NETMONASTERY
NETWORTH SECURED

DETECTION - FLY PAGE

Detecting threats with deadly accuracy

Since the last decade, CNAM has been the only platform to correlate threat detection as a composite part of the threat management program. Standard off the shelf detection tools available leave plenty to be desired in terms of coverage and detection capability. CNAM brings on board a comprehensive set of modules, designed to detect the latest attacks and provide complete coverage to the threat spectrum. **An extensively researched detection system with measurable benefits is available on an easy pay-as-you-go model just for your enterprise.**

23
Million threats
Processed by
CNAM, Every Day !

This is what we mean when we say **"Threat Detection"**

Managed Intrusion Detection
In the core is a strong, customised detection unit

-- A strong intrusion detection device, far advanced from just a signature based detection system
-- Individual customisation for each network segment with a continuous update process
-- Managed cutting edge profiles for trends

Traffic Anomaly Engine
Picking threats from patterns of network usage

-- Special engine for detection of attacks on traffic
-- Uses rapid samples to detect deviations in historic profiles and protocol usage
-- Detects attacks like DoS, DDoS, BotComs, proxies and p2p violations

Protocol Analysers
Identifying threats that fail to comply

-- Detection engines for application protocols in use, which help to reduce false positives
-- Centrally coordinated to build trends
-- Detect attacks like app violations, injections and app based data structure attacks

Collaborative Outbreak Detection
Compiling threats across intelligence sources

-- Detecting outbreaks early is a key to security for any enterprise, CNAM does it with a custom engine
-- Detects attacks like worms, advanced persistent threats and malware based threats

Trend Development
Detecting threats based on zero precedence

-- Real-time packet normalisation and trending, which help build your own intelligence pool
-- Detects attacks like BotComs, exploit kits, advanced persistent threats, p2p malware and aid in correlating attacks from other engines

Application Kits
Get into the application layer, see the difference

-- Standard Apps operate without communicating with the security infrastructure
-- CNAM integrates your apps into the detection
-- Detects a large number of application attacks that are otherwise undetectable
-- Accurate detection of SQL injection, XSS, BlindSQLi and manual auth brute forcing

Want to know more.... get a private demo arranged.
Write to us at **sales@netmonastery.com**

NETMONASTERY NSPL
+91 22 40111 911 netmonastery
netmonastery.com