DATASHEET

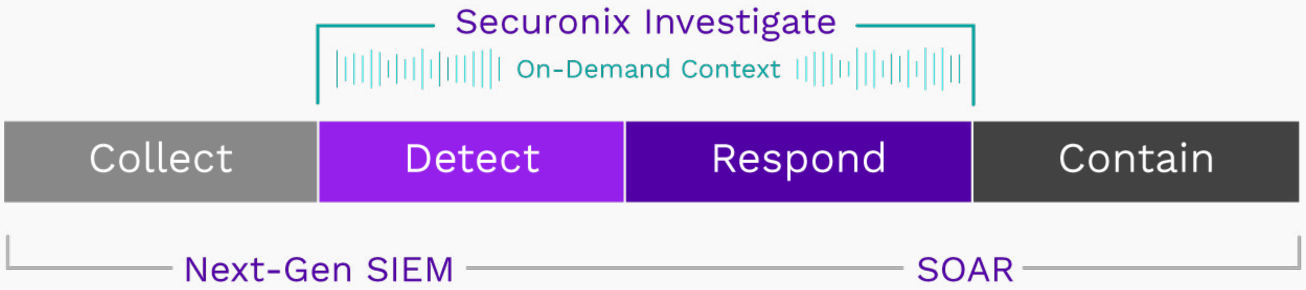
Securonix Investigate

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. Securonix Investigate leverages generative artificial intelligence to deliver deeper details about observations to keep the investigation moving forward. 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. Share knowledge and collaborate across teams by annotating context strings with relevant insights.

Accelerate Threat Mitigation

Dynamically enrich incidents under investigation with context and automatically gather updated details.

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.

Curate Relevant Information via AI

Get AI-generated information about technologies, entities, and other observations by simply asking any question within the Securonix Investigate window.

Communicate Knowledge Across Teams

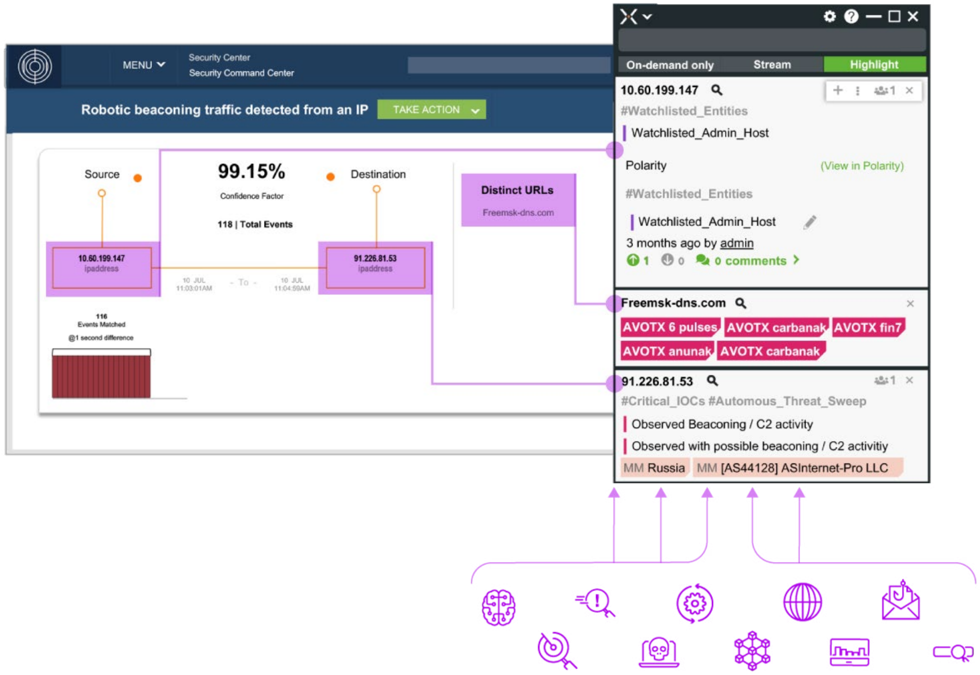
Annotate, document, and share observations across trusted groups within investigation workflows.

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.



Robotic beaconing traffic detected from an IP

99.15% Confidence Factor

118 | Total Events

10.60.199.147 ipaddress — 10 JUL 11:03:01AM - To - 10 JUL 11:04:59AM — 91.226.81.53 ipaddress

116 Events Matched @1 second difference

Distinct URLs: Freemsk-dns.com

10.60.199.147
#Watchlisted_Entities
Watchlisted_Admin_Host
Polarity (View in Polarity)
#Watchlisted_Entities
Watchlisted_Admin_Host
3 months ago by admin
1 0 0 comments

Freemsk-dns.com
AVOTX 6 pulses AVOTX carbanak AVOTX fin7 AVOTX anunak AVOTX carbanak

91.226.81.53
#Critical_IOCs #Automous_Threat_Sweep
Observed Beaconing / C2 activity
Observed with possible beaconing / C2 activitiy
MM Russia MM [AS44128] ASInternet-Pro LLC

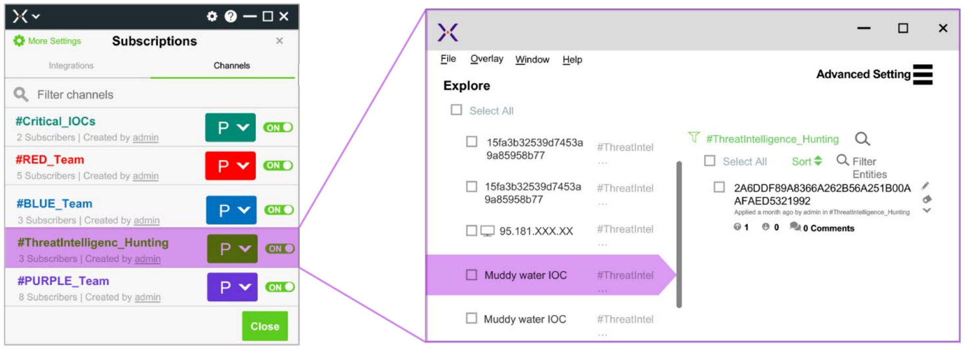
Harness the Power of AI

Interact with Generative Artificial Intelligence via ChatGPT alongside all other Securonix Investigate data sources for a central view of relevant context and to cross reference data. Through natural language you get AI-powered responses including explanations about unfamiliar technologies, information about command purposes, and help to create threat content. Securonix Investigate provides additional security controls and auditability to protect against sensitive data leaks and to meet compliance. This results in higher efficiency, shorter investigation times, and faster threat remediation.

ChatGPT

Collaborate Across Teams

Annotate, document, and share observations made during investigations to improve efficiency. 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.



#Critical_IOCs
2 Subscribers | Created by admin

#RED_Team
5 Subscribers | Created by admin

#BLUE_Team
3 Subscribers | Created by admin

#ThreatIntelligenc_Hunting
3 Subscribers | Created by admin

#PURPLE_Team
8 Subscribers | Created by admin

□ Select All
□ 15fa3b32539d7453a9a85958b77 #ThreatIntel
□ 15fa3b32539d7453a9a85958b77 #ThreatIntel
□ 95.181.XXX.XX #ThreatIntel
□ Muddy water IOC #ThreatIntel
□ Muddy water IOC #ThreatIntel

#ThreatIntelligence_Hunting
□ Select All
□ 2A6DDF89A8366A262B56A251B00AAFAED5321992
Applied a month ago by admin in #ThreatIntelligence_Hunting
1 0 0 Comments

Note: Securonix Investigate is only available directly from Securonix.

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