Cloud is tailored to each customer's unique environment, aligning remediation efforts with their critical workflows and operational needs.

Business Impact and Key Benefits

- Automatically tag critical infrastructure and assets based on their sensitivity, exposure, and business impact.
- Prioritize Prisma Cloud alerts using Tamnoon's contextual insights directly within the remediation platform by combining the power of AI with Security expertise.

Remediate Issues Effectively

- Manage the communication between security and developers, providing both sides with the necessary technical and business context to resolve issues swiftly and effectively.
- Avoid wasting time on lower-priority issues and focus on the most important risks.
- Leverage Tamnoon's developer-friendly playbooks to reduce MTTR by up to 50%, ensuring safer and faster remediation aligned with business priorities.

Actively Protect Your Organization

- Continuously monitor and reassess asset prioritization as the cloud environment evolves.
- Defend high-value resources from emerging threats using Tamnoon's preemptive prevention mechanisms.
- Proactively identify and remediate misconfigurations or vulnerabilities in production environments that could impact regulatory requirements, ensuring a strong security posture that aligns with compliance best practices.

Use Cases in Action

The Tamnoon x Sentra collaboration at work:

Prioritizing Exposed Sensitive Blob Storage

Scenario:

Prisma Cloud flags multiple misconfigured S3 buckets.

Solution:

Prisma Cloud identifies misconfigured S3 buckets, generating alerts to highlight potential risks. While Prisma excels at detecting and flagging these issues, it doesn't provide the detailed context or prioritization needed to act efficiently. Tamnoon enhances these insights by analyzing the flagged resources in depth, considering factors such as exposure level, encryption status, critical vulnerabilities, and the environment type. Resources identified as high-risk—such as those publicly exposed, unencrypted, or in production—are automatically prioritized. Tamnoon then boosts the criticality of the most at-risk buckets, assigns concrete tasks to the responsible staff, and provides tailored playbooks to the development team, ensuring swift and effective remediation.

Focusing on Over-Permissive IAM Roles

Scenario:

Prisma Cloud detects ten over-permissive IAM roles.

Solution:

Tamnoon analyzes the flagged IAM roles in the context of their associated cloud resources and environments. Tamnoon's Security Experts & AI Enrich the alerts with context such as exposure, resource criticality, and usage patterns. This allows security teams to prioritize roles that pose the greatest risk to the organization further. Finally, Tamnoon provides actionable tasks and remediation playbooks to ensure permissions are reduced to the minimum required for functionality, all without disrupting cloud operations.

Addressing Publicly Exposed Databases

Scenario:

Prisma Cloud detects three publicly exposed RDS instances with potential misconfigurations and vulnerabilities.

Solution:

Tamnoon conducts a comprehensive investigation to assess exposure risks. Using VPC flow logs, it identifies malicious traffic from external IPs, including a known threat from China. Tamnoon pinpoints internal assets linked to the exposed database, such as an API server and a bastion host. Tamnoon prioritizes remediation based on key factors like public exposure, encryption status, and misconfigured network access controls (e.g., Security Groups and NACLs).

By integrating Tamnoon's automated investigation and tailored remediation workflows, security teams can resolve vulnerabilities effectively and prevent future misconfigurations, ensuring that RDS instances remain secure and compliant.