securonix

DATASHEET

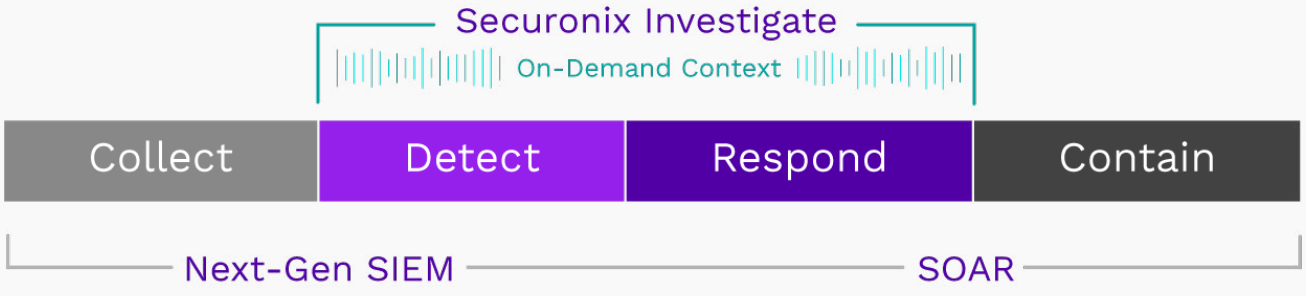
Securonix Investigate

Content Enrichment When and Where You Need It

Improve Investigation With On-Demand Context and Collaboration

When investigating an incident, it is mission critical to have the right contextual information. However, security analysts don't always know what context they need before they need it. Security teams need on-demand context during investigation to better understand threats, while communicating key findings across the team without leaving the investigation.

No longer comb through multiple data sources or develop and run playbooks when additional or new context is needed. Securonix Investigate automatically extracts context from internal and external data sources for investigations in flight. You can annotate findings within the investigation workflow to share knowledge without pivoting to external tools like ticketing, email, or messaging platforms. With Securonix Investigate you shorten investigation time by automatically enriching content and streamlining information sharing.



Expedite Investigations and Capture Investigator Knowledge

Gather context from your security operations, threat intelligence, penetration testing, endpoint security, internal data repositories and many more systems that store relevant data. Note key findings directly within the context window. Share knowledge and collaborate across teams by annotating context strings with relevant insights.

Accelerate Threat Mitigation

Dynamically enrich incidents under investigation with context and intelligence. Automatically gather new and updated details and align them to alerts.

Better Understand Threats

Bring key details to light by integrating Securonix Investigate with internal and external data sources, presented in the local language regardless of where they originated.

Communicate Knowledge Across Teams

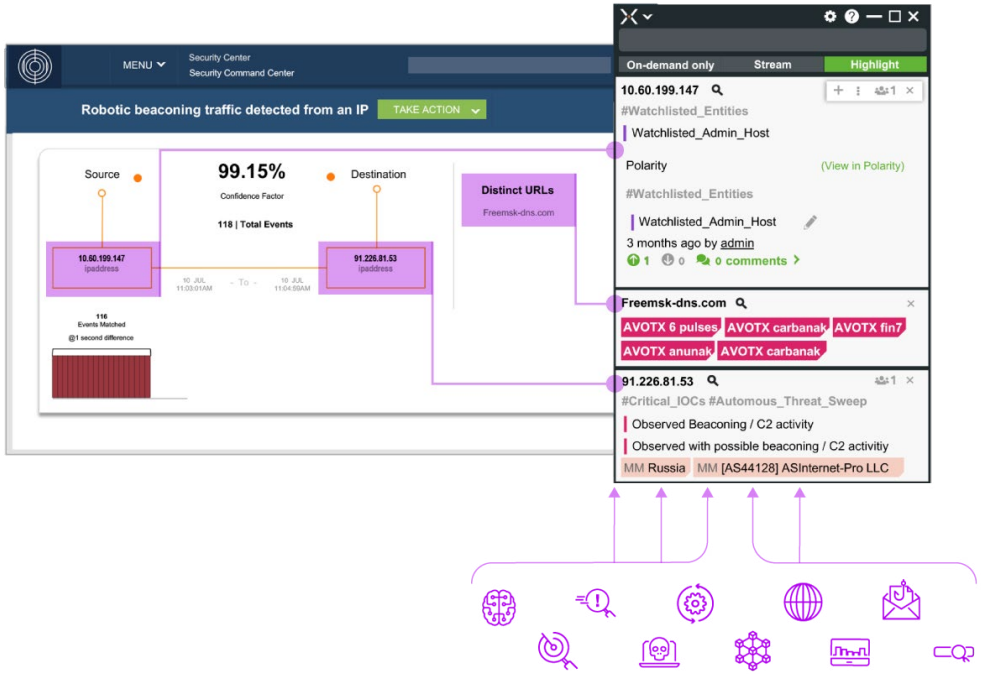
Annotate, document, and share observations across trusted groups within investigation workflows.

Add Details to Investigations in Flight

Securonix Next-Gen SIEM provides vast context as data is ingested, but context is dynamic. With Securonix Investigate you can automatically gather new or updated contextual data when and where you need it. This timely context brings threat details to light to speed incident mitigation.

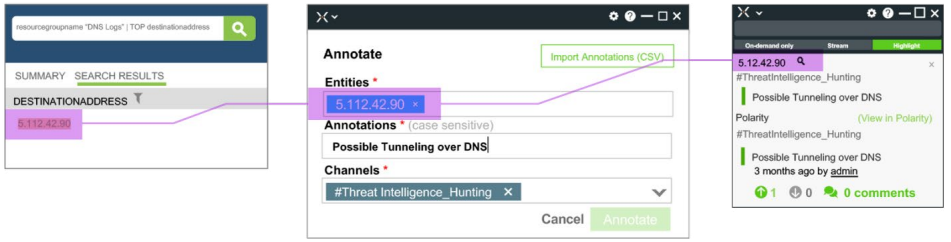
On-Demand Enrichment of Data

Empower your security analysts and threat hunters throughout the investigation phase, not just at the time alerts are announced. Alerts and data enrichment can be added or refreshed at any time to keep context up-to-date and relevant. Automate the gathering of system level data and publicly available threat intelligence. Enhance log data with insight about user assets, identified suspicious domains, data from open-source intel reports, and even relevant dark web chatter.



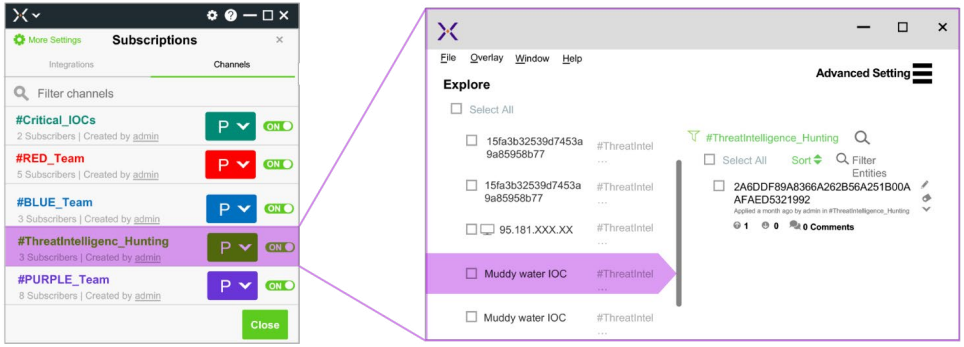
Annotate Within Workflows

Comment, document, and share observations made during investigations to improve efficiency. Using color-coded best practices, you can easily see patterns based on data type, urgency, and source.



Collaborate Across Teams

Share specific information across teams or trusted groups through dedicated channels. Examples of these trusted groups include inter-organization, intra-organization, red, blue, and purple teams. These channels serve as a mechanism to provide relevant details about threat detection, investigation, and response activities.



For more information about Securonix Investigate, schedule a demo at: www.securonix.com/request-a-demo

securonix