Demisto And Securonix
For Automated Incident Management

Benefits
• Automate incident response and playbook-driven triage of security alerts.
• Enrich investigation data with rich user context, activity timelines, and violations.
• Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility
• Products: SNYPR Security Analytics
• Product Versions: SNYPR 6.1+
• Platform: Hadoop

Security teams face unique challenges in today’s data-heavy landscape with sophisticated attackers and vast threat surfaces. Separating insights from noise, handling insider threats, battling alert fatigue, and standardizing IR procedures all weigh heavily on the security analyst's mind.

To help meet these challenges, users can now enhance Demisto playbooks and investigations with Securonix’s security analytics and threat intelligence capabilities.

Securonix and Demisto integration features:
• Ingest violation data from Securonix SNYPR console into Demisto Enterprise.
• Trigger specific playbooks for gathering more information about Securonix violation fields or for responding to Securonix violations.
**USE CASE #1**

**EXTRACTING CONTEXT FROM INVESTIGATION DATA**

**Challenge:** During investigations, analysts need to check indicators, find out whether they are malicious, and weave a contextual thread through the endless holes of data at their disposal. Faced with many indicators sans context, this can be a repetitive and time-consuming process.

**Solution:** After ingesting violations from Securonix, Demisto uses hypersearch to give analysts critical context about the indicators associated with an incident. Analysts can view indicator malice, repeating patterns, and cross-correlations at a glance in both the work plan and war room windows.

**Benefit:** Contextual viewing of data allows for quicker identification of remediation procedures and running the respective playbooks/actions to curtail the incident.

---

**USE CASE #2**

**STREAMLINED INCIDENT INGESTION ACROSS CONSOLES**

**Challenge:** If a security analyst uses different platforms for incident management and security orchestration and automation respectively, it can be tough to track the lifecycle of an incident due to flitting between screens, fragmented information, and lack of single-window documentation.

**Solution:** If SOCs use Securonix SNYPR for incident management and Demisto Enterprise for security orchestration and automation respectively, they can trigger actions for specific violation types in Securonix to create an incident in Demisto.

**Benefit:** Demisto playbooks and investigation toolkits can gather additional information needed for triage and resolution of Securonix violations. Analysts get a comprehensive view of the incident’s lifecycle, can access documentation from a single source, and forego the need to switch between screens.

---

**About Securonix**

Securonix, the leader in Security Analytics, uses the power of Hadoop and machine learning to radically transform enterprise security with actionable intelligence. Our purpose-built UEBA and Next-Gen SIEM platforms consume, enrich and analyze massive volumes of data in real-time to detect and prioritize the highest risk threats to organizations. Using out of the box content, Securonix detects insider threat, cyber threat, cloud and fraud attacks automatically and accurately. Visit us at www.securonix.com

**About Demisto**

Demisto Enterprise is the first and only comprehensive Security Operations Platform to combine security orchestration, incident management, machine learning from analyst activities, and interactive investigation. Demisto’s orchestration engine automates security product tasks and weaves in the human analyst tasks and workflows. Demisto enables security teams to reduce mean time to resolution (MTTR), create consistent incident management process, and increase analyst productivity. Demisto is backed by Accel and other prominent investors and has offices in Silicon Valley and Tel Aviv. For more information, visit www.demisto.com or email info@demisto.com.