securonix

DATASHEET

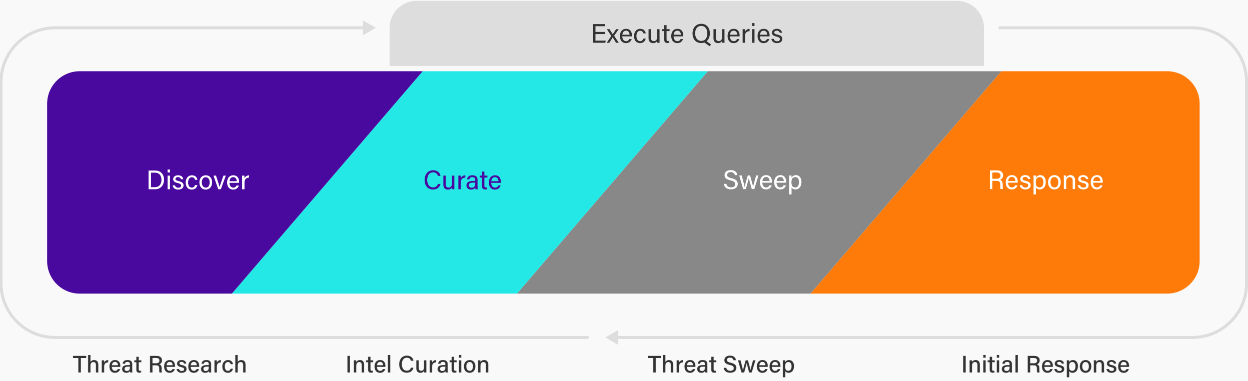
Autonomous Threat Sweeper

Automate Threat Advisories and Post-hoc Detection
for Cyber Rapid Response

Provide Air-Cover for Your SOC

Security teams are under tremendous pressure to keep pace with the velocity of new and emerging threats. As cyberattacks continue to grow in breadth and scale, organizations need autonomous solutions that can assess the exposure to emerging threats on an ongoing basis.

Leveraging the latest research and threat content from Securonix Threat Labs, Autonomous Threat Sweeper (ATS) codifies many of the manual aspects of investigation. Our solution acts as an air-cover for your security team by automating the process of assessing your exposure and initiating incident response.



ATS helps you detect unknown threats present in your environment with curated threat intelligence, and automated detection engineering and investigation.

The Benefits of ATS

Stay Ahead of Emerging and Developing Threats

Empower your team to prioritize high-risk threats with continuously curated threat intelligence. ATS acts like an extension to your SOC with retroactive searches across large volumes of logs and historical time frames.

Quickly Know Your Exposure

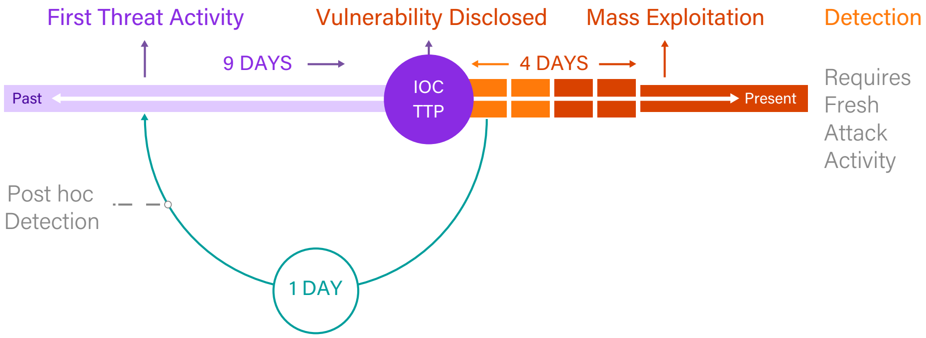
Quickly know your exposure to emerging threats with attack-centric IOC and TTP-based detection. ATS enhances your SIEM with the ability to detect low and slow threats through post-hoc detection of both IOCs and TTPs, extracted and codified by Securonix Threat Labs.

Accelerate Cyber Rapid Response

Accelerate cyber rapid response with automated reporting, alerting, and incident creation. By continuously monitoring your environment and curating intelligence on emerging threats, ATS helps security teams drive down their mean time to respond (MTTR) and prioritize critical threats.

Unlock SOC Efficiency with Autonomous Threat Sweeper

ATS' robust feature set enables security teams to offload many day-to-day investigation tasks so they can focus on the threats that matter most.



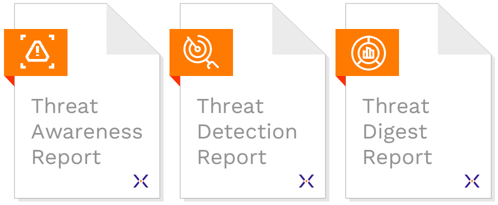
Curated Threat Advisories

Know when threats are present with up-to-date threat content and reports.

Threat Intelligence: Get up-to-date threat content curated by the experts on our Threat Labs team.

Bring Your Own Intelligence: Upload your own IoC's via ATS to sweep against all of your data sources. This allows you to nvestigate multiple malware-related indicators by consolidating and searching all relevant data sources in one place.

Threat Awareness Reports: Get notified immediately as emerging, critical threats appear in your environment.

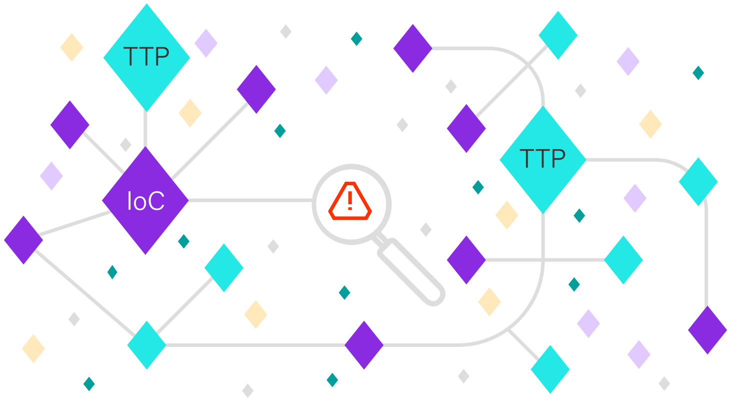


Multi-Vector Detection Mode

Leverage multiple detection methodologies to discover both "known-known" indicators of compromise and "known-unknown" indicators of action derived from TTPs.

IOC Detection Mode: Extracts Indicators of Compromise from threat intelligence to hunt for emerging threats hidden in your long-term, historical data.

TTP Detection Mode: Analyzes the Tactics, Techniques, and Procedures, helping threat hunters identify Indicators of Action in the absence of prior knowledge about IOC's.



Advanced Reporting and Alerting

ATS alerts your security team and provides comprehensive reporting, automated incident creation, and actionable guidance for remediation.

Automation: ATS speeds up detection and response by executing searches and queries to automatically sweep your environment for signs of compromise in current and historical data.

Actionable Guidance: Get detailed findings and remediation guidance if IOCs and TTPs are detected in your environment.

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