SECURONIX Security Analytics. Delivered. | DEMISTO

SOLUTION BRIEF

# Securonix and Demisto Deliver Automated Incident Management

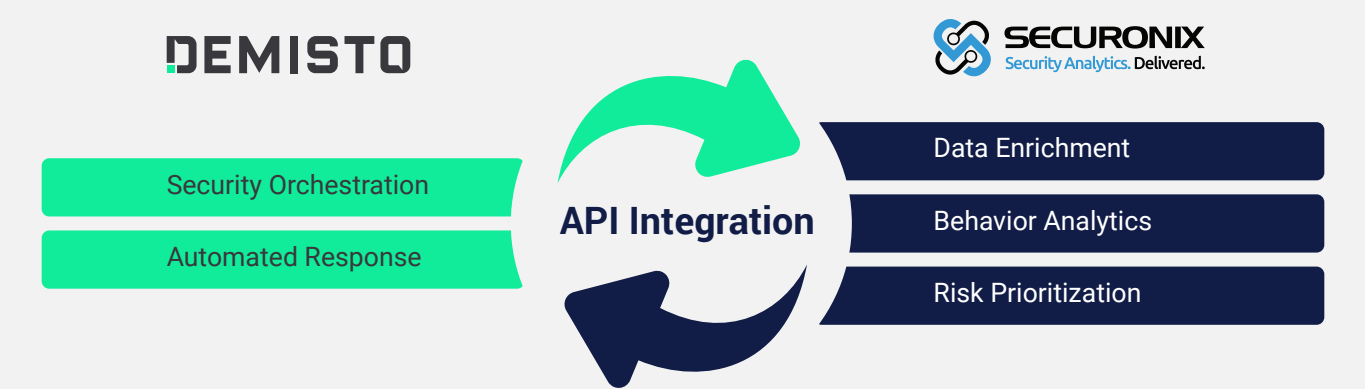
Your security team faces unique challenges in today's data-heavy landscape. Separating insights from noise, handling insider threats, battling alert fatigue, and standardizing incident response procedures all weigh heavily on your security analyst's mind.

Built on big data, Securonix Security Analytics Platform combines log management, security incident and event management (SIEM), and user and entity behavior analytics (UEBA) into a complete, end-to-end platform that can be deployed in its entirety or in flexible, modular components. It collects massive volumes of data in real time, uses patented machine learning algorithms to detect advanced threats, and provides actionable security intelligence for quick response. Demisto enables you to automate security product tasks and weaves in the human analyst's tasks and workflows. Powered by its machine learning technology, Demisto acquires knowledge from the real-life analyst interactions and past investigations to help Security Operations Center (SOC) teams with analyst assignment suggestions, playbook enhancements, and investigation next steps.

When you integrate your Securonix deployment with Demisto Enterprise for security orchestration and automation, you can trigger actions for specific violation types in Securonix to create an incident in Demisto. 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.

## Integration Benefits

- Analysts get a comprehensive view of the incident's lifecycle and can enrich investigation data with rich user context, activity timelines, and related events.
- Shorten decision-making cycle by automating incident response and playbook-driven triage of security alerts with analyst review.
- Access documentation from a single source, and forego the need to switch between screens.



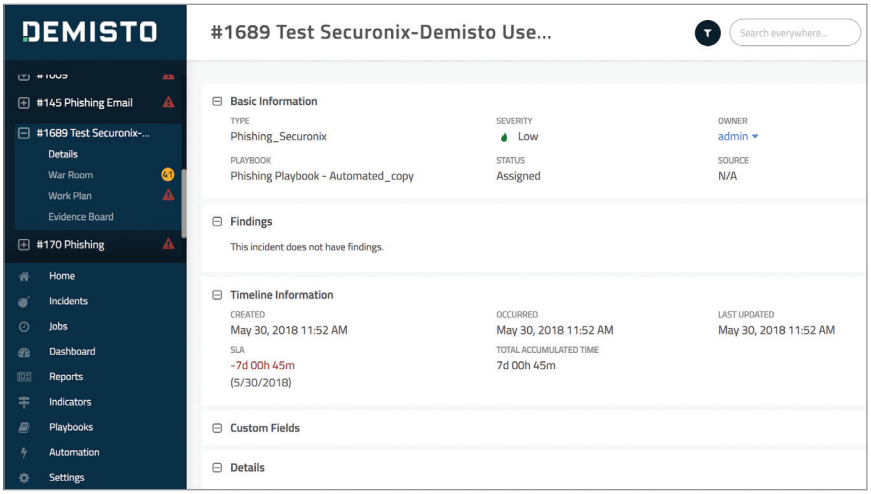

Threats detected by Securonix automatically create events in Demisto's automated response system.

## Extracting Context From Investigation Data

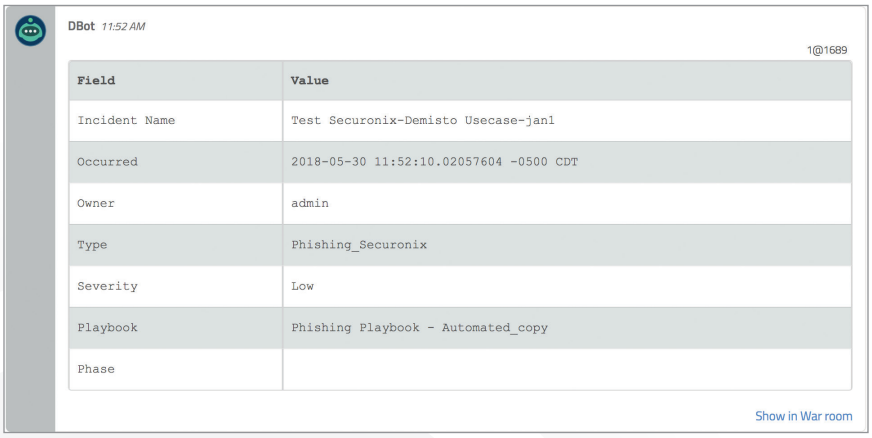
Unlike legacy SIEM solutions that rely on signatures, Securonix Security Analytics Platform applies sophisticated machine learning algorithms and threat chain modeling to event data in real-time to accurately detect advanced and insider threats. Every alert is automatically ranked so analysts can prioritize their response.

After ingesting alerts 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.

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




Securonix analyzes data sources, identifies phishing scam behavior, and sends the warning to Demisto.




Demisto's security orchestration and response system contains response-based playbooks. These playbooks can be automated or agent triggered. Depending on the type of security event, specific playbooks can be used.

## How it Works

- Ingest event data from Securonix into Demisto Enterprise.
- Trigger specific playbooks for gathering more information about suspicious events or for responding to malicious events.

## About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.

## About Demisto

Demisto is the only comprehensive Security Operations Platform to combine security orchestration, incident management, and interactive investigation into a seamless experience. The platform automates security product tasks and weaves in the human analyst tasks and workflows. For more information visit www.demisto.com.

SECURONIX
Security Analytics. Delivered.

**LEARN MORE**
www.securonix.com

**LET'S TALK**
+1 (310) 641-1000

14665 Midway Rd. Suite #100, Addison, TX 75001 | ©2018 Securonix