





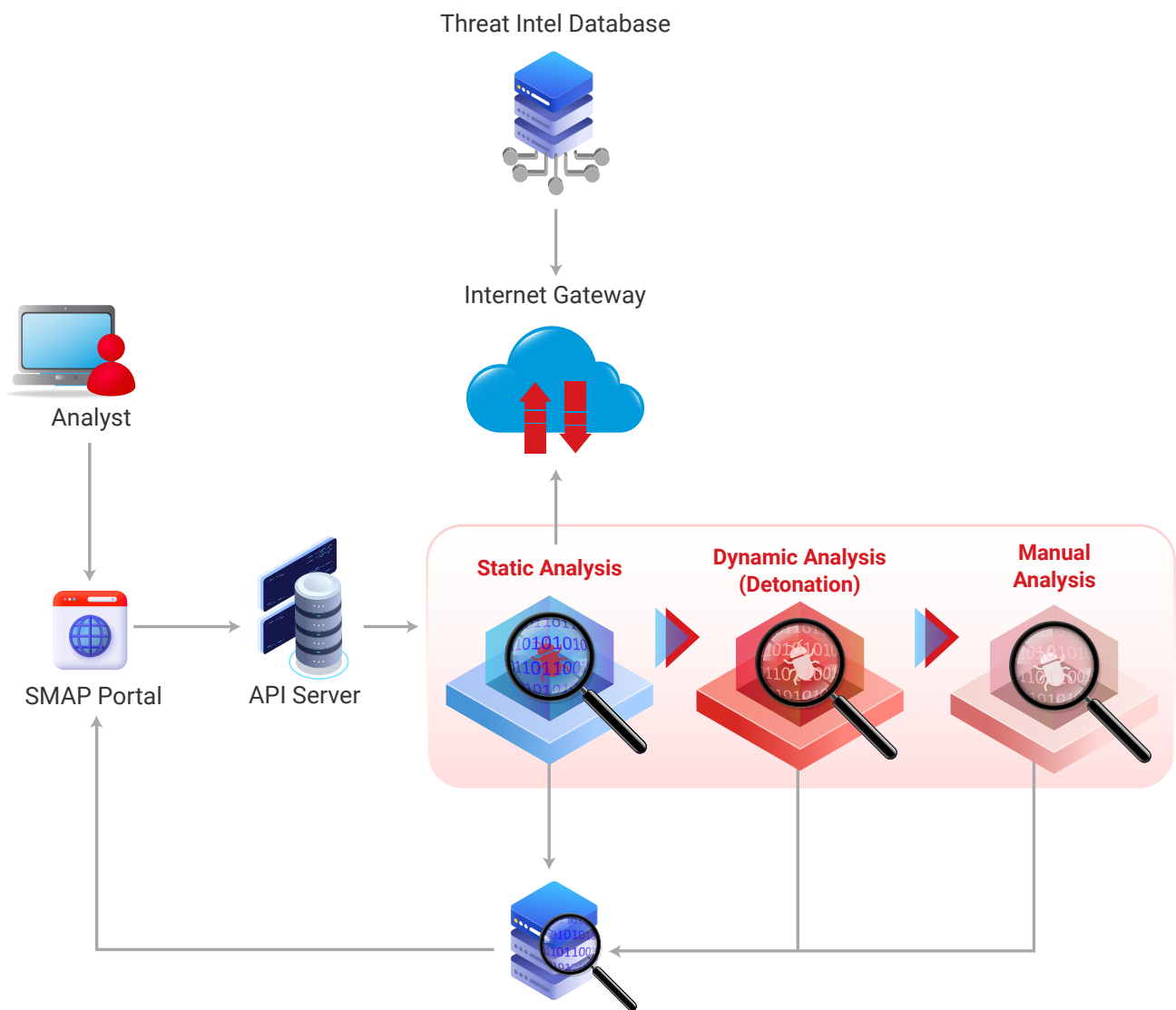
Introduction

Seqrite Malware Analysis Platform (SMAP) is an advanced cybersecurity solution designed to detect, analyze, and respond to evolving malware threats. The platform leverages multi-stage processing, behavior-based detection, and deep forensic analysis to deliver comprehensive threat intelligence. It integrates seamlessly with **SIEM**, **SOAR**, and **EDR/XDR** platforms, ensuring enhanced threat detection and mitigation.



Seqrite Malware Analysis Platform Architecture

An architecture which powers deep malware insights through layered analysis, real-time verdicts, and seamless integration into your security ecosystem.





Key Capabilities



Multi-Stage Analysis

Combines Static, Behavior-Based, and Manual Analysis for comprehensive threat assessment.



Behavior-Based Detection

Detects suspicious or malicious behavior by monitoring runtime activities and Indicators of Compromise (IOCs).



IOC Extraction

Automatically extracts and presents all observed Indicators of Compromise for threat hunting and correlation.



Threat Researcher Support

Allows analysts to contribute manual findings and enhance detection accuracy and knowledge base.



On-Premise Deployment

Fully functional in air-gapped or restricted network environments, ensuring data privacy and compliance.



Detailed Reporting

Generates JSON and PDF reports mapped to MITRE ATT&CK. Includes graphical process trees, parent-child process relationships, and visual evidence of execution.



Role-Based Access Control (RBAC)

Provides secure, multi-user access with customizable permissions based on roles and responsibilities.



Tagging

Automatically classify files based on malware family, category, TTPs (Tactics, Techniques, and Procedures), and extracted IOCs.



Signature-Based Detection

Quickly identify known malware using existing pattern databases.



Network Traffic Analysis

Analyzes network behavior to detect C2 (Command-and-Control) communications, botnet traffic, and data exfiltration attempts.



Reputation Lookup

Leverages over one billion classified records (Clean/Malicious) for quick threat intelligence enrichment.



Extensive File Type Support

Supports analysis of executables, documents, PDFs, scripts, archives, and more.



Automated Sample Queuing

Supports bulk uploading and queued processing of large volumes of files for seamless automation.



Integration with Interfaces

Enables automated sample submissions and seamless integration with external threat security control e.g. SOAR, SIEM, XDR etc.



Advanced Search

Enables granular search across SHA-256 hashes, file types, severity levels, verdicts, and more.



Seqrite Malware Analysis Platform Portal

Intuitive user interface with built-in analytics and dashboards, including threat trends from Seqrite Lab with visibility into India-specific threat activity.



Benefits of Seqrite Malware Analysis Platform



Comprehensive Protection

Analyze files across multiple stages to detect and mitigate a wide range of threats.



Extensive Repository Access

Leverage insights from over five lakhs daily analyzed samples in Seqrite's comprehensive database.



Faster Incident Response

Reduce Incident response time by performing a Reputation lookup or Detailed Behavior analysis for the suspicious sample using our Seqrite Malware Analysis Platform.



Improved Compliance

Helps meet industry standards by proactively identifying and mitigating risks.




Actionable Insights

Detailed analysis reports provide immediate steps to address vulnerabilities.



Scalable Architecture

Suitable for enterprises of all sizes.



About Seqrite

Seqrite is a leading enterprise cybersecurity solutions provider. With a focus on simplifying cybersecurity, Seqrite delivers comprehensive solutions and services through our patented, AI/ML-powered tech stack to protect businesses against the latest threats by securing devices, applications, networks, cloud, data, and identity. Seqrite is the Enterprise arm of the global cybersecurity brand, Quick Heal Technologies Limited, the only listed cybersecurity products and solutions company in India.

Today, 30,000+ enterprises in more than 70+ countries trust Seqrite with their cybersecurity needs.



Quick Heal Technologies Limited

Phone: 1800-212-7377 | info@seqrite.com | www.seqrite.com |    /seqrite

All Intellectual Property Right(s) including trademark(s), logo(s) and copyright(s) are properties of their respective owners. Copyright © 2024 Quick Heal Technologies Ltd. All rights reserved.