securonix

SOLUTION BRIEF

Securonix Threat Coverage Analyzer

Easily understand your threat coverage and SOC maturity with one simple tool

Why Securonix Threat Coverage Analyzer?

Eliminating gaps in your threat coverage remains a pressing concern for many organizations. With industry standards and frameworks constantly shifting, it can be difficult to know where you stand.

That's why we built Threat Coverage Analyzer (TCA) that lets you quickly assess your SOC maturity and threat coverage on an ongoing basis. With TCA, implementing programs for MITRE ATT&CK, PCI, Insider Threat, and others becomes straightforward. We eliminate complexity for analysts with visualized dashboards and assist you in strategizing the next steps to meet your organization's cybersecurity requirements.

Solution Benefits

Achieve Faster ROI with your SIEM

By understanding gaps in threat coverage and then onboarding threat content to cover your gaps, you are able to get the most out of your SIEM. New customers are also able to map existing use cases to Securonix out-of-the-box content in order to migrate their use cases more efficiently

Implement Industry Frameworks with Ease

See how your coverage stacks up and aligns with popular frameworks like MITRE to protect your organization against emerging threats.

Take a Strategic Approach to Security Programs

Easily understand where you are in your security maturity journey and leverage easy-to-understand assessment tools and visualized analytics to make data-informed decisions on your security program's next steps.

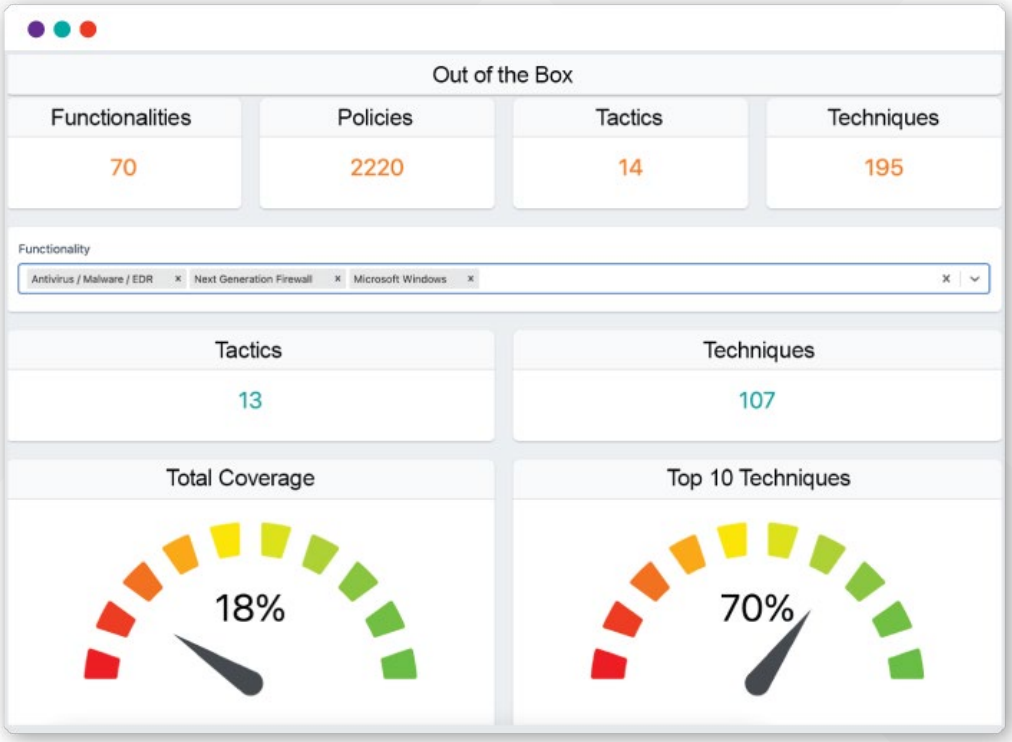

Figure 1: TCA scans SIEM content, maps it to frameworks, and identifies gaps so our team of experts can provide recommendations for next steps.

How It Works

Threat Coverage Analyzer gives you the information you need to improve your security posture and offloads repetitive and tedious tasks. TCA is part of Unified Defense SIEM and contains features that give you an interactive way to navigate, study and search security standards and frameworks.

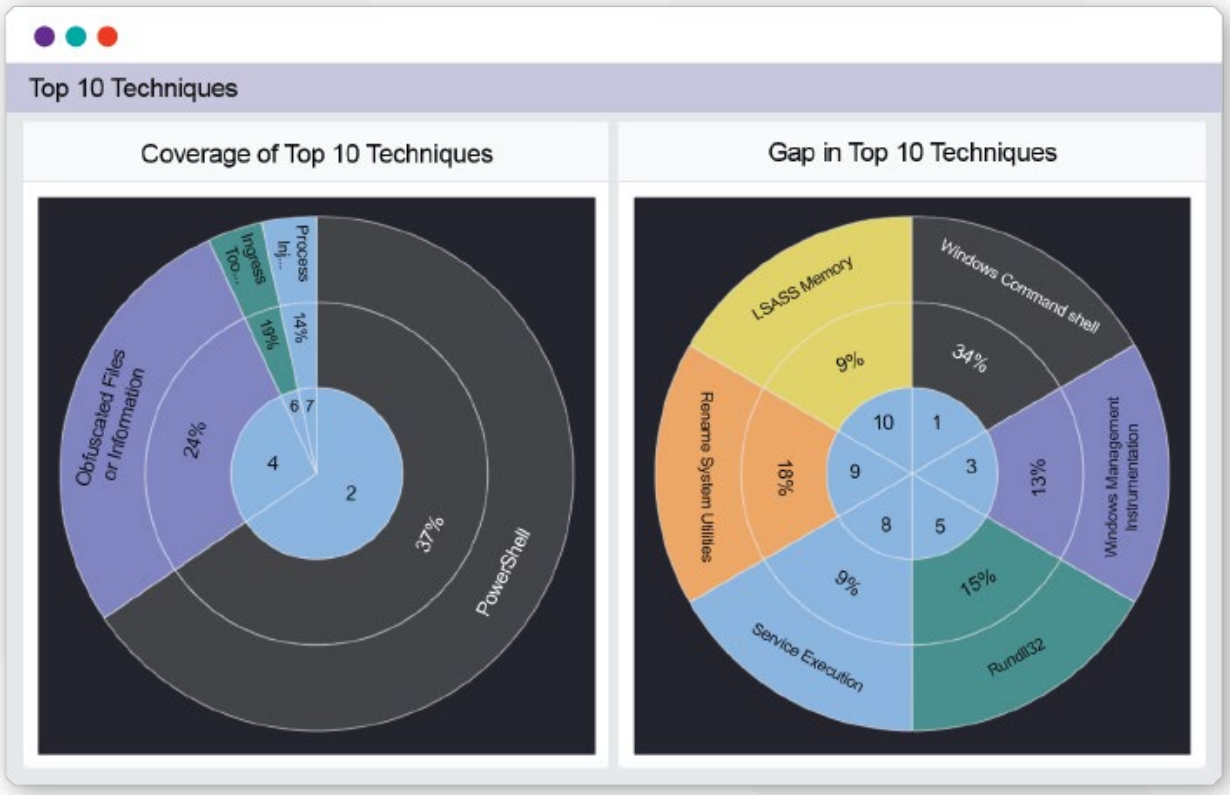

Figure 2: Utilize visualized dashboards to quickly understand your threat coverage

Threat Coverage Analyzer consists of the following features:

- **Planner:** Plan your SIEM and UEBA coverage according to popular industry frameworks and models like MITRE, PCI, and ITP-Insider Threat Programs. The Planner helps you identify your SIEM coverage and plan a strategy for various data onboarding scenarios such as onboarding a new IDS/IPS solution.
- **Reflector:** TCA's Reflector feature provides insights into your current data sources and their alignment with popular frameworks. Visualized through dashboards, this analysis shows your existing coverage. Combined with the Planner, these features enable comparing current and future SIEM / UEBA content and coverage.
- **Advisor:** This feature helps you visualize coverage against industry standards and recommends the best threat modules to be enabled for your environment.
- **Security Assessment:** Using Securonix Security Assessment (SSA), an interactive survey, you can identify SOC maturity gaps in areas like threat intel integrations, threat hunt capabilities, vulnerability management, risk assessment, SOAR capabilities, staffing and training needs, physical security, and more. This assessment is used by our professional services team to help you take a strategic approach to budgeting and planning.
- **Use Case Mapping (UCM):** With UCM, we take into account your specific organizational needs and recommend possible matches from our extensive library of 2,000 out-of-the-box content. By using fuzzy matching, MITRE techniques, and other advanced methods, we assist in a more tailored migration process to your unique organizational requirements. Our goal is to make the transition to Securonix easier and more efficient for you, ensuring a seamless experience as you embrace our platform.

Figure 3: Take a custom assessment to understand your maturity across dozens of areas

Use Cases for Threat Coverage Analyzer

Threat Coverage Analyzer helps simplify manual and tedious processes and enables security teams to understand the state of their security environment. Typical use cases for TCA include:

- Understand which security standards are available to you without having to search through CSV files and read through manuals.
- Easily transition to Securonix from another SIEM with a tailored migration that maps and imports your use cases for you.
- Assess where your organization is in their SOC maturity journey.
- Find gaps in the following areas: processes KPIs data source, ingestion watch lists, threat, intel, integrations, threat, hunt capabilities, vulnerability management, activities processes, risk assessment, soar capabilities, staffing needs, training needs, threat, team capabilities, physical security and more.

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

securonix

About Securonix

Securonix is leading the evolution of SIEM for today's hybrid cloud, data-driven enterprises. Securonix Unified Defense SIEM provides organizations with the first and only content-driven threat detection, investigation and response (TDIR) solution built with a highly scalable data cloud and a unified experience from the analyst to the CISO. The innovative cloud-native solution enables organizations to scale up their security operations and keep up with evolving threats. For more information visit securonix.com