CrowdStrike Falcon® x Tamnoon

Enhancing CNAPP Alerts with Rich Context for Smarter Prioritization, Faster Remediation, and Proactive Defense.

The Challenge

While CrowdStrike Falcon® provides unparalleled detection of threats and vulnerabilities in cloud environments, many organizations struggle with bridging the gap between identifying issues and effectively investigating and remediating them. The nature and beauty of this solution is the amount of visibility it gives into complex cloud environments. However, the volume of alerts generated can overwhelm even the most experienced security teams.

While this leaves no stone unturned in identifying risks it can often make it difficult to determine which risks and vulnerabilities should be prioritized and are the most impactful. This can lead to inefficient resource allocation, with teams spending valuable time on less impactful issues while critical vulnerabilities remain unaddressed. Security and developer teams need a solution that adapts to their unique cloud environments, considering their architecture, business priorities, and critical assets to ensure effective remediation.

Our Integrated Solution

The partnership between **CrowdStrike Falcon® and Tamnoon** combines robust detection capabilities with intelligent prioritization and expert-guided remediation support, delivering a seamless, end-to-end alert management solution, from detection all the way to resolution, that empowers security teams to resolve issues faster and more effectively.

- **CrowdStrike Falcon®** is an industry-leading CNAPP solution that provides detection and visibility into threats, vulnerabilities, and misconfigurations across multi-cloud environments. CrowdStrike Falcon® identifies risks at scale, enabling teams to uncover attack paths and secure their cloud workloads.
- **Tamnoon** enriches CrowdStrike alerts with context like the asset's role, its exposure level, the sensitivity of its data, and historical patterns by combining insights from its powerful AI solution and its Cloud Security Experts. This enables security teams to focus on the most critical risks first. Tamnoon also delivers tailored remediation advice and step-by-step playbooks to guide teams in resolving issues efficiently, ensuring minimal disruption to production environments.

This collaboration bridges the gap between detection and resolution, empowering organizations to prioritize, remediate, and prevent cloud vulnerabilities at scale. Tamnoon tailors its enrichment and remediation strategies to each organization's specific architecture, critical infrastructure, and business needs, ensuring solutions align with operational priorities.

Business Impact and Key Benefits

Enrich CNAPP Alerts With Expert and AI insights

- Automatically tag critical infrastructure and assets based on their exposure, criticality, and business impact.
- Tamnoon enriches CrowdStrike alerts by incorporating key factors such as the criticality of impacted assets, exposure to public networks, the type of vulnerability detected, ownership details, historical incident trends, and operational environment. This deep context ensures security teams have the full picture, enabling smarter decision-making and faster remediation.
- Tamnoon tailors its enrichment and remediation strategies to each organization's specific architecture and critical business needs.

Remediate Issues Effectively

- Facilitate collaboration between security teams and developers by delivering tailored technical and business contexts the teams need to resolve issues efficiently
- Save valuable time by deprioritizing less critical alerts and focusing on the most pressing risks, making sure they never return in the future.
- Use Tamnoon's developer-focused playbooks and guidance by our Cloud Security Experts enhanced by AI to streamline remediation and accelerate remediation time.
- Through a detailed impact-analysis, Tamnoon ensures that remediation is production-safe, reducing average MTTR by up to 50%.

Actively Protect Your Organization

- Continuously monitor evolving cloud environments and stay ahead of threats by reassessing and prioritizing assets as your cloud environment grows and evolves.
- Identify your Critical Infrastructure and safeguard it from emerging risks by leveraging Tamnoon's proactive threat prevention and mitigation strategies.
- Ensure secure and stable operations by proactively identifying and resolving misconfigurations or vulnerabilities in production environments to maintain a strong security posture and prevent operational disruptions.

Use Cases in Action

Enforcing Multi-Factor Authentication (MFA)

Scenario:

CrowdStrike Falcon® flags accounts across multiple AWS environments without MFA enabled for root or IAM users. These accounts are at heightened risk of unauthorized access, potentially exposing sensitive resources.

Solution:

Tamnoon's Cloud Security Experts in tandem with AI, conduct a detailed investigation, analyzing impacted accounts and their associated environments. Based on their impact analysis the following steps are suggested:

- **Scope Reduction:** A Service Control Policy (SCP) is applied at the organizational level, restricting all console activities unless MFA is enabled.
- **Policy Injection**: For IAM users, Tamnoon shows how to automatically create and apply a tailored IAM policy that enables users to configure MFA for themselves.
- **Root Account Enforcement**: For root accounts, Tamnoon ensures either hardware or virtual MFA is activated by guiding administrators through a detailed, step-by-step process.

In addition to remediation, Tamnoon provides actionable playbooks for both hardware and virtual MFA enforcement, ensuring changes are made securely and with minimal operational impact. The result? Immediate risk reduction through enforced MFA requirements, safeguarding critical accounts, and reducing exposure to unauthorized access. Find the detailed playbook here.

Encrypting Unsecured EBS Volumes

Scenario:

CrowdStrike Falcon® identifies multiple EBS volumes across AWS environments that are not encrypted, leaving sensitive data at risk of unauthorized access. These volumes range from unattached instances to those in Auto Scaling Groups, requiring a phased approach for remediation.

Solution:

Tamnoon's Cloud Security Experts, supported by AI, conduct an impact analysis to categorize and prioritize the volumes based on their usage and criticality:

- **Phase** 1: Low Impact – Unattached Volumes
  Volumes not attached to any instances are encrypted with no disruption to production systems.
- **Phase** 2: Medium Impact – Non-Auto Scaling Instances
  Volumes attached to instances outside of Auto Scaling Groups are encrypted during scheduled maintenance windows to minimize downtime.
- **Phase** 3: High Impact – Auto Scaling Group Instances
  Volumes attached to instances within Auto Scaling Groups are encrypted with Tamnoon's automated process, including steps to suspend health checks, remediate volumes, and restore Auto Scaling operations without affecting the instance's functionality.

With Tamnoon's detailed remediation playbook and automated tools, security teams resolve encryption gaps efficiently, safeguarding sensitive data while maintaining operational integrity. The result? A secure, compliant, and robust cloud infrastructure. Find the detailed playbook here.

Better Together

Combining CrowdStrike's Falcon® advanced detection capabilities with Tamnoon's expertise in prioritization and remediation delivers a comprehensive solution for cloud security. Organizations gain a streamlined approach to mitigating critical risks, ensuring that every detected vulnerability is resolved with precision and confidence.