

## **Centralized Active Threat Management with Command, Control, Communication and Resolution (C<sup>3</sup>R) capability for IA/CND**

### **Abstract:**

As incidents of malicious attacks on corporate information and resources rise, organizations must fortify their security practices and implement more proactive measures to ensure the ongoing safety of their networks, servers and applications. The Command, Control, Communication and Resolution (C<sup>3</sup>R) capability needed to deal with threats in a best-of-breed, multi-vendor, network-centric infrastructure of an Enterprise are daunting. With mammoth amount of information from variety of sources, format differences in information received, lack of analysis and correlation tools plus lack of unified workflow tools to leverage the existing knowledgebase and capture new knowledge for future use, prevents implementation of effective IA/CND solution within an enterprise. This paper explores, the current implementations that have began to address these issues and identifies a road-map for future enhancements in this capability based on the commercial industry experience.

### **Overview:**

Today's multi-vendor environment presents additional challenges to the network and security administrators. The typical network may have network and security devices from leading vendors such as Cisco, Intel, CheckPoint, SonicWall, Netscreen, and Raptor platforms. The IDS sensors themselves may be from Internet Security Systems (ISS), SNORT and Cisco. Each vendor device comes with its own management system, its own log analysis and reporting tools that do not look beyond the individual vendor platform. An added challenge is that the event information being received such as system alerts, logs or SNMP traps may be presented in a standard or a proprietary format which may vary with different versions of the product.

The problem is further compounded by the massive amount of event data that needs to be gathered, analyzed and reported to the security administrator on a daily basis. Each firewall or IDS system could easily generate multi-gigabytes of information per day. If there is an attack in progress the data size may increase by ten fold. With the current set of limited tools from device vendors that do not scale across multiple platforms, most of the security event data is completely ignored or partially attended to, creating a massive hole in the security management of the enterprise.

The IA/CND solution must address this business need by providing data collection, data reduction and event correlation function across leading firewall, VPN, IDS and Server platforms. The goal is to have security administrators and analysts focus on taking the necessary action to address the events of a critical nature and not be deluged by the non-critical events. The solution needs to uniquely identify threats by relying on a combination of signature and behavior based network traffic analysis. This will allow administrators responsible for IA/CND to detect new intrusion attacks that are yet to be identified by signature based IDS solutions or individual system management platforms.

**Presenter:**

**Kaustubh (Kaus) Phaltankar**, Founder, Chairman and CEO, ViewTrust Technology

Kaus brings more than 10 years of Internet, network engineering, technical sales and management experience from leading corporations including CLEAN, MCI, Citicorp and Hewlett Packard. Kaus holds a Masters of Science degree in Telecommunications & Computers from George Washington University in Washington, DC, a Bachelors of Engineering degree in Electronics and is a graduate of the Leadership Development Program at the Center for Creative Leadership in Greensboro, N.C.

Kaus is also a published author of a 'how-to' guidebook "Practicle guide for Implementing Secure Intranets and Extranets", published by Artech House with a forward from Dr. Vint Cerf, also known as the 'Father of the Internet'.

Kaus holds patent in the area of "High Resiliency Network Infrastructure".

Kaus is a frequent industry speaker on security at industry events and organizations such as 'Brookings Institution'.

ViewTrust Technology Inc., his current company is a leading provider of 'Active Threat Management' and 'Compliance Reporting Solution' for Managed Service Providers and Enterprise customers worldwide. ViewTrust empowers security-conscious organizations to focus on their core business by optimizing their existing investment in network security infrastructure. The Company has two fully-developed and tested proprietary products, ThreatVision™ and LogVision™ and is currently delivering both products.

The patent-pending ThreatVision product delivers highly scalable, flexible, efficient, out-of-the-box solution for obtaining enterprise-wide view of the security through a single management console. ThreatVision provides solution across multiple vendors and multiple-platforms for firewalls, Virtual Private Network (VPN) gateways, Intrusion Detection Systems (IDS), Routers, Switches and Windows or UNIX server platforms. The LogVision product provides centralized log analysis and reporting solution for CheckPoint and Cisco platforms.

Prior to founding ViewTrust, Kaus was the Founder, Chairman and CEO of CLEAN, a global Managed Security Service provider with Fortune 500 customers in Americas, Europe and Asia. CLEAN provided Managed Firewall, VPN and Intrusion Detection solution to medium to large enterprises.

Prior to CLEAN, Kaus was the chief engineer and chief architect for MCI's Internet Solutions Center. He was also an executive staff member of MCI's Web hosting architecture division. In this capacity, Kaus designed and implemented numerous Internet, intranet and extranet solutions for MCI's Fortune 100 customers.