

What is Threat Intelligence and How It Helps to Identify Security Threats

Saturday, November 07, 2015 Wang Wei

[G+1](#) 59
 [f Like](#) 393
 [f Share](#) 201
 [t Tweet](#) 44
 [in Share](#) 6
 [Share](#) 282



Simply put, threat intelligence is knowledge that helps you identify security threats and make informed decisions. Threat intelligence can help you solve the following problems:

- How do I keep up to date on the overwhelming amount of information on security threats—including bad actors, methods, vulnerabilities, targets, etc.?
- How do I get more proactive about future security threats?
- How do I inform my leaders about the dangers and repercussions of specific security threats?

Threat Intelligence: What is it?

Threat intelligence has received a lot of attention lately. While there are many different definitions, here are a few that get quoted often:

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. – Gartner

The set of data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators – SANS Institute

Why is everyone talking about it?

Verizon's 2015 DBIR estimated a financial loss of \$400 million from 700 million compromised records, which resulted from 79,790 security incidents!

As long as security threats and breaches occur, every business will look for ways to protect their data. The threat landscape is always changing and the business risk is increasing because of our dependence on IT systems.

WHENEVER,
WHEREVER
YOU NEED.

Only \$1 a week for 26 weeks!

Subscribe Now

Ads by Google



- [Cyber Security Threat](#)
- [Information Security Risk](#)
- [Threat Intelligence](#)

Threats come from internal as well as external sources. Bottom line is, organizations are under

tremendous pressure to manage threats. Though information in the form of raw data is available abundantly, it is hard and time-consuming to get meaningful information based on which proactive measures can be set.

This naturally pulls more and more users towards threat intelligence as it helps to prioritize threats within the deluge of data, alerts, and attacks and provides actionable information.

The table below presents several common indicators of compromise that can be identified with threat intelligence feeds:

Category	Indicators of Compromise	Examples
Network	<ul style="list-style-type: none"> IP addresses URLs Domain names 	Malware infections targeting internal hosts that are communicating with known bad actors
Email	<ul style="list-style-type: none"> Sender's email address and email subject Attachments Links 	Phishing attempts where internal hosts click on an unsuspecting email and "phone home" to a malicious command and control server
Host-Based	<ul style="list-style-type: none"> Filenames and file hashes (e.g. MD5) Registry keys Dynamic link libraries (DLLs) Mutex names 	External attacks from hosts that might be infected themselves or are already known for nefarious activity

Threat Intelligence capabilities

Attacks can be broadly categorized as user based, application based and infrastructure based threats. Some of the most common threats are SQL injections, DDoS, web application attacks and phishing.

It is important to have an IT security solution that provides threat intelligence capabilities to manage these attacks by being both proactive and responsive.

Attackers are constantly changing their methods to challenge security systems. Therefore, it becomes inevitable for organizations to get threat intelligence from a variety of sources.

One of the proven methods to stay on top of attacks is to detect and respond to threats with a [SIEM](#) (Security Information & Event Management system).

A SIEM can be used to track everything that happens in your environment and identify anomalous activities. Isolated incidents might look unrelated, but with event correlation and threat intelligence, you can see what is actually happening in your environment.

Nowadays, IT security professionals must operate under the assumed breach mentality. Comparing monitored traffic against known bad actors sourced from threat intelligence would help in identifying malicious activities.

However, this could be manual and time-consuming. Integrating indicator based threat intelligence to a SIEM security solution would help in identifying compromised system and possibly even prevent some attacks.

Best Practices

Integrating threat intelligence and responding to attacks is not enough to combat the ever-changing threat landscape. You need to analyze the situation and determine threats you are likely to face, based on which you can come up with precautionary measures.

Here is a list of several best practices:

- Have an application whitelist and blacklist. This helps in preventing execution of malicious or unapproved programs including, .DLL files, scripts and installers.
- Check your logs carefully to see if an attempted attack was an isolated event, or if the vulnerability had been exploited before.
- Determine what was changed in the attempted attack.
- Audit logs and identify why this incident happened – reasons could range from system vulnerability to an out-of-date driver.

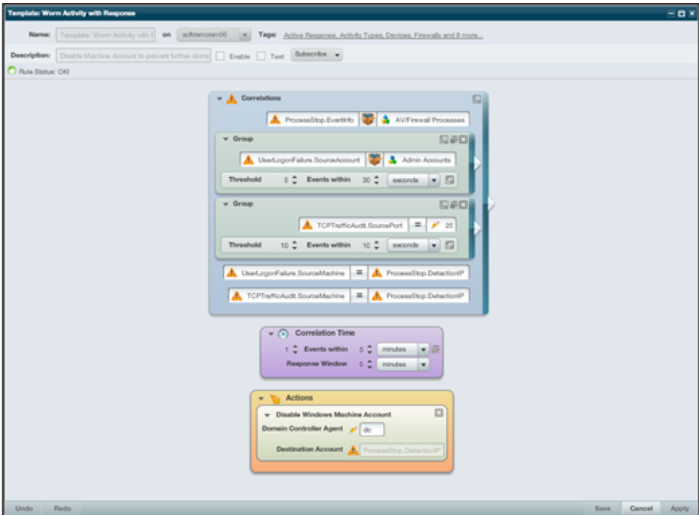
What will threat intelligence enabled SIEM solve

A SIEM, like SolarWinds Log & Event Manager, collects and normalizes log data from monitored traffic and automatically tags suspicious events.

With integrated threat intelligence mechanism and built-in rules, the monitored events can be compared against the list of constantly updated known bad actors. You can quickly search & monitor for hits from the bad actors against the log data in real time and identify common indicators of compromise.

You can automatically respond with actions like blocking known bad IP addresses, in case of malicious attack attempts.

Watch how [threat intelligence](#) works in a SIEM and download your free trial of a [leading SIEM](#) from SolarWinds.



- Ads by Google
- [Security Vulnerabilities](#)
 - [IBM Intelligence Security](#)
 - [Password Security](#)

Cyber Attack, Cyber Security, Cyber Threat Intelligence, Cyber War, Hacking News, Malware, Network Security, SIEM, SolarWinds Log & Event Manager, Threat Intelligence, Vulnerability

Join us on Facebook: You, 熊邪惡 and 801,444 others like this.

ABOUT THE AUTHOR



Wang Wei
Security Researcher and Consultant for the government, Financial Securities and Banks. Enthusiast, Malware Analyst, Penetration Tester.

IT'S HERE...
2015 GARTNER MAGIC QUADRANT FOR SIEM

COMPARE THE TOP SIEM VENDORS NOW ►

SUBSCRIBE TO UPDATE

Want more Interesting Articles to your Inbox every Morning?.

What's your email?

Sign Me Up

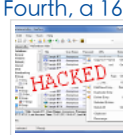
LATEST STORIES



Hackers have Hacked into US Arrest Records Database
What is Threat Intelligence and How It Helps to Identify Security Threats
FBI Deputy Director's Email Hacked by Teenager Who Hacked CIA Chief
ProtonMail Paid Hackers \$6000 Ransom in Bitcoin to Stop DDoS Attacks



Anonymous Group Leaks Identities of 1000 KKK Members



Fourth, a 16-year-old Hacker, Arrested over TalkTalk Hack
Researcher releases Free Hacking Tool that Can Steal all Your Secrets from Password Manager
Backdoor in Baidu Android SDK Puts 100 Million Devices at Risk



COMMENTS

0 Comments The Hackers News

Исследовательс...

Recommend Share

Sort by Newest



Start the discussion...

Be the first to comment.

ALSO ON THE HACKERS NEWS

WHAT'S THIS?

Hackers WIN \$1 Million Bounty for Remotely Hacking latest iOS 9 iPhone

4 comments • 5 days ago

buck rogers — i heard the pangu team did it first anyway for free?

Meet The World's First Person Who Hacked His Body to Implant a Bitcoin Payment CHIP

3 comments • 5 days ago

DefToneR — Its just another NFC chip under the skin. You buy a mifare keychain, you open it, you cut your skin, end of the "Bio Hacking". Come ...

Kim Dotcom's Decentralized Internet — For You, Powered By You

11 comments • 5 days ago

WeAreYourGods — Awesome. Hopefully the alphabet boys don't kill him before it gets off the ground.

Fourth, a 16-year-old Hacker, Arrested over TalkTalk Hack

1 comment • 4 days ago

Commonsensediet — Well, when children can break into your systems and wreak have who's fault is it really? Maybe we should stop letting ...

Subscribe Add Disqus to your site Privacy

DISQUS

IT'S HERE...
2015 GARTNER
MQ FOR SIEM

ALLEN VAULT

NEW 2015

Quadrant for Security Information and Event Management

COMPARE THE TOP SIEM VENDORS NOW ►

研華物聯網無線I/O模組
解決方案

直接上雲、輕鬆應用、瞬間感知
WISE-4000系列

資料發布


資料處理


資料擷取


搶先了解





Popular Stories


- 


Researcher releases Free Hacking Tool that Can Steal all Your Secrets from Password Manager
- 


Anonymous Group Leaks Identities of 1000 KKK Members
- 


Hackers WIN \$1 Million Bounty for Remotely Hacking latest iOS 9 iPhone
- 

Kim Dotcom's Decentralized Internet — For You. Powered By You
- 


Anonymous Hackers to Leak 1000 of KKK Members Details on Million Mask March (Nov 5, 2015)
- 

Meet The World's First Person Who Hacked His Body to Implant a Bitcoin Payment CHIP
- 

FBI Deputy Director's Email Account Hacked by Teenager Who Hacked CIA Chief
- 

Fourth, a 16-year-old Hacker, Arrested over TalkTalk Hack
- 

Warning: 18,000 Android Apps Contains Code that Spy on Your Text Messages



ProtonMail Paid Hackers \$6000 Ransom in Bitcoin to Stop DDoS Attacks



WHENEVER, WHEREVER YOU NEED.

Only \$1 a week for 26 weeks!

Subscribe Now