threatsentry

COMPONENTS & PROCESSES

REQUEST

Conventional Rules Engine

KNOWLEDGE - BASE	KNOWLEDGE – BASE INTERFACE
Pre-configured rule-set comprised of known exploitive techniques and attack characteristics.	Module enables system administrator to add, remove or edit the knowledgebase, and pre-assign classification values to specific IPs and IP ranges.

Behavioral Engine

ADAPTIVE SECURITY ENGINE	ASE INTERFACE
Neural system profiling and comparative analysis engine organizes server requests into a multi-dimensional baseline of typical activity. Server connections are compared against the baseline (after filtering through the knowledgebase) to identify, trigger notification and take preventative action against any activity falling outside of trusted parameters.	The system administrator can influence the baseline by reclassifying training events or security alerts. Intrusion prevention capabilities progressively improve as the baseline evolves automatically or based on input from the system administrator.

EVENT CLASSIFICATION

TRUSTED

UNTRUSTED

NOTIFICATION/ACTION

Monitoring- Inactive	✓ Display, audio, email, pager, cell phone
Monitoring - Active	✓ Display, audio, email, pager, cell phone ✓ Post 404 error for Blocked IPs ✓ Add untrusted IPs to the Blocked List ✓ Block Untrusted requests ✓ Close all ports to Blocked IPs – Firewall ✓ Stop web services (IIS)

LOGGING/REPORTING/AUDIT

✓ Training Database
✓ Security Alert Log
✓ Event Details, WHOIS DB Lookup
✓ Log/Event search, sort, export
✓ Blocked/Trusted IP Lists
✓ Re-classified Event IDs
✓ HTML Reports