

SOC as a platform (SOCaaS), a next-gen SOC-as-a-Platform offering, which includes people, process and technology. SOCaaS offers full white-label capability that makes it easy to add managed security services to a portfolio.

White Label our SOC Platform with Your Brand

Comodo's complete SOC platform offers full white label capability for any MSP, MSSP or enterprise. SOCaaS is ready-made to provide access to your own SOC in under 24 hours, with zero capital outlay. It provides full-stack autonomous security that eliminates false positives and reduces attacker dwell time to seconds. It also includes the following:

Protection with Auto Containment

The patent-pending auto containment technology is the world's only active breach protection that stops ransomware, malware, or cyber-attacks from causing damage. This allows protection of the systems without having to rely on detection of any sort.

SOC Management Platform

A cloud native platform covering SIEM, analytics, case management and threat sharing, with artificial intelligence capabilities and a semi-supervised artificial intelligence engine that learns from the activities, events and operations.

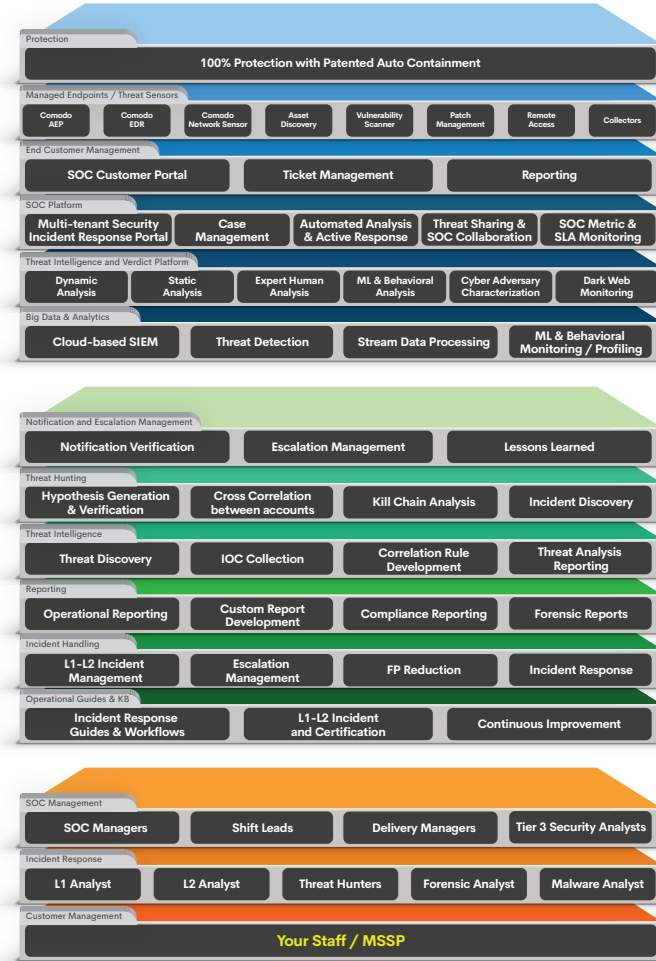
Cloud-Native Network Detection and Response

Enterprise-class network traffic analysis that detects suspicious behaviors, prioritizes investigations for the highest risk threats, and automates responses. It captures network traffic, generates extensive metadata for important network protocols, and sends this data to the cloud to correlate with endpoint sensor data.

SOC-as-a-Service

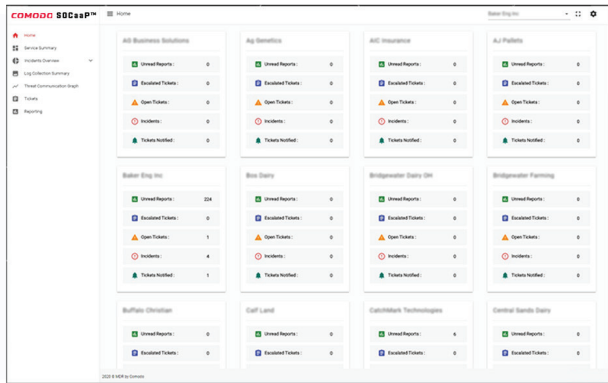
Full blown SOC services with threat hunting teams combined with system-generated alerts to detect malicious activity and provide incident response. It incorporates artificial intelligence capabilities with a semi-supervised artificial intelligence engine that learns from activities and operations of Comodo's cybersecurity experts, accelerating the detection and response to new threats.

TECHNOLOGY
PROCESS
PEOPLE



Visual Analytics

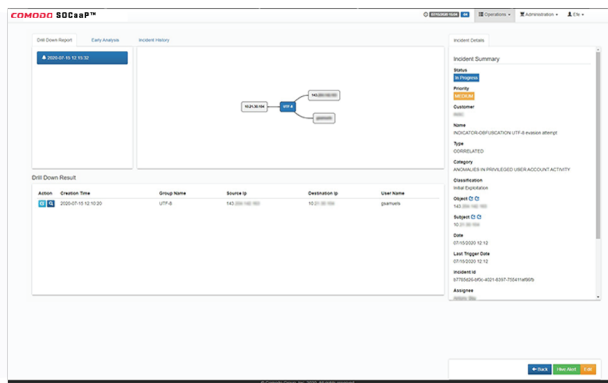
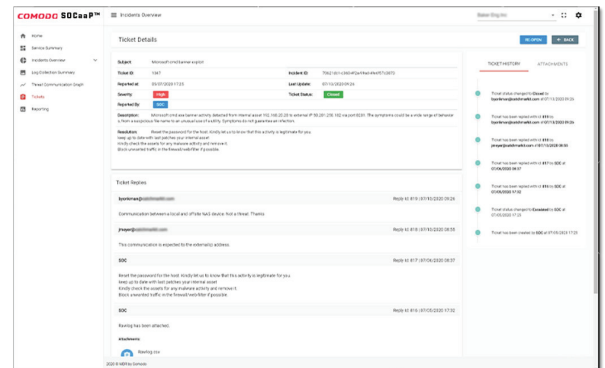
Co-managed SIEM and visual analytics platform accessible by you and customers. It enables highlighting hidden threats and helps with understanding the main causes of any incidents so it can be described to customers.



Multi-Tenant Security Incident Response Portal Gives a snapshot of customer's security statuses, incident escalations and reporting needs. It is also a central portal where all customer interactions can be managed.

SOC Customer Portal

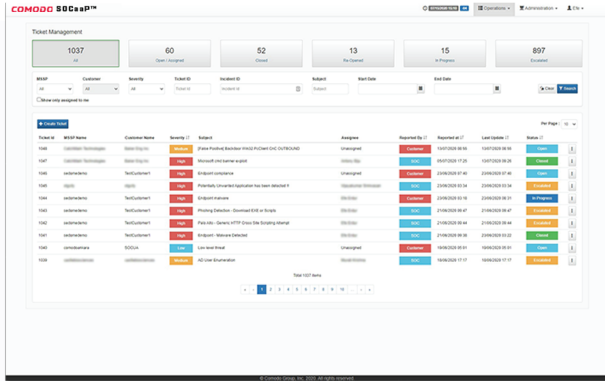
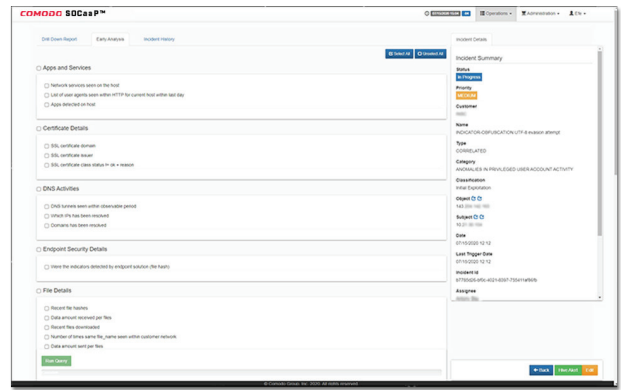
Co-managed SIEM and visual analytics platform accessible by you and customers. It enables highlighting hidden threats, helps you understand the main causes of any incidents and describe it to your customers.



Snapshot Reporting Gives a snapshot of your customer's security statuses, incident escalations, reporting needs. It is also a central portal where all customer interactions can be managed.

Analyzes and Automates

Automates all necessary early analysis, the system will analyze all observables that's been collected and prepares a consolidated result that can be used in the investigation and incident reporting. It combines various analysis tools into one unique service.

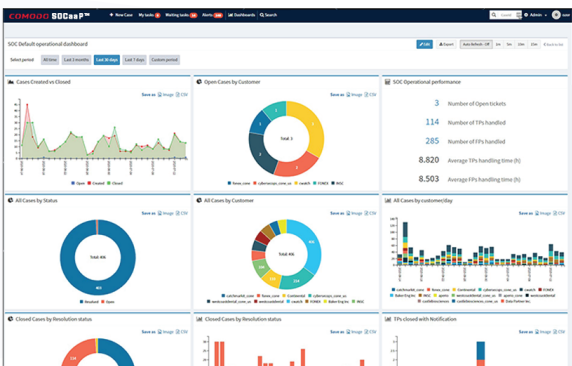
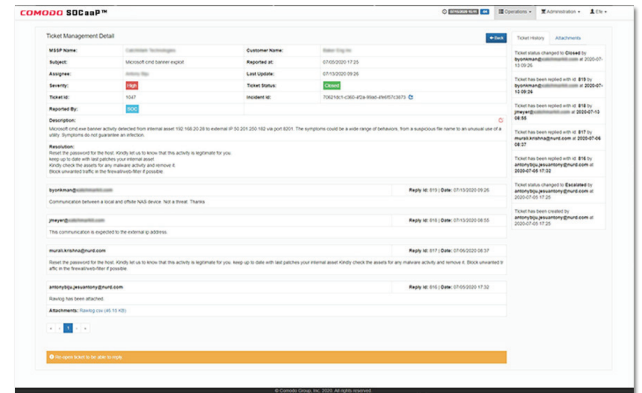


Collaborative SOC Platform

Provides central management of all incidents and responses. With our shared responsibility model, Comodo SOC will also collaborate with you to give the best security service for your customers. We can analyze, escalate, hunt and report together.

Ticket and Case Management

Provides security related ticket and case management. All security incidents can be escalated and reporting to your customers is in one place; all relevant evidences are automatically attached and sent to the customer.



SOC METRIC & SLA MONITORING

Extract all SOC related operational metrics and monitor SLAs to your customers. Improving the efficiency is always highest priority where it starts with visibility over all SOC operations and metrics.