



Detect | Collaborate | Secure

See **collaboration** in your existing perimeter Defense **infrastructure**

Enhance the capability of your existing security infrastructure by integrating a **real-time collaborative** ecosystem that cross processes **intelligence** to provide timely and accurate **active attacker** detection.

Correlate every threat with the most **updated security information** and take preventive action in areas where conventional security system with external update dependencies would fail.

Scale up to your requirements rather than making your network adjust to a proprietary box package. Grow or redeploy the system with **ease and speed**.

Manage threats even at a local level effectively without over-dependence on connectivity with external systems. Gather, manage and **interpret data** from multiple devices and **deal with threats** based on their priority.

Automate and **speed up your analysis** and detection **process with accuracy**.

Stay assured with an ever-watchful **team of intrusion analysts** and skilled team to take care of any support requirements.

Avoid capital expenditure for a license / upgrade and avail the best technoservice. Stay in **control of your costs** with the benefits of a simple and scalable service model.

ACTIVE ATTACKER DETECTION

- Real-time visualization of active attackers across geographical location
- Vulnerability driven prioritization of attacks
- Detection of worm outbreak without updated signatures or anti-virus updates
- Early warning system for floods across clients detecting anomalies in traffic patterns

ATTACK MANAGEMENT

- Decentralized collection and management of events data by on-site data collection engine
- Real-time translation, normalization and prioritization of attack data
- Attack and attacker trend identification without transfer of log outside local network perimeter

PROCESS INFORMATION

- Complete attack analysis and management framework for incident handlers
- Event escalation and response procedures between multiple handler teams
- Manual verification option for each action chain within the automated framework

INTELLIGENCE

- Continuous development of attack trends across devices / sites / groups / organizations monitored by CNAM
- Consolidated data with repeated cross site validation of generated trend data
- Automated rule deployment with real-time updates on trend and analytic information
- Integration with advisory engine for dissemination of intelligence gathered

SCALABILITY

- Quick integration of sites into CNAM framework across the globe
- Multi-site integration with granular detection parameters and weights

- Single view monitoring of security devices with wide intelligence data across organizations
- Easy SOC rollout options with central integration of sites into CNAM framework

SUPPORT / MAINTENANCE

- Round the clock monitoring of RAW data generated by on-site security infrastructure
- Automated device and data monitoring with continuous health checks for detection errors
- Data freshness monitoring for management of data-sources
- L1 / L2 / L3 support by partner teams and intrusion analysis operating on predefined processes guidelines for maintenance

AUTOMATION

- Automated data collection, trending, correlation rule design and deployment
- Rule management for detection engines with automated updates and centralized configuration
- Automated data / configuration backup and archival for on-site data engines
- Comprehensive notification engine on all events configured for each stakeholder

DETECTION SUPPORT

- Customization support for deployed detection infrastructure with custom detection rules
- Proprietary engines for early detection of worm outbreaks and floods
- Community framework for sharing intelligence data to improve detection accuracy

PRICING

- SaaS model delivers shared costs across clients using CNAM
- No capital expenditure
- Pay per use licensing providing small / medium sized enterprises value for money
- Flexible pricing options for wide enterprise users thereby easing out expansion worries



netmonastery
active threat defacement

NetMonastery Network Security Private Limited
Tel: +91 22 40111911 E Mail: sales@net-mon.net