Technical white paper

HP Attack Life Cycle use case methodology

HP Enterprise Security Products Global Services

Table of contents

Introduction

The purpose of this document is to introduce the concept of an Attack Life Cycle methodology, show how HP Attack Life Cycle methodology can be applied for the authoring of use cases and showcase the benefits of using an attack life cycle methodology over standalone use cases.

This is considered to be advanced content in use case authoring and readers are expected to understand ArcSight ESM use case capabilities as well as general security product capabilities. The rules referring to Windows tools and registry are synonymous with configurable Malware and Virus forensic events.

Attack Life Cycle

Attack Life Cycle Use Cases

The phrase “attack life cycle” describes the structure of the intrusion, and the corresponding model, which guides analysis to inform actionable security intelligence. The attack life cycle is a useful way to group disparate security “events” into a context that centers on the attacker and/or the attack. Rather than trying to look at network security events in isolation they should be combined with host based security events. Data sets should be integrated and correlated by grouping them according to attack vectors, attack payload delivery profiles and intrusion compromise behaviors.

Using this method provides analytic enhancements to find events that would otherwise be ignored, known as a false negative; but also find the noise produced by point solutions, known as a false positive. The different data sets can be combined or chained to reduce false negatives. False positives can be reduced by processing more events through the SIEM aimed at the different pieces of the attack life cycle. This allows the SIEM operations staff to attain better situational awareness through post correlation to define further compromise, such as command and control and data exfiltration events, and chain them.

Industry discussion and analysis of many recent high profile cyber-attacks such as the RSA and Sony breaches—indicate that these attacks each followed a distinct, multi-stage approach to penetrating the organization’s network, targeting sensitive data and successfully stealing it. There has been a tremendous focus on stopping an initial breach, but little focus on following a staged approach to compromise.

Attack life cycle attack phases

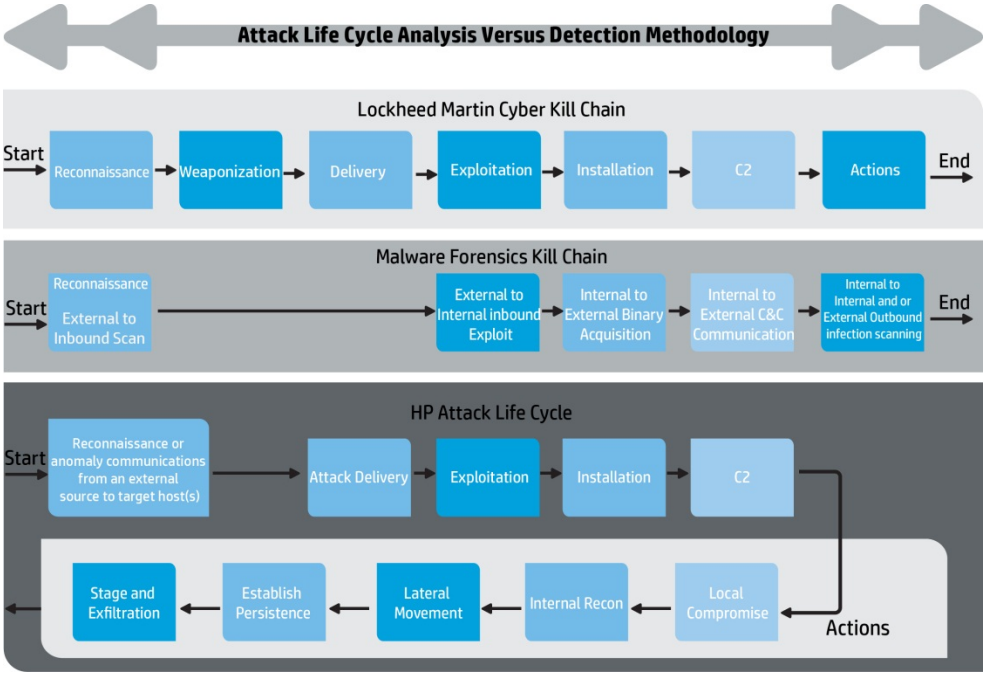
Let us assume the attacker breaches the perimeter, establishing a beachhead inside the network. Then, the attacker establishes a backdoor connection to a command and control server to download toolkits and additional payloads from an external site, but this is only the initial breach. Once the breach has occurred, the attacker begins to move laterally around the network taking inventory of the resources and looking for opportunities to collect additional credentials, or escalate the privileges they already have, to gain access to the organization's data. Finally, the attacker can collect and eventually exfiltrate the data.

Many security organizations using SIEM technology write use cases in a standalone manner. They typically make use of single individual use cases as indicators of compromise. This results in incident alerts that may be considered a premature event and manual human analytics is needed to further review events to validate them as indicators of compromise. An attack life cycle approach allows use cases to be written to group events and provide post correlation to further reduce the manual analytics effort.

HP has created a methodology around the event attack life cycle to better position the ArcSight SIEM capabilities for use case development.

The diagram below depicts three attack life cycle methods:

The Lockheed Martin Cyber Kill Chain, The Malware Forensics Kill Chain Method, and the HP Attack Life Cycle which is used to describe security events in the context stages for security intelligence and use case development. HP also uses the attack life cycle to help understand risk in a particular area of the attack life cycle.



Note
The below section describes each phase of the methodology starting with Lockheed Martin's reconnaissance explanation, then the Malware Forensics kill chain reconnaissance external to inbound scan phase, and then the HP Attack Life Cycle reconnaissance or anomaly communications phase. Then it will go back to Lockheed Martin's next phase. This is to help the reader understand the differences between methodologies.

Reconnaissance—As described by Lockheed Martin, this stage is the research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies. This is typically known as non-intrusive intelligence gathering.

Reconnaissance external to inbound scan—As described by the SANS Institute, this stage involves the active reconnaissance of a target network by inbound scanning events. The Malware forensics procedures assume that a detectable reconnaissance scan can be detected as an event.

Reconnaissance or anomaly communication from an external source to target host(s) As described by HP Attack Life Cycle, this stage involves the initial communications from an external source to a target host or hosts which are considered attack vectors. In the context of SIEM, tooling a perimeter event is not necessarily specific to the external Internet network perimeter. An external source could be an insider source to a secure internal network or host. Anomaly communication is used to describe the various communication techniques that are used to reconnaissance a network, such as:

i. Very slow scanning that wouldn't create discernible scanning events in firewalls or intrusion prevention systems indicating that a scan has taken place.
ii. Communication traffic that is known to be from bad or blacklisted source host addresses.
iii. Communication traffic that is outside of normal profiled (white listed) or network / asset model communication trends which is considered an anomaly.
iv. Communication traffic that is from an unusual geo location source.

Weaponization—Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Client application data files, such as Adobe Portable Document Format (PDF) or Microsoft Office documents are increasingly being used to serve as the weaponized deliverable.

It should be noted that the HP Attack Life Cycle use cases largely ignore weaponization as a practical part of the HP Attack Life Cycle as it is largely dependent on third party products and understanding known malicious binaries which is covered in the later aspects of the life cycle

Delivery—As described by Lockheed Martin, this stage is the transmission of the weapon to the target environment. The three most prevalent recorded delivery vectors for attack payloads are: email attachments, websites hosting malicious content, and USB removable media.

Attack Delivery—The HP Attack Life Cycle takes into account events and use cases to review events of interest for delivery of potential payload (ex. spear phishing email). Exploited weaknesses in browsers or other 3rd party applications can lead to a high false positive event rate. HP use cases take this information into account as a filtered watch list to correlate with other events.

Exploitation—After the weapon is delivered to a victim's host, exploitation triggers the intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code. Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.

External to Internal inbound Exploit—As described by SANS Institute Malware forensics, this stage of the attack life cycle describes the detection of an inbound exploitation event from an external to an internal host. The delivery mechanism looks for events for:

i. Direct exploitation of the host through an open service port.
ii. Malicious email attachments.
iii. Infected P2P media.
iv. Drive-by-download infections for malicious websites.

Host Exploitation—The HP Attack Life Cycle takes into account both the Lockheed Martin and SANS Institute methodologies, however host exploitation described through SIEM use cases should account for events from:

i. Third party vendor product events such as Intrusion Prevention Systems, Antivirus, and Antimalware.
ii. Events that are potentially overlooked or less obvious changes made to an operating system such as new processes being started and others being stopped.
iii. External to inbound communications traffic.
iv. Correlated vulnerability information.
v. Correlated network and asset model information.

Installation—Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.

Internal to External Binary Acquisition—In the case of Malware forensics, the next stage in the attack life cycle methodology is to communicate to the source of the attack and download a binary payload to install on the compromised host. In the case of some well-known exploits, traffic can be viewed leaving the compromised hosts towards an external source. This is typically on a Windows DCE or RPC port such as TCP 135 in order to gain shell access to the compromised host.

Binary Installation—As described in the HP Attack Life Cycle, this stage involves the detection of events released to known attack payload delivery profiles. For example, on a Windows machine there are malicious binaries that are not detected by point solutions such as antivirus or anti-malware software. The analytics of attack payload delivery profiles need to be examined such as the addition of registry settings or the increase in the number of Windows processes, protection software (antivirus) services being terminated, and other heuristic events such as memory usage and operating system firewall outbound sockets.

C2—Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conducting activity automatically. Once the C2 channel has been established, the intruders have "hands on the keyboard" access inside the target environment.

Internal to External C&C Communication—The next step in the Malware forensics kill chain for the newly infected machine is to establish a listen port to accept new binary updates or command and begin scanning other external victims on behalf of the botnet for lateral movement.

Command and Control—This step is very similar in the HP Attack Life Cycle, Lockheed Martin and SANS malware forensic methods. Use cases are produced to correlate source to destination communications to recognize command and control (C2) transactions back out to the network. This strategy focuses on identifying the web sites and IP addresses that attackers use to communicate with malicious code already infiltrated onto our computers. This is known as blacklisting. While some of these sites are legitimate and have been compromised, the majority are new domains registered by attackers solely for the purpose of command and control. Targeted attacks from advanced persistent threats are unlikely to exist in publicly available blacklists. For this situation, HP recommends making use of white lists and asset model based use cases to address exfiltration in the attack life cycle.

Actions on Objectives—This stage of the Lockheed Martin methodology describes actions and objectives an attacker may take after progressing through the first six phases. Typically, the objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment. Violations of data integrity or availability are potential objectives as well. Alternatively, the intruder may only want access to the initial victim box for use as a hop point to additional compromised systems to move laterally inside the network.

Internal to Internal and or External Outbound infection scanning—This step in the Malware forensics kill chain describes when the infected host begins interacting as part of a larger botnet and begins scanning other external victims on behalf of the botnet to spread infection.

Local Compromise—This step in the HP Attack Life Cycle is to review events of local compromise. This is considered different to both the attack life cycle phase of binary installation and the later phase of persistence as the use cases in this area are specifically focused around the creation of local accounts, privilege escalation, compromise of existing local accounts, changes made to group policies, permission changes for file and folder access, and the use of common command line tools in Windows and Unix.

Internal Recon—HP Attack Life Cycle describes this step as a compromised host profiling the network for other vulnerable targets or to establish the location of the target data or interest of the attacker. Typical use cases in this phase are the use of command line tools such as netstat, looking for communications between the compromised host and other hosts such as beaconing.

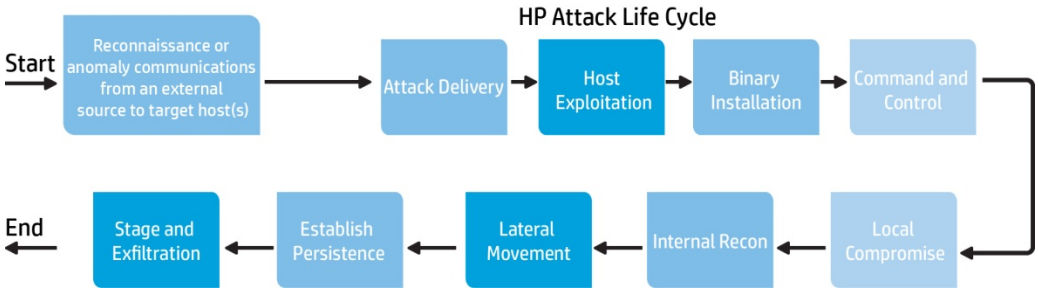
Lateral Movement—HP Attack Life Cycle describes this step as the movement from the compromised host to other hosts. Use cases in this area look for such events like netlogin, remote registry, remote WMI communications, remote group policy editor and remote session communications such as file share access, RDP, SSH, HTTPS.

Establish Persistence—The HP Attack Life Cycle describes this phase as actions taken by the attacker to establish a foothold in the network. Often, if an attacker has compromised this much of the environment without being detected then they are going to invest in staying within the environment. Use cases look for events of less obvious command and control communication from internal to external hosts. For example: newly spawned communication services between internal hosts, such as HTTPS, between servers that should not provide this service; common unknown processes being found on multiple hosts; and new binaries being added to the compromised host.

Stage and Exfiltration—The HP Attack Life Cycle describes this step as an attacker taking active steps to steal and exfiltrate data. Use cases would look for the access, movement and central storage of sensitive data. Often attackers will encrypt the stolen content locally before exfiltration. Exfiltration specific use cases should look for communication spikes in the network that are anomalous to the everyday use of the compromised host.

Example 1: HP Attack Life Cycle Phishing Use Case

The purpose of use cases used in the attack life cycle are related to the event filtering and cross-event correlation. This allows for reduction of false positive triggered events from a point solution and event reviews with context that would otherwise be ignored by automate rules.



An example HP Attack Life Cycle use case can look like the following.

Threat / Business Risk: Phishing attacks.

Summary of Risk: The business has noted an increase in malicious emails that are targeted at specific business users. The emails often contain harmful email attachments or malicious Internet URLs.

Events are often seen by various point solutions in a non-consistent way. For example, desktop antivirus software quarantines attachments in isolation of the email gateway which finds and blocks email attachments prior to being delivered to the desktop. During further analysis, it is thought that there are potential unknown viruses or malware within the business network going undetected.

Use Case Example

Attack life cycle Stages: Reconnaissance or anomaly communications from an external source to target host(s). Define rules to short list (shortlist 1) when an email attachment travels through the email gateway where the attachment contains a potentially harmful file type and where the sender email address is not a trusted email source (from a list) or internal company IP address. Email attachments include potentially harmful files such as Microsoft Excel, Microsoft Document, JPEG images, PDF documents, M4A files, M4P file, MP3 audio file, Movie file. Add email recipient machines source IP address of the event to shortlist 1.

Attack life cycle Stages: Attack Delivery. Define rules to capture events when an email attachment has been opened that is potentially harmful, but are accepted file types used for everyday business use: Microsoft Excel, Microsoft Document, JPEG images, PDF documents, M4A files, M4P file, MP3 audio file, Movie file. Add source IP address of the event to shortlist 1.

Attack life cycle Stages: Host Exploitation and Binary Installation. Define rules to escalate all antivirus and anti-malware software events where the events would be raised as incident alerts and the source IP address would be added to the compromised host active list. Define a second high-level rule that cross correlates to determine if the host source IP address is also found on shortlist 1. If so, this will trigger an incident alert and the source IP address of the host will also be added to the compromised host active list. Other specific rules, not relying on antivirus or anti-malware events include:

i. Rule 1: A registry change has occurred in one of the registry start locations such as \Runonce.

ii. Rule 2: If new unknown process has been spawned.

For rules 1 and 2 add the source IP address to shortlist 1.

Attack life cycle Stage: Command and Control. Define rules for the context of both this threat and the business risk and general use case. Does a source IP address communicate with known (black listed) malicious command and control servers? Raise the results of this rule as an incident alert and add the IP address to the compromised active list.

Attack life cycle Stage: Local Compromise. Define rules that look for events from local operating system logs where:

i. Rule 1: Creation of local accounts.

ii. Rule 2: Creation of escalation of privileges.

iii. Rule 3: Group policy changes.

iv. Rule 4: If Antivirus or Antimalware software processes have been terminated.

v. For rule 1 to 4: Add source IP address to short list (shortlist 2)

vi. Correlation rule if an IP address exists on shortlist 2 more than once raise and incident alert.

Attack life cycle Stage: Internal Recon. Define a rule to look for network communications anomalies for a source IP address that has been added to our shortlist 1 or shortlist 2. Network communication anomalies include deviations from known white list profiles. For example:

i. Rule 1: Peer to peer communications.

ii. Rule 2: HTTPS communications between desktop servers where HTTPS doesn't exist as a service on our desktop environment.

iii. Rule 3: Beaconing of desktop network communications trying to find a way of routing to the Internet this would show as firewall drop events.

iv. Rule 4: Multiple communications where the source network zone is desktop and the destination network zone is desktop.

v. Correlate rules 1-4 where the source also exists on either shortlist 1 or shortlist 2 and if it does raise this as an incident and add the IP to the compromised host asset list.

Attack life cycle Stage: Lateral Movement. This stage is in the attack life cycle is closely related to internal recon but rules go a step further identifying event transactions between devices rather than simply communications. We can define several rules for this stage such as:

i. Rule 1: Windows program audit events where netstat has been used add source IP to shortlist 2.
ii. Rule 2: Windows net logon event add source IP address to shortlist 2.
iii. Rule 3: Windows remote registry event add address source IP address to shortlist 2.
iv. Rule 4: Windows remote WMI event add address source IP to shortlist 2.
v. Rule 5: Windows remote policy editor event add address source to shortlist 2.
vi. Rule 6: Windows program audit event where psexec has been used add source IP to shortlist 2.
vii. Correlation rules 1: where a single source IP address appears on shortlist 2 more than once raise this as an incident alert and add compromised host asset list.
viii. Correlation rule 2: If rules 1—6 correlate with an IP address on shortlist 1 raise as an incident alert and compromised host asset list.

Attack life cycle Stage: Establish Persistence. Establish Persistence. This stage in the attack life cycle is closely related to local compromise. In this phase we would be looking for further communication anomalies and changes to the local host which can be illustrated by the following rules:

i. Rule 1: Windows policy event changes make to file and folder access.
ii. Rule 2: Internal to Internal communications between hosts in the same network zone on unknown communications channels for example a desktop communicating to another desktop using HTTPS.
iii. Rule 3: large download of data from an external host that is not commonly visited or first time visited
    a. 3.1: Netflow event anomies as a trend for deviations
    b. Correlate 3.1 with a query to a proxy server looking for low talking website visits.

For any correlation event found in rules 1-3, add the source IP address to shortlist 2. Where a single source IP address exists in shortlist 2, raise this as an incident alert and add to the compromised host asset list.

Attack life cycle Stage: Stage and Exfiltration. At this stage of the attack life cycle an attacker would be looking to consolidate stolen data and exfiltrate it from the network. Rules for exfiltration would be:

i. Rule 1: Windows program audit event where NTbackup has been used add source IP to shortlist 2.
ii. Rule 2: Windows events for registry access to the following registry locations as this indicates the Windows SAM file has been accessed. Raise an incident alert and add to shortlist 2

    HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\JD

    HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Skew1

    HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Data

    HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\GBG.
iii. Rule 3: Windows event for file movement across network shares
    a. 3.1: Correlate where movement from network shares events have occurred as well as folder permissions change events from the same host. Add to shortlist 2.
iv. Rule 4: Netflow anomalies over a trended period of time where the destination address is in a unusual GEO location add source IP address to shortlist 1.
v. Rule 5: Correlate access event to hosts that store sensitive information and correlate this with email sending events to unknown email (white listed) recipients. Add to shortlist 1
    a. Correlate multiple email sending events where attachment are being sent to a single unknown email in the same day and the for a total data size of > 100mb Add to shortlist 1.

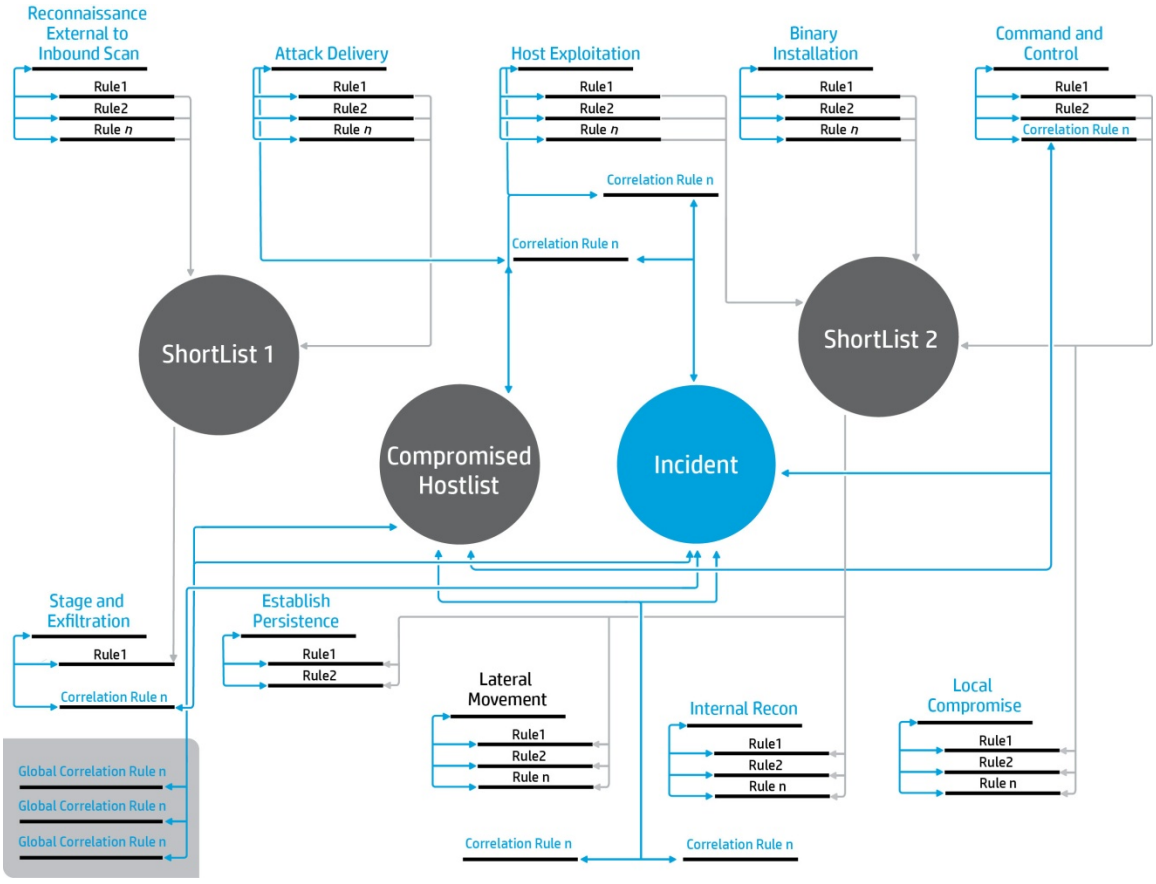
The diagram below depicts all of the uses cases from the phishing attack example in the HP Attack Life Cycle phases.

As described, a number of use cases will supply a short list of potential events of interest. If the same host has been listed numerous times in a short list with indicators of compromise, an incident will be generated The incidents are indicated by the grey lines in the diagram and the light blue global correlation rules section.

Specific events of interest with a high degree of certainty, such as alerts from host malware software, would raise incident alerts as indicated in the diagram.

When an incident is raised on a host, the host will be added to the compromised host list. This allows the security operations team to quickly understand if a compromised host has multiple indicators of compromise throughout the attack life cycle rather than just looking at events in isolation.

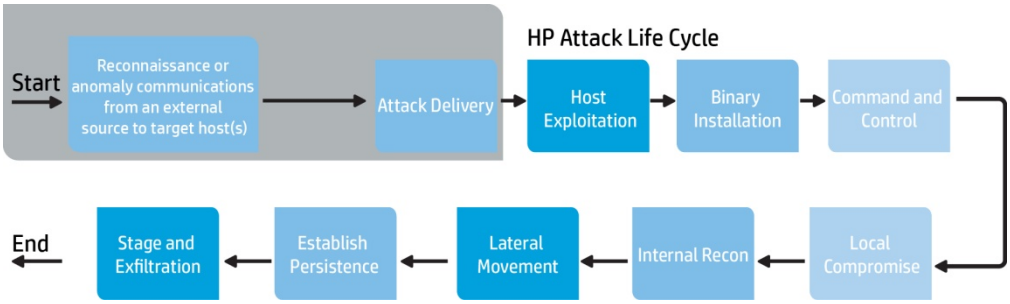
The short lists can also be quickly reviewed to understand if there are additional compromise indicators to provide a better understanding of the scale of the incident to help inform and action the triage and mitigation steps.



Example 2: HP Attack Life Cycle Reusable Use Cases

This example shows how the use cases from example 1 can be reused throughout the attack life cycle stages and applied to other applicable threat vectors.

This example will focus on a perimeter threat as the threat vector which will have the largest changes in the use cases for reconnaissance, anomaly communications, and the attack delivery attack life cycle stages. These are indicated by the red box in the diagram below. The example reuses all other use cases from example 1 and adds in a few use cases to other stages of the attack life cycle to align them to the new threat vector.



Threat / Business Risk: Perimeter attacks to DMZ hosts.

Summary of Risk: The business has been made aware of a risk to DMZ security as discovered through a number of penetration test reports. The risk indicates that there is an inherent weakness in segregation of DMZ hosts meaning a compromise from one host machine in the corporate DMZ which is a low value asset maybe used to gain access to a higher value assets through lateral movement. The risk mitigations should make use of a layered security approach where high value assets make use of more security controls and the low value assets have less security controls addressing the cost of implementation.

The business is looking for a solution making use of their SIEM technology and security operations department to mitigate the risk to an acceptable level without spending additional money on security controls for the lower value assets.

Controls in the DMZ that can be used by all assets include firewall, intrusion prevention system and antivirus as a minimum set of controls.

Use Case Examples

Attack life cycle Stage: Reconnaissance or anomaly communications from an external source to target host(s). Define the following rules to shortlist events of interest:-

i. Rule 1: Add source IP address of hosts that attempt that attempt to make TCP / UDP connections that are defined as packet anomalies such as SYN, ACK, FIN packets to the suspicious IP address short list. These events would appear at both the firewall and Intrusion Prevention System.

ii. Rule 2: Add source IP of hosts that perform a network scan IP address to the suspicious IP address short list. These events would appear at both the firewall and Intrusion Prevention System.

iii. Rule 3: If the source IP address is a known bad IP address from our threat intelligence active list and attempts to make a connection to a DMZ asset raise an event of interest and add this IP address to suspicious IP address short list.

iv. Global rule: if an IP address appears on suspicious IP address short list more than once add this source IP address to threat intelligence active list.

Note: The suspicious IP address short list will have a short term time to live for source IP address values and the intelligence active list is a long term active list that helps filter false positives.

Attack life cycle Stage: Attack Delivery. Define the following rules to shortlist events of interest:-

i. Rule 1: add the source IP address of the host that "attempts" to exploit a system to the suspicious IP address short list. These events would appear from the Intrusion Prevention System. Note attempt indicates the IPS has taken action to stop the attempt to exploit a system. We add the IP address to the suspicious IP address short list as the first event from the IPS may be a false positive.

ii. Rule 2: Raise an alert if the source IP address of the host that attempts to exploit a system that is considered a sensitive or a priority asset in our asset model. Add the source IP address to the suspicious IP address short list. We add the IP address to the suspicious IP address short list as the first event from the IPS may be a false positive. However we raise an alert as the asset is considered of a high enough priority to be investigated as a priority using manual human analytics.

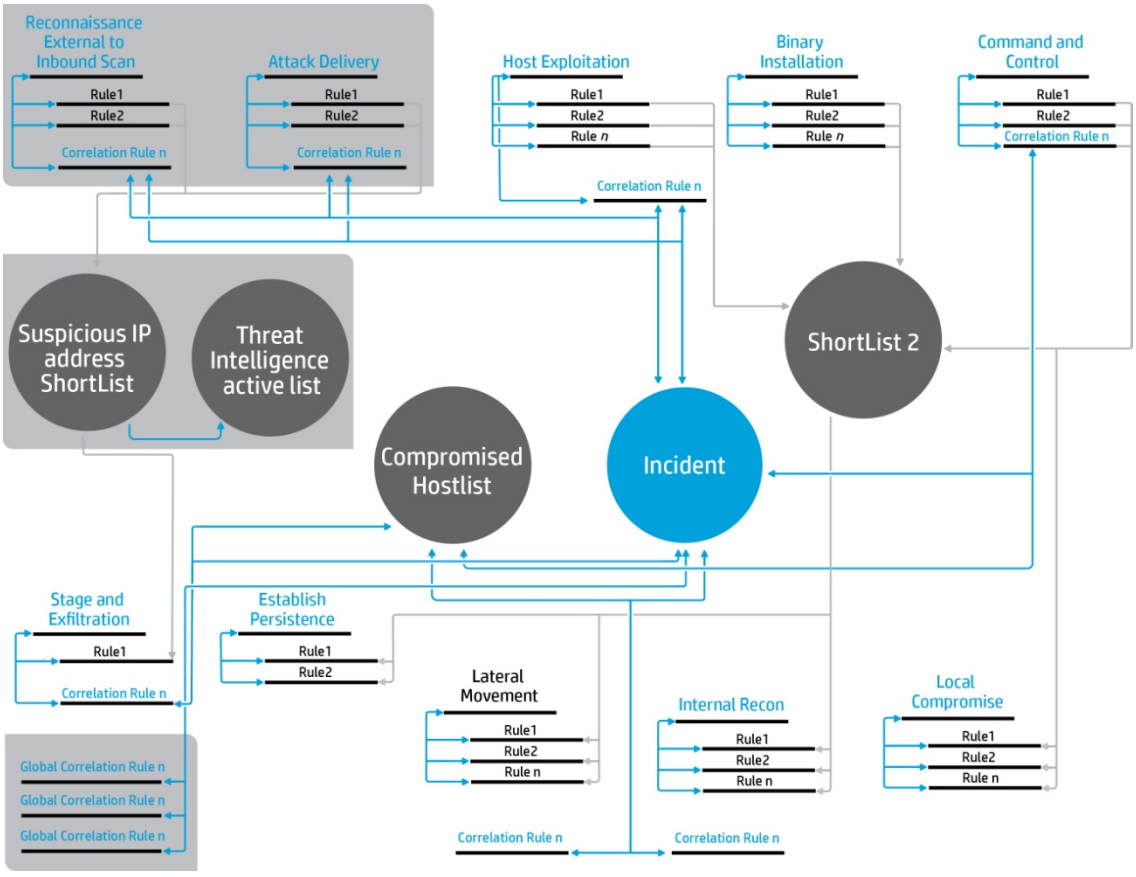
iii. Rule 3: Raise an alert if the source IP address attempts to exploit a host that has a known vulnerability. Add the source IP address to the threat intelligence active list. Add the destination host asset IP address to the compromised host list.

iv. Global rule: if an IP address appears on suspicious IP address short list more than once add this source IP address to threat intelligence active list.

Attack life cycle Stage: Stage and Exfiltration. For this specific attack life cycle phase to add the following rules:

Rule 1: If our firewall or Netflow detects outbound communication to an IP address that is on the threat intelligence active list raise and alert and add the source host IP address to the compromised list.

All other rules from example 1 are still applicable as indicators of compromise to this use case and there are changes to reflect the attack vectors as indicated in the diagram.



Summary Benefits of a attack life cycle

There are many benefits to using a attack life cycle approach versus standalone use cases. The examples shown previously demonstrate that developing use cases to layer events using the HP Attack Life Cycle methodology provide benefits in the areas of:

Defined Threat Coverage
Defining the use case coverage of threat vectors and ensuring a layered security approach makes use of a security in-depth strategy as opposed to the traditional practice of defining use case rules for standalone events.

Reduction of false positive
Trusting single events from point solutions such as intrusion prevention systems is prone to false positives and can cause large overhead for human analytics. Relaying on events from other solutions such as antivirus or anti-malware software can limit the information reaching the security operations regarding the initial attack vector.

Making use of the HP Attack Life Cycle methodology allows for false positive reduction and enhanced situational awareness of events from point solution by continuously evaluating ongoing events of other indicators of compromise throughout the attack life cycle.

Providing greater coverage over false negatives
Applying the HP Attack Life Cycle Chain methodology allows the SIEM to further correlate and post-correlate events via rules throughout the life cycle. This allows for inclusion of events into use cases that would otherwise be ignored by security operations due to their volume and potentially false positive nature. Missing events of interest is known as false negatives. False negative reduction provides a huge value to situational awareness of both automated and manual analytics, both pre- and post-incident.

Enhanced situational awareness—Events of interest versus actionable incidents
Making use of the HP Attack Life Cycle methodology to raise events of interest as incidents but also to further filter events and define IP addresses and compromise values in shortlist (Active Lists) provides significant enhancements to situational awareness allows the security operations team to respond faster to security incidents throughout the attack life cycle as part of the triage and CIRT response.

Enhanced Situation awareness—Event visualization to aid in human analytics
The two examples in this white paper demonstrated how to use short lists with contextualized information to make better use of visualization tools to aid in analytics.

Shortlist 1 was created to filter events that would otherwise be ignored: users opening emails that are potentially dangerous from untrusted email senders. The values shortlisted would be:

<Source IP address of the email client>

<receiver email address>

<sender email address>

<email attachment name>

From an analytics perspective, this information is valuable for reporting and dashboards as well as for event graphs. Visualizations and reports could show how many people received an attachment named x.y.z and even though only one recipients may have opened the attachment, others may have received it. This intelligence allows the security operations team to take informed action to notify the other recipients to not open the email attachment or to allow the emails with this attachment to be deleted on behalf of the recipients. It also allows for the black listing of sender email addresses to stop further attacks originating from this sender.

Enhanced situational awareness—Provide Metrics and Continuous Improvement of Threat Actors
Making use of the HP Attack Life Cycle methodology allows for the reporting on key threat actors in a specific risk domain for an organization to better understand if the security controls in a particular area are performing per the risk needs. It also allows for the focus and investment of time in a specific area of concern for continuous use case improvement in a structured and informed manner.

In example 1, if a number of phishing emails containing harmful attachments have managed to route through the email gateway without being quarantined, and at the same time we see the desktop antivirus and malware software is detecting these harmful attachments, it allows for the quantitative analysis of the performance of the email gateway as a security control. This is achieved by comparing the shortlist (active list) of filtered events.

Provide Reusable Use Cases in the Attack Life Cycle Phases
As demonstrated in example 2, the HP Attack Life Cycle allows for the reuse of use case rules from different stages of the attack life cycle across multiple risks. This positions each of the attack life cycle phases as a compensating security control that can be measured across a risk framework.

The additional benefits of renewable use cases helps save time and research in evolving use case rules for new threat vectors with a reduced overhead of time and resources.

Learn more at
hp.com/go/espservices

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA4-9490ENW, March 2014, Rev. 2