APT PROTECTION | SIEM/SOC | NETWORK FORENSICS | INCIDENT FORENSICS | DATA BREACH DETECTION

PineApp CyBoWall

CyBoWall is an on-premises, non-intrusive, agentless solution that leverages deep packet inspection (DPI), honeypots and network scanner technology to analyze related network traffic - including Security Information and Event Management.

Comprehensive Security for Advanced Persistent Threats

Provides a single platform that internally interacts with multiple detection vectors, active scanning of traffic, network traps, active and ongoing vulnerability detection of host and network's services.

Abnormal Behavior

Algorithms identify normal and abnormal entity behavior and will detect anomalous logins and abnormal resource access. Creates dynamic behavioral profiles for each entity in the organization and builds an Organizational Security Graph

Near Real-Time Detection & Prevention

DPI and information from other sources to identify advanced attacks such as Golden Ticket, remote execution on the domain controllers, Skeleton Key malware, honey token activities and more.

SOLUTION AT A GLANCE

CyBoWall provides a simple and fast way to understand what is happening within an organization's network by identifying and blocking suspicious users and device activity. CyBoWall provides clear and relevant threat information on a simple attack timeline.

Low False Alerts

CyBoWall consists of several different engines working together. The mitigation (policy) engine is the "brain" of the system, the commander engine that receives data from the different engines, can crosscheck and fuse the information it gets from the different engines, and decide whether and what kind of mitigation activity to operate.

Network Sensor

The network sensor will identify any abnormal and suspicious activity of a user or a service, based on a captured traffic activity.

Network Scanner

As opposed to the network sensor that receives online traffic, the network scanner is actively looking for information that is contained in the organization's computers and servers at all times - offline. The network scanner uses deep packet inspection (DPI), information from log files, DLLs, and information from SIEM systems, in order to detect advanced threats.

Network Traps

CyBoWall allows for the utilization of a honeypot module that includes the creation of multiple virtual hosts on the CyBoWall system. The honeypot can be created under detailed specifications including defining the operating systems and are set to run predefined services (web server, FTP, normal end points, windows share) that will get an interested intruder.

Two-way Syslog server support for SIEM integration.

The capability to communicate with SIEM solutions is very important since it gives CyBoWall access to logs of devices that it does not have direct communication with. CyBoWall supports CEF and LEEF messages for additional SIEM server integration.

SOLUTION HIGHLIGHTS

Real Time, Total Security

Internally interacts with multiple detection vectors, active scanning of traffic, network traps, active and ongoing vulnerability detection of host and network's services.

Proactive Resolution

System can react immediately to suspicious behavior before the network is compromised

Deep Reporting Capabilities

Data parser will collect and analyze across protocols: SMTP, HTTP, HTTPS, DNS, FTP, POP3, IMAP, RDP, VNC, TOR, IRC, ARP, NTP, SSH, ICMP, P2P, ICMP, SIP, MAPI

PineApp

Since 2002 PineApp has been a leader in the field of information security and cybersecurity. With a global installation base spanning over 50 countries, PineApp offers innovative solutions in network security for SMTP, HTTP and DNS protocols. PineApp Solutions for Service Providers, Enterprise, and National Security - Our Innovation is Your Security.

PineApp, Ltd. | p. +1.718.213.4803 | e. info@pineapp.com | www.PineApp.com