Executive Summary

Since the beginning of contemporary network security, the practice of information technology (IT) security has been a cat-and-mouse game between the offense (hackers) and the defense (security). Today, the offense clearly has the edge in this game as indicated by the increased frequency, sophistication, and success rate of cyber-attacks. According to the 2013 Verizon Data Breach Investigations Report, in the year 2012 alone there were an excess of 44 million quantifiable compromised records, 621 confirmed data disclosures and 47,000 reported security events. This number continues to rise and add to the over 1.1 billion security incidents reported within the last decade�. The hacker community’s practice of open sharing of source code for evolving exploitation techniques means that defense is likely to fall further and further behind as lower-end actors reuse advanced capabilities while higher-end actors continue to develop next-generation techniques. Due to the increasing creativity of malicious actors, the methods necessary to identify and remediate the growing number of security incidents need to evolve, too, and include techniques involving big data approaches, heuristics, active defense countermeasures, and community threat sharing.

The current threat landscape portrays an exponential increase in threats as they evolve over time. Hacker culture, whether independent or state-sponsored, embraces technology faster than businesses, resulting in risk growth over time and causing an enormous gap between security solutions and the threat. Eventually, organizations will reach a breaking point where they are no longer able to allocate resources to adjust to the rise in anomalous activity; this type of resource allocation would only be realistic in the government and intelligence community, and even then it is becoming harder to maintain pace with the threat culture.

Hexis Cyber Solutions’ HawkEye G is designed to combat the unconventional techniques utilized in advanced infiltrations by leading the charge in automated active defense mechanisms. It will detect, engage, and remove advanced persistent threats (APTs) attempting to compromise the enterprise. The core design leverages a powerful big data security analytics platform, an enterprise pervasive policy engine, a countermeasure manager, which serves as an arsenal that eliminates threats and cyber malware, and real-time threat intelligence updates. This capability is coupled with a robust and intuitive user interface that enables enterprise-wide visibility with total control for remediation. HawkEye G is the only proactive cyber defense solution designed to provide true start-to-finish security, from the investigation and detection to the automated isolation and removal of the threat. Next-generation threats, with their self-mutation capabilities, are not unlike viruses. The threat and threat defense landscapes remain complex layered environments where the capabilities of the most advanced threats are shared with less-sophisticated actors, creating a knowledge curve which puts pressure on traditional cyber security methods. Hexis Cyber Solutions Security Operations Center (HSOC) is an internet-based threat intelligence command center that is responsible for developing and distributing the latest threat defeat tactics to each enterprise’s HawkEye G instance. This includes the latest threat defeat analytics and threat intelligence sourced from the greater HawkEye G community. With the ability to share information about new threats from within the HawkEye G community, we benefit in the same way that the hacker community does, increasing our collective knowledge and awareness of threats as they are investigated, reported, and removed. The complex process of dynamically refining heuristics as the system learns is designed to combat that self-mutation capability and counter the threat head-on before a massive compromise ensues. The more intelligence gathered and shared via the HSOC to the HawkEye G community, the more exponentially advanced the analytics and remediation techniques become, resulting in an
automated process to engage, investigate, and effectively remove the threat.

**Traditional Methods of Enterprise Security**

Malicious actors expect, and take advantage of, traditional methods of enterprise security that rely solely on “known” signatures. Coupling that with the malicious actors’ culture of embracing the challenge of hacking and sharing techniques with others in their community makes it difficult for today’s end-point solutions to keep pace with the resulting exponential increase in threats.

Currently, threat detection is based primarily on signature identification, and the identification of a new signature typically takes days, weeks, or even months to be discovered. Within that time interval, a data breach has most likely already compromised the network and the data exfiltration stage has completed, leaving the enterprise still vulnerable to the loss of other valuable intellectual property and data. The attacker’s goal in breaching the enterprise is to steal valuable information and ensure a capability that enables future data exfiltration. The resulting cost for the organization to rebound from the exfiltration of intellectual property and valuable proprietary information becomes exorbitant. Current point solutions, which leverage signature-based detection, are intrinsically unable to catch threats in time to prevent costly losses.

Figure 2 illustrates signature-based threat detection which addresses only a small portion of the threat landscape, commonly known signature-based malicious code such as viruses, bots, worms, and trojans. Today’s solutions are partially able to perform intrusion detection on known threats in remote control sites, but the attacker still has an incredible advantage with their ability to discover, exploit, and share vulnerabilities with the hacker community. Furthermore, today’s enterprise solutions fail to consider anomalous actions that are not code-based, such as resource abuse and human data exfiltration (e.g., insider threat) which can only be detected using behavior-based analytics. As threats exponentially increase, the signature-based detection solutions’ capabilities still only mature linearly and are becoming increasingly inconsequential to closing the risk gap.

The newest generation of cyber defense strategy combines signature-based end point solutions and perimeter defense systems such as firewalls and intrusion detection systems with a big data analytics platform that performs security analytic algorithms on network data logs, flows, and events. These solutions reduce the reliance on *a priori* knowledge and incorporate analytics designed to understand and detect new threats.

The major weakness of this “big data” analytics solution is that the algorithms used are only as strong as the knowledge used to develop them. When the analytical developer does not understand fully the design of advanced persistent threats, their implemented algorithms are relatively naïve, offering little more than traditional signature-based point solutions. Moreover, behavior-based anomalous activity is not addressed with big data analytics. (See Figure 3.)
As the threat landscape evolves, anticipation of next-generation threat implementation tactics will be necessary to combat malicious adversaries. Malicious actors will always find a way to manipulate the system by changing their tactics and sharing their code and successes, precipitating the number of threats to increase exponentially. Without a heuristic capability to investigate and retain what is learned about anomalous security events, the system will never learn to block new and increasingly complex events that could potentially cripple an enterprise. Without policy-driven countermeasure development to decelerate threat proliferation, the gap between risk and threat will never be closed.

**HawkEye G Approach to Enterprise Security: Active Defense**

Signature-based defense is no longer a sufficient standard for cyber security. Active defense is the new standard, adding inference, understanding, and mitigation in an anticipatory and automated fashion. HawkEye G, the only active defense capability available, observes network behavior and utilizes event reflection to identify and understand threats living within the enterprise. Methodically, it engages isolative operations while concurrently performing investigatory measures to learn more about a threat. Proactively, its automated progressive threat mitigation strategy, which is based on its comprehensive internal and enterprise perimeter awareness, removes the threat.

In order to fill the gap left by big data analytics solutions it is essential to provide better algorithms, automated remediation, and policy adjustments. The algorithms address the user base, the networks, the hosts, and event data logs. This facilitates a robust approach to anomalous event identification. By implementing CyberCon levels of enterprise network permissiveness, HawkEye G will communicate directly with network operators to further limit exposure to threats (as indicated by the green dotted end of the threat curve in Figure 4).

The automated remediation and policy adjustments fill in the last piece of the puzzle to get closer to leveling out the threat evolution rate and the detection and mitigation rate for next-generation defense solutions.

**The Cyber Threat Taxonomy**

HawkEye G is devoted to understanding all aspects of cyber threats to the enterprise. This requires a profound appreciation for the taxonomy of malicious actors that infiltrate enterprises. The Defense Science Board six-tier, three-stage cyber-threat taxonomy illustrates different categories of motives and methods of exploit from low to high intensity. Building upon this foundation, Hexis Cyber Solutions further evolved a more detailed taxonomy which includes a full spectrum of offenses and defenses, target types, and level of involvement of adversaries (see Figure 5). HawkEye G was developed utilizing the philosophy of a graded threat matrix, making it the first solution focused on a hierarchical taxonomy.
The HawkEye G Solution

The HawkEye G solution encompasses many critical components for addressing detection, engagement, and removal of threats. The Enterprise Cyber Operations Dashboard provides immediate visibility into the detection, location, activity, and status of malware that has been identified for possible automated remediation including the ability to manually undo certain automated actions. The HSOC dashboard provides Hexis Cyber Solutions the ability to monitor the component health of each HawkEye G. Communication between each HawkEye G deployment and the HSOC occurs frequently over secure SSL-encrypted communications and client data is obfuscated in analysis reports. These reports serve as intelligence data so that the HSOC may maintain its heightened awareness of the threat and threat defense landscapes at each deployment while continuing to validate and publish new threat defeat strategies and tactics.

---

### Hexis Cyber Solutions’ Cyber Threat Taxonomy: The Spectrum of Attacks and Defences

<table>
<thead>
<tr>
<th>Attacks</th>
<th>High-caliber human and machine assaults</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unique, multi-stage exploits</td>
</tr>
<tr>
<td></td>
<td>Cryptographic mechanisms, backdoors</td>
</tr>
<tr>
<td></td>
<td>Malicious code, root kits, command-and-control architecture</td>
</tr>
<tr>
<td></td>
<td>Zero Day exploits, botnets, eavesdropping, search poisoning, DDoS</td>
</tr>
<tr>
<td>Phishing, malware, DNS attacks, trojan horses</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defenses</th>
<th>Offensive tactics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Automated countermeasures</td>
</tr>
<tr>
<td></td>
<td>Security information and event management</td>
</tr>
<tr>
<td></td>
<td>Infrastructure / community enforcement</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Targets</th>
<th>Consumer</th>
<th>Small Business</th>
<th>Medium Business</th>
<th>Enterprises, Public Figure</th>
<th>Global 2000, Governments, Critical Infrastructure</th>
<th>Nations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Individual data, inconvenience</td>
<td>Bulk data breach, loss of customer confidence</td>
<td>Business interruption, loss of brand or stock value</td>
<td>Political exposure, community chaos</td>
<td>Service outage, business collapse, loss of intellectual property</td>
<td>Espionage and national security breaches, death, destruction</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Adversaries</th>
<th>Hackers</th>
<th>Organized Criminals</th>
<th>APT Agents</th>
<th>Targeted Actors</th>
<th>Hostile Nations</th>
<th>Full Spectrum Attackers</th>
</tr>
</thead>
</table>

---

Figure 5. Hexis Cyber Solutions Cyber Threat Taxonomy serves as the foundation of HawkEye G’s policy-driven analytics and countermeasure constructs.

Figure 6. HawkEye G Architecture
DETECT Using Near-Real Time Methods

HawkEye G threat detection goes beyond typical network perimeter security with the ability to not only detect known threat types in real-time using deep packet inspection technology, but also to identify them using historical event data and a robust security analytics platform. As event data logs are captured and investigated by HawkEye AP: The Analytics Platform and compared to the known baseline activity of the enterprise, anomalous activity and devices becomes known to the system based on event ID, time signatures, MAC addresses, user account information, or computer or workstation information. What makes HawkEye G unique is the synergy between HawkEye AP and the deep packet inspection/manipulation (DPI/DPM) component. The DPI/DPM technology enables recognition of communications to known malicious domains and URLs and redirects suspected bot traffic to a Bot Trap for remediation, while HawkEye AP identifies anomalous events based on time, user account and workstation information which deviates from known and accepted enterprise behavior. Devices detected on the network are compared to a MAC whitelist which allows approved devices access to the network but flags unknown devices for further investigation. If an anomaly is detected immediately by the DPI component, immediate isolation and removal of a threat occurs via the Bot Trap. The Bot Trap component is where network-oriented malware is sent if detected at the network perimeter. The goal is to eliminate network oriented malware before it has the ability to infiltrate the enterprise.

HawkEye AP is a unique high-performance event data warehouse solution which serves as the database critical to collection and analysis for the HawkEye G solution. HawkEye AP leverages a patented columnar database uniquely designed for time-stamped structured data to be correlated and analyzed, either in real time or over months or even years. The solution runs on a platform employing massive parallel processing and commodity hardware and storage for enhanced load and query throughput, very high data compression (up to 40:1 compared to relational databases) and extremely large data retention (up to petabytes a year). It provides the ability to correlate events across multiple data sources and systems, either in real-time or on a historical basis. HawkEye G enhances network security intelligence coverage by adding a portfolio of analytics on top of the event data warehouse. At this layer, data logs, net flows, and event reflections are analyzed with our unique algorithms to generate anomaly triggers for the rules engine.

The DPI portion of this component allows for blocking or redirection of outgoing malicious DNS requests at first detection. While this method works well for known threats, new malicious designs can easily gain access. This requires different techniques, implemented in HawkEye G, which can recognize malware in motion, resource inconsistencies, and a plethora of other anomalies that people experienced in malware craft can build algorithms to detect. HawkEye G distinguishes itself from competitors by performing these actions with a low cost appliance with very low latency.

ENGAGE with HawkEye Analytics Platform, Analytics, and Policy

Once an unknown threat is detected within the enterprise after passing through the DPI/DPM engine but detected by the HawkEye AP, the anomaly is investigated using active engagement to gather more intelligence. The Enterprise Cyber Operations dashboard provides a user-friendly interface allowing analysts and administrators alike to view network activity, investigate any findings, and ultimately remediate determined threats based on gathered intelligence.

The Enterprise Cyber Operations Dashboard, a rich analytics interface, enables security personnel to manage policy triggers and countermeasure rules to best fit the needs of the enterprise. Permissions can be assigned based on level of involvement with the HawkEye G from observer to administrator level. The dashboard also provides asset tracking, a list of active accounts and devices, and the number of incidents by day, week, month, and to-date. It also allows the user to perform heuristic operations, manually or automatically, labeled as gather more info capabilities such as walk directories, list processes, and walk registry. The activity of all of these actions and the resultant intelligence are visualized using the network operations dashboard.

When HawkEye G is engaged in the investigation of a threat that has breached the perimeter of the network, it digests information gained from the heuristics of gather more info processes and uses that learned intelligence for agile policy development. There are three main goals of heuristic analytics for agile policy development and implementation:

1) Provide complete enterprise visibility and insight.

2) Perform enterprise analysis and reporting for policy-based countermeasure development.
3) Recognize baseline pattern and deviations.

HawkEye G analytics provide an assessment of the enterprise ecosystem and learns not only to mitigate known anomalous events, but also predict and recognize unknown events based on deviations from those known events. This heuristic approach to threat classification and determination of appropriate manual or automatic actions based on threat categorization is pertinent for combating diverse and dynamic threats.

**REMOVE utilizing CMM Rules and the Analytics Interface**

After further intelligence is gathered and the anomaly is categorized, it is time to take action to remediate the threat to prevent damage to the enterprise. The Counter Measure Manager (CMM) rules and subsequent countermeasures are hierarchical and reflect enterprise policy derived from the Cyber Threat Taxonomy. The CMM relies on policy-based triggers to dictate perceived level of threat based on the intelligence gathered during the engagement phase. It first checks the enterprise’s policy to determine what automated mitigation techniques are permissible for this network entity. Once the policy is checked, the rules engine will engage the CMM to perform a sequence of escalating mitigation strategies until the threat is removed or rendered harmless. This provides ultimate flexibility in countermeasure management and allows for the use of pre-loaded policies in conjunction with organization-initiated policies to give the system the ability to respond rapidly and mitigate the impact of threats using analytics and security workflow automation capabilities.

Automatic or manual countermeasures based on investigative analytics include disabling the network interface, expiring user credentials and blacklisting the MAC address of a device by adding it to a threat list. A company may want a human in the decision loop for critical networks services such as a SCADA device or trading platform whereas with insider resource abuse they may want to automatically disable the port and expire user account credentials in near-real time, which is why the ability to perform these operations manually or automatically is imperative. The CMM also incorporates Hexis Cyber Solutions’ offense technologies by performing an attack against the infected entity such as disabling network functionality, “killing a process,” cleaning the infected host, and prohibiting a threat from executing.

**Hexis Security Operations Center (HSOC)**

The HSOC performs maintenance operations and analyzes component health for each of the HawkEye G deployments. It receives and analyzes obfuscated reports from all client sites for trend analysis and emergent attack vector identification. The reports are obfuscated in order to anonymize data and focus on the attack vector characteristics rather than enterprise information. It also houses new behavioral identifiers, mitigation techniques developed by Hexis Cyber Solutions’ Offensive Technology Team (OTT), and software updates for the rules engine and CMM. The HawkEye G platform connects to the HSOC and fetches updates to the threat database and components. It also provides a means to exercise the local HawkEye G system to verify component health, performance and coverage. Lastly, it provides a place for the experts on Hexis Cyber Solutions’ Advanced Persistent Threat Team (APT Team) to aid in the analysis of new attacks without exposure to the client base.

**Sample Use Cases**

Below are seven exemplar HawkEye G use cases:

**Internal Bot**

If an attacker is attempting to breach the enterprise, they may attempt to insert a bot within the network that will wreak havoc on the organization’s ecosystem. The internal bot use-case addresses security at the perimeter of the enterprise. The DPI engine identifies network-oriented malware attempting to infiltrate the network and the DPM uses packet redirection to send the malware to the Bot Trap, where several techniques will be used to attempt near real-time remediation of the compromised host. If the Bot Trap cannot remediate the threat, HawkEye G will activate its countermeasure manager to use more sophisticated techniques to remove the malicious software from the infected device.

**Resource Abuse**

In some cases, the bot signature will be unknown to the DPI/DPM system and the bot will be able to establish a connection with its external controller, creating a successful breach of the perimeter defense. However, as it moves through the network to its target of interest, the malicious software will likely present itself as an abuse of a network resource (user credential or file system access as examples). As it moves through the network, the bot leaves behind a trail of “digital exhaust” that HawkEye G’s detection algorithms are designed to detect. When an anomalous event is detected, *gather more info* is triggered.
to confirm if the event is associated with an attack or just a spurious network event. Should the event be deemed a threat, HawkEye G would then follow a policy-driven remediation approach to remove the threat from the enterprise.

**Rogue Network Device**

An unrecognized device that attempts to penetrate the network can be hazardous. It can either be a wired or wireless host. With the Enterprise Cyber Operations Dashboard, the user is able to keep track of devices that are permitted access to the network. If a device is detected that is not a permitted device, HawkEye G will disable the network port and remove the device from the network to prevent malware from transferring from the device to the network or prevent access to network resources.

**Distributed Active Defense**

The distributed active defense use case is the main use case for the central command of the HSOC. The HSOC is able to analyze reports and trends imported from the HawkEye G platform and use this intelligence to update signatures, countermeasures and configurations not only for that HawkEye G, but for all HawkEye G clients. This facilitates the intelligence sharing between users in the HawkEye G community and allows for up-to-date threat information dissemination throughout the community.

**Risk, Compliance, and Configuration Analysis**

Risk, compliance and configuration analysis is beneficial for greater clarity regarding the stability of the organization’s environment. HawkEye G will analyze compliance posture versus required organization policy. In addition it will identify risky or dangerous configurations weighted by potential threat vectors and properly prioritize and proactively remediate these configurations automatically.

**Vulnerability Assessment**

According to a defined and prioritized routine, HawkEye G will gather vulnerability information from assets within the network through active scans. Data collected through the scan can then be compared to accepted vulnerability databases. Deviations from the database are noted and prioritized based on risk exposure. Based on policy, HawkEye G can then recommend or take automated remediation actions to correct the issue. If remediation is not possible and the risk is high enough, HawkEye G could disable connectivity through the network interface.

**Asset and Network Mapping and Awareness**

A useful function for the organization is asset and network mapping and awareness. HawkEye G collects data from net flows, logs, and scans, analyzes the data and synthesizes it into a logical representation of the network environment. Current representations can then be compared to past representations and deviations are highlighted and reported across various time boundaries. If desired, representation and deviations are forwarded for follow-up and analysis.

**Summary**

HawkEye G is a dynamic active defense system designed to leverage existing security assets while providing advanced cyber security analytics and automated countermeasure techniques. The combination of the traditional signature-based and new behavior-based heuristics leads to heightened awareness of standard network activity and deviations that could indicate a potentially disastrous situation. Understanding the full threat and defense landscape is crucial for cyber security mitigation and the HawkEye G team has invested the time and resources into developing that holistic solution.

HawkEye G is a single deployable unit that easily integrates with an enterprise’s current IT investment. Reduced human workload due to accelerated mitigation of network security events and automated implementation of policy means that human capital can be redistributed to focus on the most complex issues. Furthermore, HawkEye G’s automated capability minimizes error, increasing the consistency and accuracy of detecting anomalies. Organizations will now be able to align staff capacity to evaluating surfaced network compromises rather than to threat discovery and investigation.

The vastness of the potential threat landscape affects everyone, from small businesses to large, and any vertical market that uses networked technology to store information. The malicious actor does not differentiate between the type and size of business; they are after intellectual property, strategic information and assets that could potentially affect the functionality and stability of an organization.

HawkEye G’s unique proactive defense posture makes malicious actors’ tactics costly and more risky than
traditional cyber solutions, while decreasing the total number of successful breaches. As they continue to develop new techniques for breaching enterprises, the countermeasures and remediation will adjust and evolve, ultimately making the time and energy spent by malicious actors on infiltrating the network futile.

At some point along the threat continuum, there is a divide between threats solvable by enterprise IT specialists and those that have been trained in a government capacity in both defensive and offensive tactics. The HawkEye G team consists of specialists with experience in both disciplines, providing necessary expertise for closing that risk gap using automated defensive and offensive techniques. Using defined policy, the HawkEye G solution engages for further investigation of the threat and deploys countermeasures based on that investigation. The invocation of automated policy forces malicious actors to stretch their resources in attempting to discover and exploit new vulnerabilities in the network and causing them to use more risky approaches. This force against the threats stifles its growth and as HawkEye G has increased success in investigating and removing threats, intersects with the threat growth and closes the risk gap.

About Hexis Cyber Solutions

Hexis Cyber Solutions, Inc., a wholly-owned subsidiary of The KEYW Holding Corporation (NASDAQ: KEYW) based in Hanover, Maryland, provides complete cybersecurity solutions for commercial companies, and government agencies.

Our mission is to ensure that business IT infrastructure is equipped with tools and capabilities to detect, engage, and remove both external and internal cyber threats. Cyber terrorists, organized crime, and foreign governments focus tremendous effort on commercial, government, and military interests as their prime targets. Hexis Cyber Solutions’ HawkEye family of products offer active, multi-disciplined approaches to achieve a higher standard of cybersecurity that is based on our expertise supporting advanced cybersecurity missions within the US, ensuring your business or organization operates at its maximum potential. For more information contact Hexis Cyber Solutions, 7740 Milestone Parkway, Suite 400, Hanover, Maryland 21076; Phone 443-733-1900; Fax 443-733-1901; E-mail info@hexiscyber.com; or on the Web at www.hexiscyber.com.