

Security Monitoring 360

Transform your investments in the existing security infrastructure into an effective real-time attack detection system



netmonastery
active threat defacement

Common Pain Areas

netmonastery.com

Issues commonly faced by enterprise and or an organization with web presence

Un-Monitored Traffic

Attack alerts from security devices are often only reviewed on a periodic basis resulting in delayed reaction to critical attack notifications.

Plug and play devices are often deployed without much customization, resulting in loss of accuracy in detection of specific attacks.

Information Overload

The volume of logs generated by security devices makes it practically impossible for a team to analyze in a reasonable amount of time in order to identify attackers.

Intrusion Prevention Systems are not deployed in the blocking mode due to fear of blocking legitimate business users, thereby losing its application.

Threat Awareness

Attack methods once successful are re-used continuously to increase the return from a single vulnerability.

Infected hosts infect their network and a large infected network is a source of typical worm outbreaks that bring down operations.

Security Insights

An Intrusion Detection System produces an average of 78,000 alerts a day

Top 10 attackers reported by popular log analysis tools are likely to identify only 6% of the actual active attackers

88% of intrusion prevention systems operate in the alert only mode

Active attackers probe and interact with the target for an average of 210 hours before attempting a breakdown

Average survivability time on the internet is approximately 20 minutes



netmonastery
active threat defacement

Integrated Security Management

netmonastery.com

A brief preview of Comprehensive Network Attack Monitoring (CNAM)

Integration

Quick and seamless integration with pre-existing security infrastructure such as Intrusion Detection / Prevention System, Firewall, Servers and Application.

Log Management of monitored devices is delivered with practically no change to the existing topology. Additionally, CNAM's out of band architecture negates and risk of failure and latency.

Security Management

Real-time processing and prioritization of attacker data identifies net-suspicious event patterns, which are correlated with intelligence to identify active attackers.

CNAM provides integration of multiple security services in order to empower the customer with the required visibility and control its network assets.

Log Compliance

CNAM operates in a distributed model providing benefits of the process and compliance to its customers. A CNAM deployment does not demand log transfer or any kind of log data aggregation to remote site

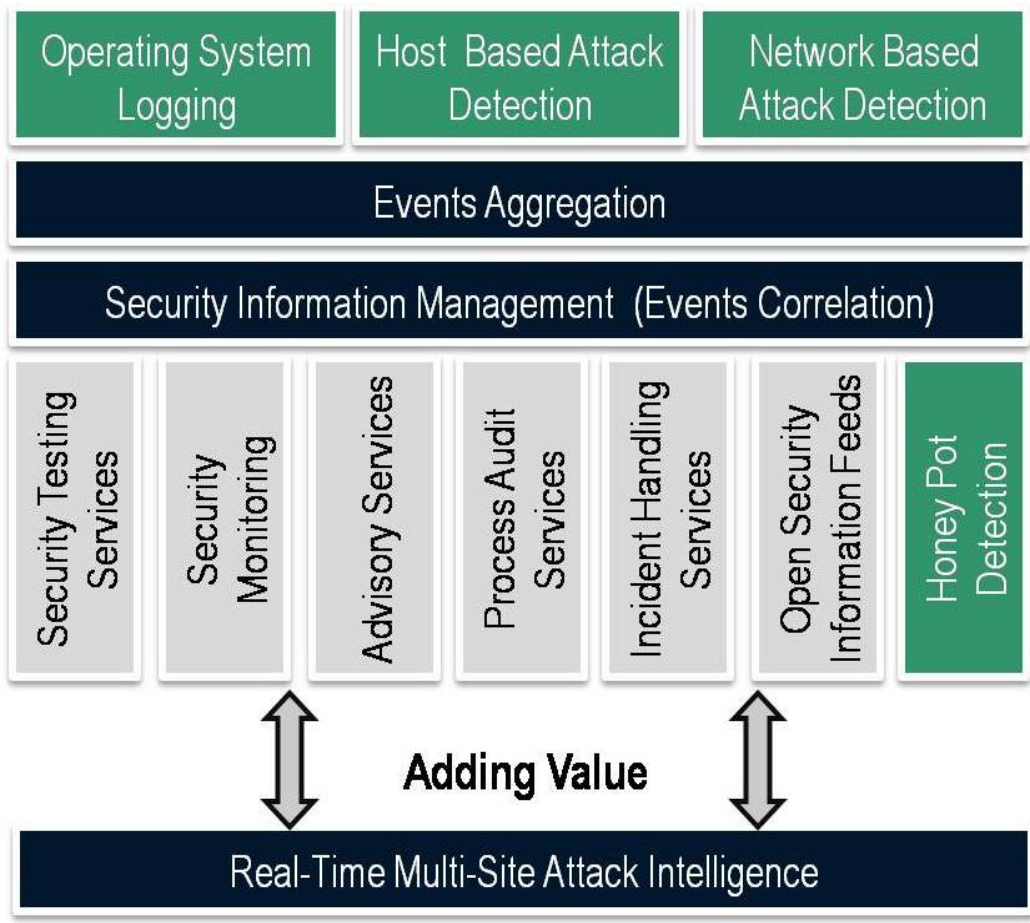
Deployment of CNAM also reverses the need to build a log aggregation network across multiple sites, infact the Central Intelligence Processing Facility function with minimal transactions with each CNAM site



netmonastery
active threat defacement

Deliverables and Benefits

A shortlist of key deliverables and their corresponding benefits



CNAM Benefits

Use existing infrastructure to **proactively prevent attack** against our network

Software as a Service (SaaS) **requires no CAPEX**

Manage security operations effectively and **reduce overheads** of manpower and facility

Utilize neighborhood **network attack information** to improve accuracy of attacker detection

Site **specific customization** at an aggregated cost

Attacker detection now **governed by SLA**

24x7 team on intrusion **analysts to support** your security issues and protect your network assets