LTIMindtree

With SOC Prime's platform, LTIMindtree saved 4,000 hours per year on threat research and detection content coding. SOC Prime's solution enabled LTIMindtree to deliver timely, relevant threat detection content to the company's end-customers matching their unique log sources, threat profiles, and disparate security tools faster and more efficiently than before. The company increased SOC efficiency by continuously streaming the latest detection algorithms aligned with MITRE ATT&CK® directly into their customers' SIEM & EDR instances.

Industry	Region	Company Size	SIEM & XDR in Use
IT Services and IT Consulting	**India**	**46,000+ employees**	**Securonix, Splunk, CrowdStrike, Sumo Logic**

Hemant Wagh
Associate Director, Information Security at LTIMindtree

> *"SOC Prime's platform is a time-saving solution, which offers a broad selection of features in a single place. Here we can find all the latest information on new threats enriched with relevant CTI, Threat Hunting guidelines, and MITRE ATT&CK context without spending hours browsing other cybersecurity resources to perform in-depth threat research and explore the latest updates in the cyber threat landscape. With SOC Prime's platform, there is no chance to miss any latest information on emerging threats."*

Highlights

- Increasing the end-customers' level of cyber maturity by automating the delivery of curated SOC content mapped to MITRE ATT&CK
- Accelerating exposure investigation and threat detection velocity through performance-optimized threat searches in end-customers' cloud-native environment
- Automating content streaming of the most up-to-date Detection-as-Code content directly into the SIEM or EDR instance in use
- Customizing content deployments tailored to unique organizations' environments and non-standard data schemas

Challenges

Resource Constraints and Alarming Attack Volumes

LTIMindtree has long been struggling to keep pace with authoring custom detection content, including the delivery of high-fidelity alerts and behavior-based hunting queries required of a large-scale MSSP that supports hundreds of global organizations with diverse security needs.

Multiple SIEM & EDR Solutions in Use

Delivering and supporting high-quality IT Services Consulting for nearly 500 clients from across the globe presents a daunting challenge and requires a solution capable of native translations for many diverse security tools and products.

Complexity of Manual Content Deployments

LTIMindtree's end-customers leverage multiple log sources and frequently apply non-standard tables, indexes, or fields in their environments that require default mapping for smooth content deployments.

Performing these SOC operations manually is time-consuming and frequently results in parsing issues, syntax errors, and other security hurdles.

Lack of Comprehensive Visibility Into Organization-Specific Threats
The ever-growing attack surface and an increasingly complex cyber threat landscape pose a pressing challenge for MSSP organizations to gather and analyze the entire pool of data across all end-customers' assets.

Solution

LTIMindtree chose SOC Prime's platform to accelerate their end-customers' digital transformation journey while saving time on daily threat research, in-house detection content development, and ensuring customization options that match the unique security needs of hundreds of company's clients.

With SOC Prime's seasoned expertise in 25+ SIEM, EDR, and XDR solutions, LTIMindtree was able to instantly deliver relevant detection content to their clients. To facilitate dynamic communication between SOC Prime and LTIMindtree, SOC Prime launched a dedicated Slack channel to address any identified gaps and fulfill the end-customers' demands in real time. As an example of fast-tracked customer responsiveness, LTIMindtree was able to deliver Securonix use cases to their clients just three months after making a feature request for SOC Prime's integration with this next-gen SIEM solution.

Achievements

Ultra-Responsiveness to the Latest Threats & Increased Cybersecurity Awareness

Leveraging SOC Prime's platform, LTIMindtree has provided its end-customers with in-depth contextually-enriched information on the latest threats and delivery of relevant detection content within 24 hours after threat discovery. As part of the value available from the world's largest collection of detection algorithms, LTIMindtree's SOC team is continuously updated on the latest trends in the cyber threat landscape via SOC Prime's blog and Cyber Library with direct access to live webinar sessions on Threat Hunting, Detection Engineering, and other professional topics.

Delivery of Custom Detection Content Tailored for Multiple SIEM & EDR Solutions

With access to an immense library of 11,000+ Sigma rules written in the universal detection format, LTIMindtree can deliver curated behavior-based detections automatically converted to Securonix, Splunk, CrowdStrike, and Sumo Logic formats to match the environment needs of the company's end-customers. This has helped overcome cross-tool migration challenges and enabled the company to save hundreds of hours on content fine-tuning for smooth deployment to the customers' environment. Leveraging SOC Prime's platform, LTIMindtree has accelerated the delivery of custom use cases for organizations in multiple industries, including banking, energy, and healthcare sectors which require adherence to exacting compliance standards.

Increased Threat Visibility & Streamlined Threat Investigation

Aligned with the MITRE ATT&CK industry standard, SOC Prime's platform provides relevant information on adversary tactics, techniques, and sub-techniques. This has ensured LTIMindtree can increase cybersecurity effectiveness and dynamically report on individual company progress with a widely recognized MITRE ATT&CK framework reference, CTI links, and CVE descriptions.

Automated Streaming of Detection Logic Customized to Environment Needs

With SOC Prime, LTIMindtree's clients can continuously stream up-to-date detection algorithms directly into their environment using the Continuous Content Management (CCM) module. Organizations leveraging the Splunk solution can make the most of the Splunk CCM app designed to accelerate content deployment and management capabilities. Once the detection from the selected content list matches the pre-configured tags, the company's customers receive real-time alerts in the CCM app keeping their Splunk instance constantly updated on the latest threats. SOC Prime's platform also allows applying non-standard data schemas leveraging the Custom Field Mapping capabilities. Since LTIMindtree's end-customers use multiple log sources with unique field names, creating Custom Field Mapping profiles and linking them to scheduled jobs helps avoid parsing issues and streamlines non-standard content deployments.

Accelerated IOC-Based Threat Hunting

SOC Prime's Uncoder IO has enabled the company to supercharge IOC-based searches for threats leveraging automatically generated custom queries ready to run in multiple SIEM & XDR environments.

About LTIMindtree

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700+ clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by nearly 82,000 talented and entrepreneurial professionals across 30+ countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale.