Hexis Cyber Solutions

HawkEye | G: The Active Defense Grid

Benefits

- Automated remediation of full cyber threat spectrum from botnets and malware to advanced persistent threat
- Drastically shortens the time of threat removal by deploying a full-suite of “active defense” detection and countermeasures
- Reduces false positives through the use of digital diagnostic techniques
- Continuously updates detection analytics, response vectors and threat feeds
- Autonomous or semi-autonomous threat remediation based on user defined policies
- Continuous graphical network security awareness
- Built with its own high-performance event data warehouse

Actively Detect, Engage + Remove Network Threats

Malicious cyber threats get past even the most advanced perimeter defenses. Once inside the network, they can exfiltrate intellectual property, take control of sensitive processes, and proliferate. The dire need of today’s network owners is to quickly detect and then “actively defend” against the spectrum of threats from botnets and malware to advanced persistent threats through the use of automated countermeasures that remove cyber threats at digital speeds. Hexis Cyber Solutions’ HawkEye G addresses these cyber security needs.

HawkEye G is an active defense disruptive technology that detects, investigates, remediates and removes cyber threats within the network before they can compromise intellectual property or cause process disruption. HawkEye G brings speed, automation and accuracy to threat response and leverages Hexis Cyber Solutions’ unique appreciation for malicious tradecraft.

Detect

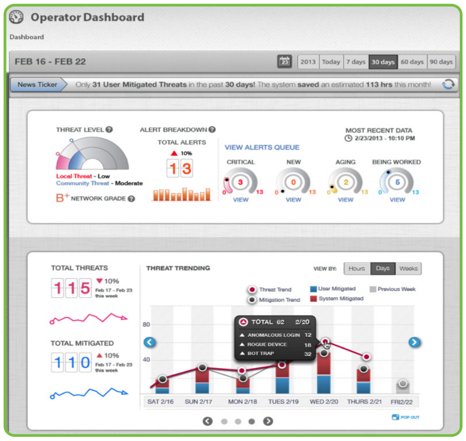
- Integrate existing infrastructure enterprise activity and threat intelligence into one comprehensive sensor system
- Correlate pattern deviations, uncommon communications and suspicious configuration changes, anomalous resource use, authentications and logins
- Using the embedded high performance event data warehouse and the most advanced analytics in existence – detects in seconds and minutes what used to be virtually undetectable

Engage

- Automatically and semi-automaticallyprosecute the threat
- Gather forensic intelligence to determine malware intent and target malware for remediation

Remove

- Launch a spectrum of cyber counter-measures against the internal threat
- Eradicate the threats in minutes and seconds
- Isolate and clean the hosts and network
- Share early warning threat intelligence
- Profile and baseline behaviors for future protection



Operator Dashboard

Dashboard

FEB 16 - FEB 22

News Ticker: Only 31 User Mitigated Threats in the past 30 days! The system saved an estimated 113 hrs this month!

Why HawkEye G is in a Class by Itself

HawkEye G was designed using knowledge gained from the most advanced intelligence community applications and by analysts that understand the tools, techniques, and procedures of the attacker.

It operates at big data scale to discover and interpret subtle behaviors in enterprise activity and identify threats that have already penetrated the perimeter.

HawkEye G automatically deploys countermeasures consistent with network policies in as automated manner as preferred by the user.

Hexis Cyber Solutions, a wholly-owned subsidiary of The KEYW Holding Corporation
7740 Milestone Parkway, Suite 400 | Hanover, MD 21076 | info@hexiscyber.com | 443.733.1900

Product Overview

HawkEye G Core

Central Servers and Storage

- 2 servers
- 1 SAN
- 1 switch

One Core per installation
7U total
3.5kW at peak

Processor/Storage

Extension Servers and Storage

- 1 server
- 1 SAN

One per 15,000 entities
4U total
1.5kW at peak

Deep Packet Inspector

Network Traffic Monitor

- 1 server
- 1 bypass module

One per gateway
2U total
1.5kW at peak

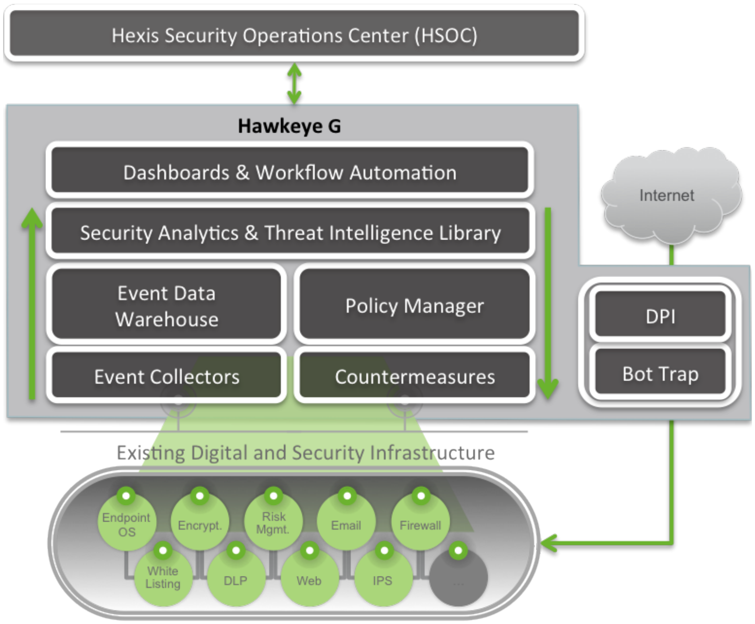
Partition Manager

Data Collection and
Countermeasure Extension

- 1 server

One per network segment
2U total
1kW at peak

HawkEye G Architecture


Hexis Security Operations Center (HSOC)
Hawkeye G
Dashboards & Workflow Automation
Security Analytics & Threat Intelligence Library
Event Data Warehouse
Policy Manager
Event Collectors
Countermeasures
Internet
DPI
Bot Trap
Existing Digital and Security Infrastructure
Endpoint OS
Encrypt.
Risk Mgmt.
Email
Firewall
White Listing
DLP
Web
IPS

The HawkEye G architecture comprises several integrated components that together enable advanced threat protection:

Event Collectors bring in data generated by the existing network infrastructure and loads the data into an Event Data Warehouse.

Event Data Warehouse, which is patented and purpose built, makes over half a year of infrastructure data immediately available to the Security Analytics & Intelligence Library, effectively turning infrastructure log data, user and host profiles, security devices, net flows and authentications into one sensor system.

Security Analytics and Intelligence Library is a state of the art portfolio of threat detection techniques that mine the Event Data Warehouse for behaviors that could indicate the presence of an advanced threat in the network.

Policy Manager is a collection of user defined rules that control the behavior of the Countermeasure Manager. Policy can be set that enables the Countermeasure Manager to run in a fully autonomous or semi-autonomous mode.

Countermeasure Manager controls the arsenal of active defense tools designed to mitigate and remediate threats discovered in the enterprise. Countermeasures include the elimination of malicious software, isolation of infected or rogue devices, the expiration of compromised credentials, and more.

Dashboards & Workflow Automation tools provides security awareness to the HawkEye G user by displaying expandable dashboards representing status, open actions, etc. Anonymized threat data is forwarded to the Hexis Security Operations Center.

Hexis Security Operations Center (HSOC) provides software and analytics updates, external threat feeds, and monitors and shares the community threat environment.

Deep Packet Inspector and **Bot Trap** will utilize real-time malware detection techniques based on threat feed information from the HSOC at the Internet gateways.

Hexis
CYBER SOLUTIONS

KEYW

Hexis Cyber Solutions, a wholly-owned subsidiary of The KEYW Holding Corporation
7740 Milestone Parkway, Suite 400 | Hanover, MD 21076 | info@hexiscyber.com | 443.733.1900