LOOKINGGLASS

Addressing the Cyber Kill Chain: Full Gartner Research Report And LookingGlass Perspectives

Issue 1

Gartner

Welcome

The ever-changing threat landscape requires us to evolve our operational practices to a more proactive cadence. As the defender, we must actively search for the telltale signs of compromise within our organization and help drive efficiency and effectiveness into our operations staff by providing them with timely, accurate and relevant information. LookingGlass has partnered with Gartner to identify methods to help move your security organization to a more informed state of proactive security and risk operations.

Gartner's Research Note *"Addressing the Cyber Kill Chain"* assembles insight from proven research on how an attack lifecycle is executed and how throughout that lifecycle there is opportunity to detect, prevent and mitigate the attack.

LookingGlass is a next-generation threat centric security company that is committed to helping your organization get on par with the attacker with critical threat information and intelligence and the ability to dynamically operationalize that intelligence to continually improve your security posture and reduce your risk. We are providing our customers with the critical information and technical capabilities to disrupt the attack lifecycle, effectively disrupting the Cyber Kill Chain.

I trust that you will find valuable insights and tools to help your organization achieve and maintain a strong security posture.

Sincerely,

Chris Coleman
CEO
LookingGlass Cyber Solution

Operationalizing Threat Intelligence for Dynamic Defense

While organization's have made significant investments in security, the frequency, sophistication and targeted nature of cyber attacks keeps security teams busy continuously evolving their defensive techniques and searching for better tools and ways to keep their intellectual property and digital assets secure.

How can security teams better stay ahead of threats? In these two reports, Gartner and LookingGlass Cyber Solutions have teamed up to provide perspectives and insights to help security teams do just that. Often times, a slight change in perspective or golden nugget of information creates an AhHa! moment that can help.

Compliments of LookingGlass, the complete Gartner research report ***Addressing the Cyber Kill Chain*** (CKC) starting on page 6 helps security teams understand how they can significantly increase the defensibility of their environment by catching and stopping threats at each phase of the kill chain. The report looks at how today's common security architectures are not addressing the entire CKC so attackers are continuing to be successful with advanced and targeted attacks.

It's one of our most often requested discussion topics so in this report, we will look at ways that threat intelligence can be used (or "operationalized") in a real world setting to improve security operations, add intelligence to the security infrastructure, and generally help organizations better manage business risk.

LookingGlass threat intelligence solutions help organizations improve their ability to prevent, detect and respond to threats by addressing them throughout the cyber threat lifecycle. Based upon our experience with some of the largest, most secure environments in the world plus a foundation of Internet Intelligence, LookingGlass solutions help organizations operationalize threat intelligence for dynamic defense across the entire CKC.

> ***"At the core, the real value of using threat intelligence is that it helps organizations understand and take action on threats that are prioritized and relevant to their specific organization in a proactive, efficient and effective way."***

Threat Data vs Threat Intelligence

Threat data is not that same as threat intelligence. Gartner's definition of threat intelligence is "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." Additionally, the technical and contextual information regarding existing or emerging threats from all available sources should be evaluated and analyzed for accuracy, timeliness, and relevancy, and implemented among an organization's tactical, operational, and strategic stakeholders.

The essential difference between data and intelligence is that threat intelligence adds context that creates a deeper understanding of the threat and relevancy to a particular organization or industry. For example:

- Threat Data: The 10,000+ new domain names created in the last 24 hours that are hosting malware, stealing credentials as part of a phishing campaign, or are an active Command and Control (C2) server

- Threat Intelligence: Identifying the 10 devices *on your network* that accessed one of those 10,000+ domain names in the last 24 hours

Business Value of Threat Intelligence

Threat data provides information. Threat intelligence enables enhanced visibility and actionability on the most important and urgent threats. It enables organizations to better address

risks and threats in a more proactive, effective and efficient manner. And, it improves the time to prevent, detect and respond to threats throughout the cyber threat lifecycle.

Using the example above, if you understood that one of those domain names was hosting malware actively targeting financial services firms like yours, you could proactively automate an alert or redirection to a safe domain (prevent), quickly discover the 10 devices that accessed one of those domains (detect), and automatically deploy rules to prevent further communications (respond).

Getting Started

Depending upon the resources, sophistication and maturity level of an organization's security operations, there are a range of threat intelligence choices to strengthen the overall security posture.

- Threat Data Feeds. Many companies start with threat data feeds which contain indicators or artifacts of potential threats.
- Threat Intelligence. As managing multiple data feeds becomes more cumbersome, many employ a threat intelligence platform to transform threat data into threat intelligence.
- Threat Mitigation. Here threat intelligence is integrated into the network infrastructure in an automated or systematic way.
- Threat Intelligence Services. Organizations may choose to augment some of their security operations with outside analysts and services such as with customized assessments of threats targeting their executives or supply chain.

Threat Intelligence Platforms

Once the volume of threat data being consumed gets large enough, many organizations look for a threat intelligence management platform to manage and get more value from the information.

For example, the LookingGlass threat intelligence platform looks at millions of elements (observables) of threat data every day. It brings over 140 data sources together (plus those of the client) into one platform where it ingests, aggregates, normalizes, enriches, analyzes, and prioritizes the data to create actionable threat intelligence that is relevant to the specific organization. Relevance is important as for example, threats impacting a financial institution are very different than those targeting a power plant. LookingGlass is the only company that layers this threat intelligence and context to the global Internet network topology through Internet Intelligence.

Internet Intelligence: Defense Starts Outside the Perimeter

Attacks are multi-phased often starting with the easiest gaps and vulnerabilities to gain access to the ultimate target in this interconnected and digital world. Understanding relationships across organizations and their Internet presence and connections provides deep, unique insights into understanding threats. A key functionality of the LookingGlass threat intelligence management platform is a foundation of global, real time Internet Intelligence.

The LookingGlass global Internet monitoring (GLIMR) network continuously monitors the global Internet and collects results from tens of millions of network probes daily. This provides a network centered view of the entire global Internet by looking at risks, threats, and activity on a broad scale as well as granularly down to its elements. GLIMR analyzes and then uses this Internet Intelligence to apply unique context to threats. This gives LookingGlass customers unparalleled insight into threats impacting their organization, industry, third party partners, and the Internet at large.

For example, one of the largest and most publicized breaches was of a major retailer in 2014. The source of the initial infiltration was reportedly one of their trusted third parties, a HVAC vendor. With Internet Intelligence, organizations can see what attacks are occurring to their public facing infrastructure as well as any organization including with trusted third party partners and other organizations in their industry. That information helps organizations better prevent, detect and respond to threats.

Integrating Threat Intelligence with Threat Mitigation

By integrating threat intelligence to automatically enable network defense solutions to take action on known bad threats or to alert network operations teams of high priority threats to investigate, security teams are able to prevent, detect and respond to threats faster.

For example, a malware outbreak or spear phishing attack often begins by establishing communication with its command and control (C2) server located on the Internet. The millions of elements (observables) of threat data that the LookingGlass threat intelligence platform looks at every day can be used to dynamically defend at the network layer. This intelligence can be used by solutions already in your infrastructure like a SIEM or by a threat intelligence optimized appliance such as DNS Defender, a protocol-specific firewall. DNS Defender automatically stops malware and provides real-time protection of an infrastructure by blocking or redirecting the malware DNS request to its C2 server which essentially prevents malware from receiving tasking information or malicious software from downloading. Protecting DNS is critically important to a strong security posture as the vast majority of malware uses DNS to operate.

The Result: Dynamic Threat Defense

Threat data feeds help organizations understand the general threats at large. By adding analysis, context, relevance, priority and timeliness, threat data turns into intelligence. With threat intelligence, companies understand the most important threats that may or are impacting their organization, their supply chain partners, and other companies in their industry to help them prevent, detect and respond to threats across the entire Cyber Kill Chain. The result is more efficient and effective security operations and a stronger security posture.

Source: LookingGlass Cyber Solutions

Research from Gartner:

Addressing the Cyber Kill Chain

The Cyber Kill Chain model describes how attackers use a common cycle of methods to compromise an organization. IT security leaders can use this research to align security programs to adversaries and improve their ability to predict, prevent, detect and respond to threats.

Key Challenges

- The current "prevention, prevention, prevention" approach to dealing with the threat landscape has failed to address advanced and targeted attacks. Organizations have not recognized the delta that their definition of "defeat" is different than an adversary's definition of "victory." The kill chain helps clarify this delta.
- IT security organizations have historical investments in a prevention-focused model that is out of balance with today's threat landscape.
- IT security organizations have largely not taken an architectural approach to dealing with adversaries; this is a key reason why attackers are continuing to be so successful.
- While the kill chain is easy to comprehend, resourcing to address it in the face of competitive business realities and constant microinnovation from adversaries is a key challenge.
- Common security architectures and compliance regimes are not prioritizing methods to address the entire Cyber Kill Chain.

Recommendations

- Understand the flow of the kill chain to better understand your adversary's methodology, and adjust your security architecture and processes to improve your security posture.
- Implement methods that help prevent or detect and respond to threats at each stage of the kill chain. This will significantly increase the defensibility of your environment, since attackers need to successfully execute all phases of the kill chain.
- Evaluate your existing environment with reference to the CKC to identify deficiencies and to implement supporting controls and processes that address the postbreach and exfiltration stages of the kill chain. Security organizations need to increase investment in this detection-and-response approach.
- Augment existing prevention methods with methods to detect, deny, disrupt and recover from the activity of your most credible threat actors.

Introduction

Targeted and more sophisticated attacks have escalated both in scale of damage and public visibility of occurrence in recent years. The importance of managing risk and the potential for financial and reputational damage resulting from a breach have increased in the era of digital business. The ease with which traditional security defenses were bypassed in some high-profile major incidents has left many organizations feeling powerless to defend themselves against these types of threats. This issue has become a concern at the executive boardroom level for some organizations.

The leading operational archetype in information security that is still widely practiced by a majority of organizations has a focus on the perimeter, often organized according to defense-in-depth principles and geared at prevention. This approach has created gaps in an organization's ability to detect and respond to threats, especially on the internal network. This decades-old approach has concentrated security resources on the most exposed assets and most common attack vectors, but it provides a false sense of security and represents a misallocation of resources when compared to today's threat landscape. This is further exacerbated as we extend our use of cloud and mobile computing. The perimeter-focused approach has created a situation that now favors adversaries that have a virtually unlimited amount of attack attempts, but only need to be successful once. Defenders, conversely, must be right every time.

This has led to a perception that, because there has been a successful malware infection or SQL injection attack against your organization, the adversary has won. The kill chain highlights that this is clearly not the case, because the adversary is victorious only once they can execute all phases of the Cyber Kill Chain (CKC)1 successfully. Rather than thinking that all is lost when an organization is initially compromised, you need to instead move to a mindset of: "They've yet to exfiltrate data or complete their final objective, and I still have time to prevent that final activity. Let's get started." Winning in information security today is not the prevention of all attacks; it is in concurrently doing a better job of prediction, prevention, detection and response.

The CKC is a reference model representing the stages of a compromise, mapped distinctively to activities that describe common methods adversaries use. It breaks an attack into seven stages or phases, each an opportunity for a breach to be detected, prevented or mitigated successfully. The attacker must successfully execute against each link in the chain, and this can provide opportunities for more effective defense in depth.

While the technologies we use and those that adversaries use against us have evolved significantly over the past two decades, the principles underpinning the CKC remain sound. If you understand the overall methodology of the attacker, then the specific techniques or motivations of threat actors are not so important. Whenever you can distill your security program down to simple principles versus complicated technologies and processes, it becomes fundamentally easier to understand, focus security investment and measure effectiveness.

Mapping your defense strategy to the CKC model shows how your organization can detect, deny, disrupt and recover throughout its phases. By aligning enterprise defenses to the same success criteria as those of adversaries, you can right size the prevention-centric approach that has dominated enterprise thinking and spending on IT security to date.

Analysis

Understand the Phases of the Cyber Kill Chain

The CKC is historically a well-understood concept in military circles that is now being applied to cybersecurity. Originally published by Lockheed Martin1 in 2011 as an intelligence-driven network defense process, it describes the phases that an adversary will take when targeting your environment, exfiltrating data and maintaining persistence in an organization. It is also similar to a majority of penetration testing methodologies still widely used and taught by various organizations; pragmatically, these are closely related and can often be referred to interchangeably.

The Cyber Kill Chain (see Figure 1) has seven stages:

1 **Reconnaissance** — This is anything that can be defined as identification, target selection, organization details, industry-vertical-legislative requirements, information on technology choices, social network activity or mailing lists. The adversary is essentially looking to answer these questions: "Which attack methods will work with the highest degree of success?" and of those, "Which are the easiest to execute in terms of our investment of resources?"

2 **Weaponization or Packaging** — This takes many forms: Web application exploitation, off-the-shelf or custom malware (meaning downloaded for reuse or purchased), compound document vulnerabilities (aka delivered in PDF, Office or other document formats) or watering hole attacks. These are generally prepared with opportunistic or very specific intelligence on a target.

3 **Delivery** — Transmission of the payload is either target-initiated (for example, a user browses to a malicious Web presence, leading to an exploit delivering malware, or they open a malicious PDF file) or attacker-initiated (SQL injection or network service compromise).

4 **Exploitation** — After delivery to the user, computer or device, the malicious payload will compromise the asset, thereby gaining a foothold in the environment. This is usually by exploiting a known vulnerability for which a patch has been made previously available. While zero-day exploitation does occur, in a majority of cases it is not necessary for adversaries to go to this expense.

5 **Installation** — This often takes the form of something that communicates actively with external parties. The application is usually stealthy in its operation, allowing persistence

or "dwell time" to be achieved. The adversary can then control this without alerting the organization — a common outcome.

6 **Command and Control** — In this phase, adversaries have control of assets within the target organization through methods of (often remote) control, such as DNS, Internet Control Message Protocol (ICMP), websites and social networks. This channel is how the adversary tells the controlled "asset" what to do next and what information to gather. The methods used to gather data under command include screen captures, key stroke monitoring, password cracking, gathering of sensitive content and documents, and network monitoring for credentials. Often a staging host is identified to which all internal data is copied, then compressed and/or encrypted and made ready for exfiltration.

7 **Actions on Targets** — This final phase covers how the adversary exfiltrates data and/or damages IT assets while concurrently dwell time in an organization. Then measures are taken to identify more targets, expand their footprint within an organization and — most critical of all — exfiltrate data. The CKC is then repeated iteratively.

One critical point with the CKC, however, is that it is a circular, and not a linear, construct. For example, once an adversary enters your environment, they start again with CKC with doing more reconnaissance, making lateral movement on the inside of your network. Also, keep in mind that while the methodology is the same, adversaries will use different methods for steps of the kill chain once inside, versus being outside the environment.

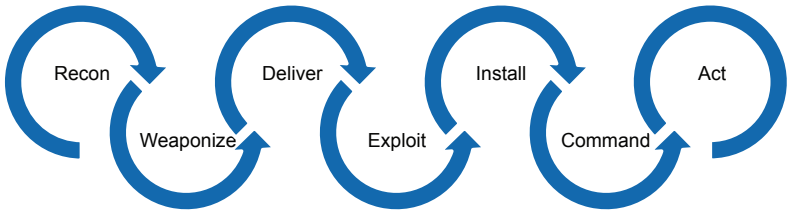
Focus on Why Attackers Are So Successful

Adversaries will continue to achieve their objective of successfully completing the kill chain, unless defenders implement an approach that takes into consideration how an attack is executed. This is difficult to achieve due to a number of factors. Applications have increased both in complexity and interconnectedness and code reuse. Application vulnerabilities abound because most software has not yet been developed using a security development life cycle, or subsequently tested independently for resiliency. People also remain a vector, via various forms of social engineering. Alas.

Although we tend to think of IT security in such terms as network security, host security and identity security, an "adversary centric" model is better-suited and is a more effective approach in today's threat landscape. Whether adversaries are motivated by geopolitical, activist or financial motives, they seek to fulfill specific goals of obtaining an organization's data.

While the traditional perimeter-centric security approach is not a panacea for all ills, it nevertheless remains essential as a solid foundation to an overall defensive strategy. However, in order to allocate and prioritize resources, the traditional approach should be extended with methods based on an understanding of the CKC.

FIGURE 1 Diagram of the Cyber Kill Chain



Source: Gartner (April 2016)

Address the Cyber Kill Chain at Each Phase

Instead of continuing to invest predominantly in defending an organization's perimeter, a more effective approach balances detection, response and a level of prediction throughout the entire environment.

A success rate of 100% for prevention against all steps of the attack chain is not attainable. This is also not necessary, as attackers must complete all phases to achieve their goals. Therefore, the key principles are planning for the prevention of privilege escalation, detecting postcompromise activity, stopping exfiltration of sensitive data and denying the attacker persistence in your environment.

At a high level, you must identify how you can detect, deny, disrupt and recover at each phase of the kill chain, as described in Table 1.

The sections that follow expand on the table above, giving specific examples and guidance that organizations can investigate. Adding more technology is often not required, but IT security leaders should take full advantage of improving the effectiveness of existing tools and processes already at their disposal.

Reconnaissance

This phase is often executed without knowledge of your organization. Approaches for this phase are:

- Perform regular external scanning and penetration testing to highlight what an adversary would find if and when your organization comes under scrutiny. This information can be used to remediate vulnerabilities, reducing the attack surface area.

Table 1. Technologies and Processes Applicable to Addressing the Kill Chain

Phase	Detect	Deny or Contain	Disrupt	Recover
Reconnaissance	Web analytics, Internet scanning activity reports, vulnerability scanning, external penetration testing, SIEM, DAST/SAST, threat intelligence, TIP	Firewall ACL, system and service hardening, network obfuscation, logical segmentation	Honeypot	SAST, DAST, hardening, patching
Weaponization	Sentiment analysis, vulnerability announcements, VA, threat intelligence			Hardening, patching
Delivery	User training, security analytics, network behavioral analysis, threat intelligence, NIPS, NGFW, WAF, DDoS, SSL inspection, TIP	SWG, NGIPS, ATD, TIP	EPP	Backup or EPP cleanup
Exploitation	EPP, NIPS, SIEM, WAF	EPP, NGIPS, ATD, WAF	NIPS, NGFW, EPP, ATD	Data restoration from backups
Installation	EPP, endpoint forensics or ETDR, sandboxing, FIM	EPP, MDM, IAM, endpoint containerization/app wrapping	EPP, HIPS, incident forensics tools, DNS filtering	Incident response, ETDR
Command and Control	NIPS, NBA, network forensics, SIEM, DNS security, TIP	IP/DNS reputation blocking, DLP, ATA	DNS redirect, threat intelligence on DNS, egress filtering, NIPS	Incident response, system restore
Action on Targets	Logging, SIEM, DLP, honeypot, TIP, DAP, UEBA	Egress filtering, SWG, trust zones, DLP	QoS, DNS, DLP, ATA	Incident response

Source: Gartner (April 2016)

- Use search engines to uncover cached content that can be used for exploits or that discloses information that would make it easier to target the environment.
- Utilize threat intelligence to look for activity (credentials and cards for sale, chatter about your organization) and intelligence (vulnerabilities being exploited, organizations being targeted) that are specifically related to your organization or industry vertical.
- Ensure that perimeter controls and Internet-facing services are aggressively enforcing the principle of least privilege, including service hardening.
- Use software application security testing (SAST) and security development life cycle (SDLC) principles to make sure that applications aren't leaking sensitive details and are processing untrusted input correctly.
- Use honeypots where adversary activity can be monitored for exploitation tactics.

Weaponization

This phase is often performed with no specific knowledge of the organization being targeted. However, organizations need to take proactive steps to:

- Keep abreast of newly disclosed vulnerabilities and have up-to-date data about which vulnerabilities have weaponized exploits available for them. With this information, you must prioritize patching them or implementing mitigating controls, such as intrusion prevention systems (IPSs), that can prevent and detect the exploitation of vulnerabilities.
- Investigate the use of threat intelligence providers that can add value with threat forecasting and advanced notification of impending activity against your organization. An example would be notification of a phishing template, or customizable toolkits designed to look identical to your organization's becoming available for sale. Another example is the identification of tools, techniques and processes (TTPs) that adversaries are commonly using against your organization.

Delivery

An array of traditional controls can assist greatly in denying access to your environment:

- Firewall to control traffic at the perimeter that includes advanced threat detection (ATD) such as sandboxing and other advanced malware detection methods, including CPU emulation.
- Next-generation intrusion prevention to provide visibility and prevention of compromise attempts. They are an efficient control to deploy on the internal network.
- Email and Web gateway security to enforce multiple methods of content inspection for malicious and unwanted activity, using a variety of simple to advanced threat detection methods.
- Distributed denial of service (DDoS) prevention to ensure the business can continue to transact under high volumes of traffic, or other methods of dealing with application-specific DDoS activity.
- Network behavioral analysis (NBA) and security analytics, where network traffic patterns and user activity and content (user entity behavior analytics [UEBA]) can be reviewed for indicators of compromise and suspicious activity.
- Security awareness training for users to increase the ability for them to recognize social engineering attempts.
- Payload inspection technology that uses techniques such as CPU emulation and sandboxing to provide a behavior-centric method of malware detection.
- DNS security to give visibility and protection against the resolution of unwanted or malicious hosts.
- NetFlow and packet capture allow complete visibility of the internal network to various degrees of depth.

Exploitation

An array of network, host and server technologies in conjunction with continuous monitoring can detect and deny access to the organization's environment:

- Security information and event management (SIEM) to correlate the events and logs from multiple security, infrastructure and identity elements to provide better visibility of malicious behavior
- Prevention-focused security technologies, such as firewall, endpoint protection platform (EPP), next-generation intrusion prevention system (NGIPS), email and Web security
- Web application firewall (WAF) to prevent the exploitation of e-commerce and other critical Web applications
- ATD or advanced persistent threat (APT) technologies that can provide improved (but not perfect) detections against new threats or variants of existing threats
- Security analytics (UEBA) to review full session analysis, with high-level details of the exploitation and subsequent activity
- Threat intelligence usage in existing security technologies (SIEM, UEBA, firewall, IPS, EDR, SWG) to provide additional detection and prevention opportunities

Installation

During this phase of the kill chain, host-specific methods are the primary method to detect the execution of malicious content:

- EPPs can deliver multiple methods of malware prevention, browser security and application whitelisting.
- EDR can be used to proactively seek out (or hunt) for recently discovered threats, or to positively prove that a threat doesn't exist on other assets in the environment.
- Enterprise mobility management (EMM) can control and deny unwanted applications to run on company-managed or bring your own device (BYOD) devices. EMM can also deny user-installed applications from accessing corporate-sensitive data via methods such as per-application authentication VPN and containerization.
- Identity and strong authentication methods can reduce the chance of installation and access to data.
- DNS filtering, using techniques such as whitelisting and threat intelligence, can be used for devices on and off the corporate network to help control what hosts are able to resolve with DNS requests.

Once identified, recover from the situation by:

- Performing incident response
- Recovering compromised data from backups
- Restoring servers and end-user devices back to a known good state
- Potentially complying with law enforcement attempts to prosecute malicious actors
- Reporting on details of the breach and other compliance mandates (such as reports to financial regulators on any further impact expected by the company)

Command and Control

With this phase of the CKC, look for methods that detect the adversary's attempts to control previously compromised assets from outside your network. If there are infected devices with remote-access trojans or rootkits, use methods such as:

- Internet Protocol (IP) and DNS reputation-filtering capabilities of NBA tools, network forensics tools, firewalls, intrusion prevention systems and secure Web gateways.
- DNS security, where internal DNS servers themselves have threat intelligence capabilities to deny name resolution of malicious hosts. Internal DNS server logs going to a central location (such as a SIEM) for analysis is also highly recommended.
- Network monitoring using network flow data (NetFlow, sFlow, and so on) is very effective at detecting anomalous behavior. Dedicated tools and most SIEMs now support this feature.
- Application control on the network and/or hosts that can limit application, network application traffic and geolocation destination policy.
- SIEMs with watchlists, threat intelligence and other policies configured to detect this type of out-of-character behavior.

Action on Targets

During this phase, the adversary is trying to perform the most important part of its activity. This is to exfiltrate the data gathered in this and earlier phases of the kill chain or some other "action." Methods to be addressed are:

- After the initial compromise, all subsequent attack activity is performed as internal or trusted users. A SIEM, UEBA, data loss prevention (DLP) or database activity monitoring and protection (DAP) function performing continuous monitoring can assist with identifying trusted user access to data that is not specific to their role, access to data in volumes previously unseen, access to data at times of day that is out of character, and access to data from locations or devices previously unseen
- Network behavioral analysis can highlight devices that are moving data around that is not part of its normal role (traffic to hosts that stand out), an exceedingly high volume of DNS traffic to an external DNS server that is not defined for external host name resolution, traffic protocols being actively used that are against policy
- Next-generation firewalls (NGFWs) and intrusion prevention systems can identify a trusted user attempting clearly malicious activity such as an FTP session to an unexpected destination

Take Steps to Augment Your Existing Prevention Methods

These steps can help take this understanding of the CKC and make it more actionable inside your organization.

- Start to inventory how many steps of the CKC you currently cover for your most critical IT assets.
- Know what's on your network (vulnerability assessment) and prioritize patching that takes into account vulnerabilities that are seeing active exploitation in the wild.
- Verify how your existing controls can be augmented (new subscriptions) or upgraded (new features) to address more steps of the CKC.
- Identify any visibility and access gaps — for example, encrypted traffic, direct-to-cloud services and identity monitoring.
- Investigate security automation and analytics tools that can help augment existing staff (due to the acute shortage of staff in the industry) and automate multiple security processes.
- Investigate whether engagement of a service partner will help for areas such as staff augmentation and 24/7 coverage.
- Prioritize to determine future investment in people, processes and technology that you will require to be better aligned to your adversaries.

Acronym Key and Glossary Terms

ACL	Access control list
ATD	Advanced threat defense
DAP	Database activity monitoring and protection
DAST	Dynamic application security testing
DBSM	Database security monitoring
DLP	Data loss prevention
EMM	Enterprise mobility management
EPP	Endpoint protection, including host-based features such as firewall, anti-malware, whitelisting and disk encryption
ETDR	Endpoint threat detection and response
FIM	File integrity monitoring
HIPS	Host-based intrusion prevention system
IAM	Identity and access management
MDM	Master data management
NGFW	Next-generation firewall
NGIPS	Next-generation intrusion prevention system
NIPS	Network intrusion prevention system
QoS	Quality of service
SEG	Secure email gateway
SIEM	Security information and event management
SSL	Secure Sockets Layer
SWG	Secure Web gateway
TIP	Threat intelligence platform
VA	Vulnerability assessment

Evidence

[1]"Lockheed Martin's Cyber Kill Chain"

Mitre's Cybersecurity Threat-Based Defense

Microsoft's Security Development Life Cycle

Source: Gartner Research, G00298058, Craig Lawson, 07 April 2016

About LookingGlass Cyber Solutions

LOOKINGGLASS

At LookingGlass, our Mission is to deliver the most advanced and comprehensive threat intelligence driven solutions so security teams have the best chance of finding and mitigating threats early before they do damage.

LookingGlass Cyber Solutions delivers comprehensive threat intelligence-driven security through a scalable solution portfolio of machine readable threat intelligence (MRTI), threat intelligence management with 140+ data sources transformed into global Internet and threat intelligence, network threat mitigation and threat intelligence services.

By addressing risks across structured Indicators of Compromise (IoCs), unstructured and open source data (OSINT), internal network telemetry, and network threat mitigation, customers gain unprecedented understanding into threats that may impact their business including cyber, physical assets, and third party partners.

Prioritized, relevant and timely insights enable customers to operationalize threat intelligence in an effective and efficient way throughout the threat lifecycle.

Source: LookingGlass Cyber Solutions

To learn more, visit the LookingGlass website at LookingGlassCyber.com.