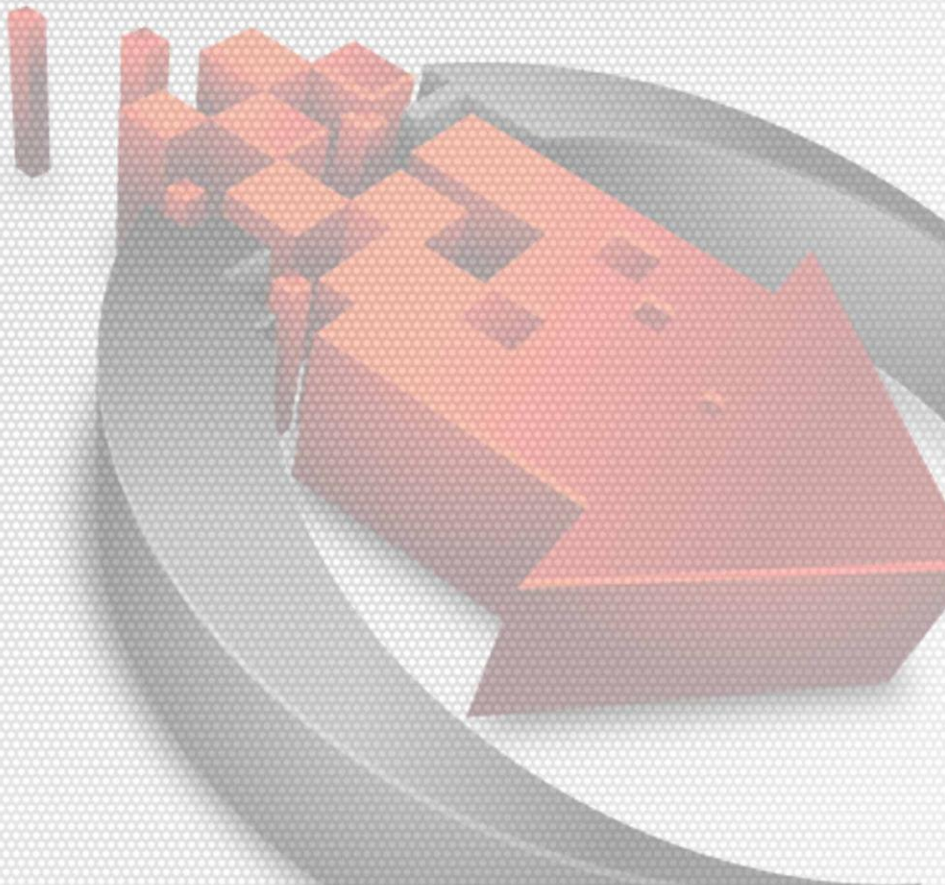
THREAT
INTELLIGENCE

BORN GLOBAL

Threat Intelligence
Managed Intelligence Service



Threat Intelligence Pty Ltd
info@threatintelligence.com
1300 809 437

Intelligence Feed #103 – Security Breach

Did you know that the faster you detect a security breach, the lesser the impact to the organisation?

If a security breach extends beyond a couple of hours then the financial impact quickly exceeds tens of thousands of dollars.

Intelligence-Based Security allows your team to identify threats before attacks are performed to prevent security breaches.

Who Is Threat Intelligence?

In the current threat environment, it is no longer sufficient to manage risk in a static manner to ensure the reputation and financial stability of your business.

The concept for Threat Intelligence is based around combining ongoing threat analysis and integrating it into security services to deliver dynamic intelligence based risk management.

This shift in mindset is required due to the slippery slope of the ever changing modern threat landscape, both globally as well as locally within your own environment.

This is supported by our ground breaking "Threat Analytics" offering that is the only product that can alert you to browser-based attacks before the attacks have actually launched. This provides you with the intelligence that you need to protect your business.

Thank you for using Threat Intelligence and we look forward to working with you in the future.

1 Table of Contents

2 Overview

2.1 Introduction

Cyber-attacks have dramatically increased in severity and frequency in recent years, leading to major security breaches and hundreds of millions of customers' data becoming compromised worldwide.

To operate within this ever evolving global threat environment, organisations must mature their traditional security strategies to an Intelligence-Based Security Framework, also commonly referred to as Threat Intelligence.

Rather than reacting to alerts for attacks, Intelligence-Based Security enables you to proactively identify threats against your organisation and dissolve them before an attack has been launched.

Threat Intelligence are experts in the area of Intelligence-Based Threat and Risk Management, and is backed up by their world-class security research and vast amount of specialist security experience across a wide range of industries. The Threat Intelligence team have trained up the likes of FBI, US Department of Defence, Australian Department of Defence, Cisco, VMware, Australian Taxation Office, and a number of intelligence agencies.

Our Managed Intelligence Services help you to integrate Intelligence-Based Security into your organisation so that your business remains safe in the ever evolving global threat landscape.

To discuss integrating Intelligence-Based Security into your organisation, then Contact Threat Intelligence on 1300 809 437 or email us at info@threatintelligence.com.

Intelligence Feed #128 – Risky Partners

Did you know that your partners are a security threat?

Hacking groups carry out parallel and multi-phased attacks to breach multiple companies to gain access to your corporate secrets.

You should always protect your data at third parties by enforcing strong security controls.

3 Managed Intelligence

3.1 Managed Intelligence Overview

When integrating intelligence into your security program, it is important to define a solid intelligence foundation. The key areas of an Intelligence-Based Security Framework include:

- Intelligence Strategy
- Intelligence Capabilities
- Intelligence Aggregation
- Threat Analytics
- Operational Intelligence

These areas can be broken down into implementation components, some of which are as shown in our Managed Intelligence Life Cycle below:

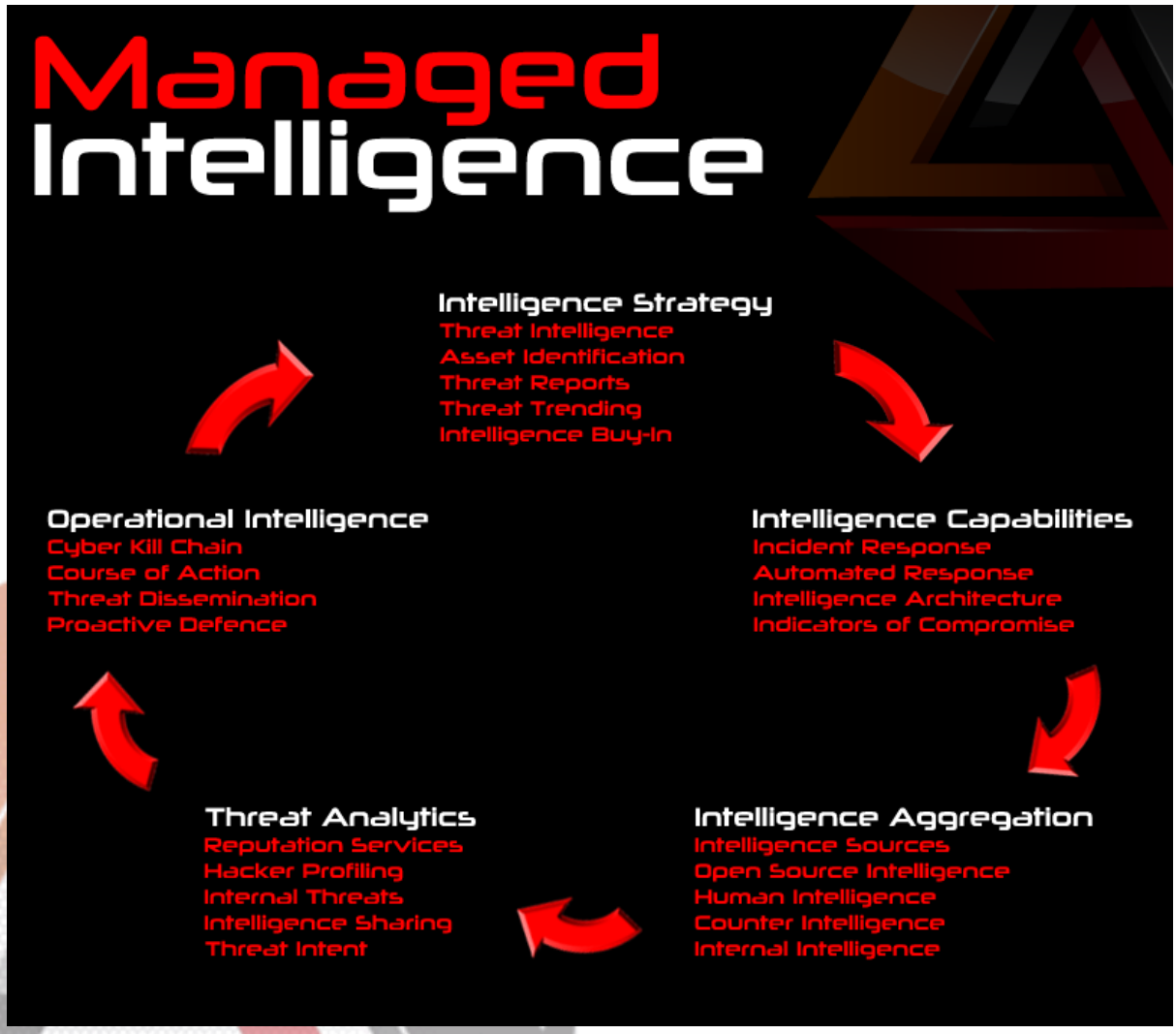


Figure 1 – Threat Intelligence, Managed Intelligence Life Cycle

4 Intelligence Strategy

4.1 Intelligence Strategy Overview

Depending upon your specific type of organisation, your business needs and limitations, and risk threshold, you need to first develop an Intelligence Strategy. This typically involves defining exactly what you want to protect and how you plan to protect it, as well as creating collateral to support the need for your proposed Intelligence Strategy.

A few of the components that you need to take into account when developing your Intelligence Strategy include:

- Threat Intelligence
- Asset Identification
- Threat Reports
- Threat Trending
- Intelligence Buy-In

This is far from a complete list, but it is aimed at providing you with an insight into what each stage involves at a high level and should be customised for each organisation.

4.2 Threat Intelligence

Threat Intelligence style-security is relatively new, which means that many people will not understand what it means, why it is important, what is involved, and what outcomes it can deliver.

For this reason, you will need to clearly define what Threat Intelligence is, in clearly explained steps aimed at a range of groups including technical staff through to executives. This will ensure that everyone is on the same page and is using the same terminology.

4.3 Asset Identification

You will need to know what you are planning on protecting. If you have data classification already in place for your organisation, then you should be able to leverage that existing information. If you have not yet classified your systems in terms of risk or sensitivity, then this is where you identify what assets (systems and/or data) are critical to the business.

Knowing what assets you are planning on protecting is a key component to any security framework, including Intelligence-Based Security Frameworks.

4.4 Threat Reports

In order to get your Intelligence-Based Security Framework approved and funded, you will need to be able to support your proposed strategy with threat statistics. Many organisations will use statistics found on the Internet to support their case. Ideally you should gather data for your own organisation for both internal and external threats.

4.5 Threat Trending

Threat Trends allow you to forecast and plan for the future, allowing your strategy to evolve each year and become more effective as the global and local threat landscapes change.

For the first round of the strategic plan you are most likely to base this trending on industry information, your security experience, and often a bit of a gut feel for where things are going. If you don't have a solid feel for the trend of where threats are going to be moving, it is recommended to engage a third party to help advise you to ensure that your strategy is a valid one.

4.6 Intelligence Buy-In

Now that you have gathered most of your information and have a clear Intelligence Strategy, you now need to gain buy-in from the executive team so that you can start integrating intelligence into your organisation.

This involves creating a 12 to 36 month roadmap of how intelligence will be integrated into the organisation, the phased approach that will be taken, the projects that will be created, the timeframes for each project, the estimated budgets for each of the projects, and the return on investment for implementing an Intelligence-Based Security Framework.

The return on investment often includes financial and reputational impacts suffered from a security breach that can be prevented, as well as a reduction in fraud through extra security controls when high risk transactions are identified.

5 Intelligence Capabilities

5.1 Intelligence Capabilities Overview

To successfully execute and manage your new Intelligence-Based Security Strategy, you need the skillsets and systems in place to ensure that it runs smoothly.

A few of the components that you need to take into account when developing your Intelligence Capabilities include:

- Incident Response
- Automated Response
- Intelligence Architecture
- Indicators of Compromise

This is not a complete list, but it is aimed at providing you with an insight into what each stage involves at a high level and should be customised for each organisation.

5.2 Incident Response

A capable incident response team (IRT) should be created if you don't have one already, as well as incident response procedures to handle the range of threats against your organisation.

If you already have an incident response team and procedures, they will need to be updated to take into account the significant shift in the concept of responding to threats rather than attacks or security breaches.

Incident response teams need to understand the various threats, threat indicators, and how to dissolve any threat to prevent a security breach, rather than cleaning up after the security breach.

5.3 Automated Response

Threat Intelligence can be integrated into security systems so that when a high risk threat is detected, proactive automated actions can be triggered to close down the threat and prevent the attack. This may be automatic injection of firewall rules, WAF rules, or IPS rules to prevent the attack.

Threat Intelligence has their own intelligence offering "Threat Analytics" (www.threat-analytics.com), which can be configured to automatically deploy a "Threat Analytics Agent" back to malicious web browsers. This is known as Offensive Counter Intelligence where automated actions can be triggered.

5.4 Intelligence Architecture

Depending upon what techniques were included within your Intelligence Strategy, you may need to make adjustments to your architecture to include Intelligence Systems.

These systems include capturing internal intelligence, aggregating external intelligence, deploying automated intelligence actions, and allowing threat analysis and reporting to be performed.

5.5 Indicators of Compromise (IOC)

Although Intelligence-Based Security allows threats and attacks to be shut down before they begin, you still have to assume that security incidents can and will occur, or potentially already have.

Security breaches leave trails that are known as “Indicators of Compromise”. These could be anything from logs, to timestamp changes, new or modified files, deleted files, new accounts, new processes in memory, network connections, network traffic, permissions changes, and the list goes on.

Systems should be put in place to search for Indicators of Compromise to identify any successful security breaches so that the incident response team can contain and clean the breach.

6 Intelligence Aggregation

6.1 Intelligence Aggregation Overview

Gathering intelligence is obviously a key part of any Intelligence-Based Security Strategy. Intelligence can come in a number of forms and from a range of sources depending upon the threats that you want to identify and protect against.

A few of the sources that you need to consider when aggregating your Intelligence includes:

- Intelligence Sources
- Open Source Intelligence
- Human Intelligence
- Counter Intelligence
- Internal Intelligence

This list is aimed at providing you with an insight into the range of intelligence sources that are available and should be customised for each organisation.

6.2 Intelligence Sources

There are a wide range of intelligence sources and types of intelligence that you can gather depending upon what you have included in your Intelligence Strategy.

You may wish to identify phishing websites related to your organisation, compromised systems within your network that have been added to a botnet, hackers planning attacks against your business, or internal rogue employees.

6.3 Open Source Intelligence

Open Source Intelligence (OSINT) is gathered from publicly available systems. This may include security feeds such as vulnerability feeds, exploits feeds, public intelligence feeds, and public comments in blogs, social media, or IRC channels. It also includes public statements by Hactivist organisations, such as Anonymous or LulzSec.

Commercial intelligence feeds are also available for purchase, typically on an annual subscription basis. These feeds are managed by companies who have made an investment to ensure that they have a net cast across the Internet, their threat rating algorithms and data is relatively accurate, and therefore, can be a valuable asset.

An example of the data that you can retrieve from these services is demonstrated below, where an IP address is provided and details relating to the threat level associated with that host are returned, such as the Risk Score, Country Risk, and type of threat, in this case being a part of a Botnet.

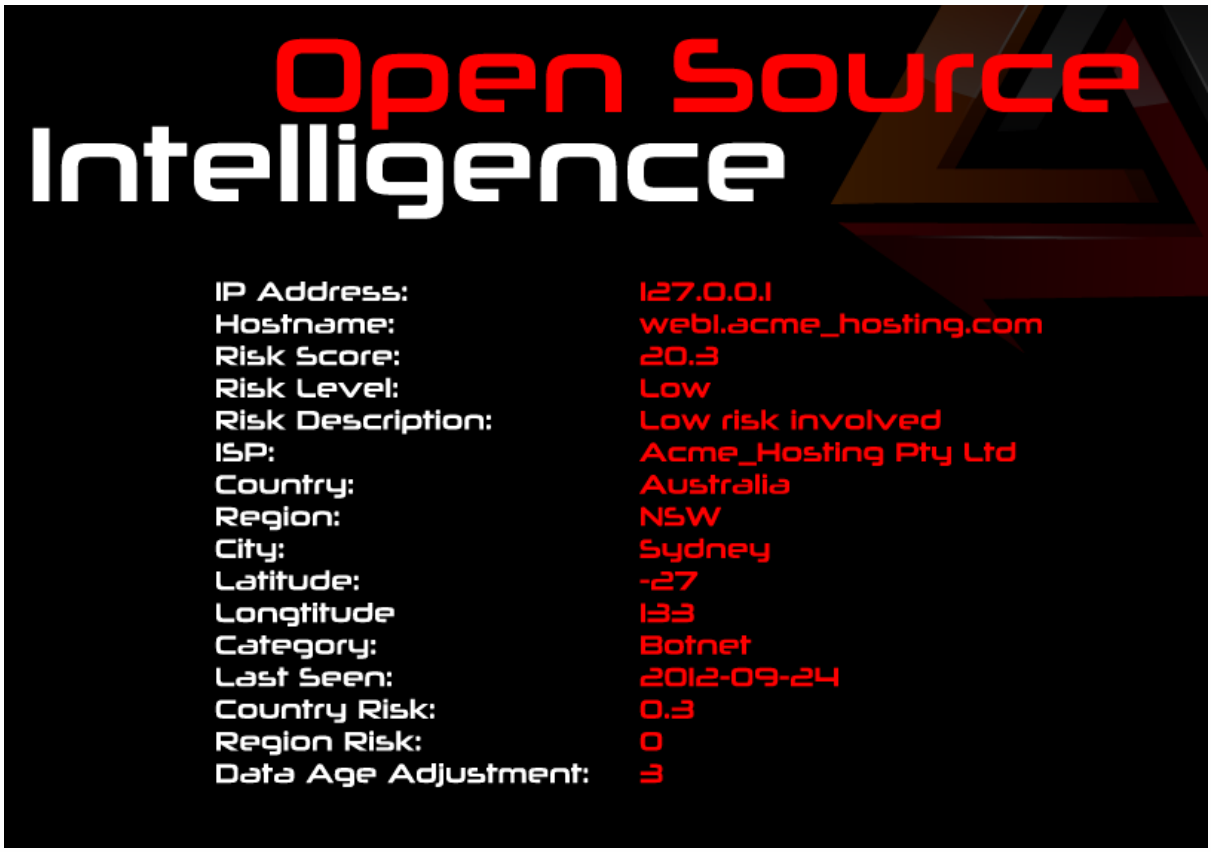


Figure 2 - OSINT data gathered from a reputation service

6.4 Human Intelligence

Not all threat data is easily available online and cannot simply be captured using automated techniques. If a deeper level of Threat Intelligence is required, then Human Intelligence (HUMINT) can be used to manually extract data from relatively difficult places.

This may involve setting up fake identities and accounts, as well as building up a reputation for that fake identity, in order to be granted access to systems and forums used by closed groups.

This type of intelligence gathering is typically more targeted towards specific groups and information, and requires a far greater investment in time and money due to the various hurdles that must be overcome to gain access to the target information.

Depending upon your business security requirements, Human Intelligence may or may not be included within your Intelligence-Based Security Strategy.

6.5 Counter Intelligence

Counter Intelligence (CI) is typically designed to deceive the attacker in order to send them down the wrong path to protect your valuable systems, or to find out more information about them.

A common type of Counter Intelligence when discussing Intelligence-Based Security is the use of a Honeypot. Honeypots expose a range of seemingly vulnerable or sensitive services to the attacker that are designed to entice them in so that you are able to monitor and classify the attacker.

Some of the commercial intelligence feeds are run by companies who have thousands of Honeypots spread across the Internet that have been designed to identify sources of attacks in order to classify malicious IP addresses, countries, and regions.

Some of the features in our online offering “Threat Analytics” (www.threat-analytics.com) fall within the Counter Intelligence space. When an unsuspecting rogue user visits your website, Threat Analytics will automatically analyse and classify the attacker, including the types of attacks that they like to perform, a trace of when and where they have performed attacks, where they are physically located, their operating system type, web browser type and version, browser plugins, and various software versions that they are running, amongst other things.

The aggressive portion of Counter Intelligence is known as “Offensive Counter Intelligence”. This is where you probe or attack the hacker in order to gather more detailed information about them.

Threat Analytics also has an Offensive Counter Intelligence component to it. When a malicious user is detected, Threat Analytics can deploy a “Threat Analytics Agent” back to the attacker’s web browser. This agent can be configured to perform a range of actions, such as probe the attacker for more information to gain a more detailed fingerprint, close the attacker’s web browser, disable the web form that is being attacked, create an overlay over the page containing a custom banner, or redirect the attacker to another website or web page.

These options are available within the Free Membership of Threat Analytics. More agent modules become available as you increase your membership level.

The configuration page for the Threat Analytics Agent is demonstrated below, where you drag and drop the displayed modules onto your policy on the right hand side.

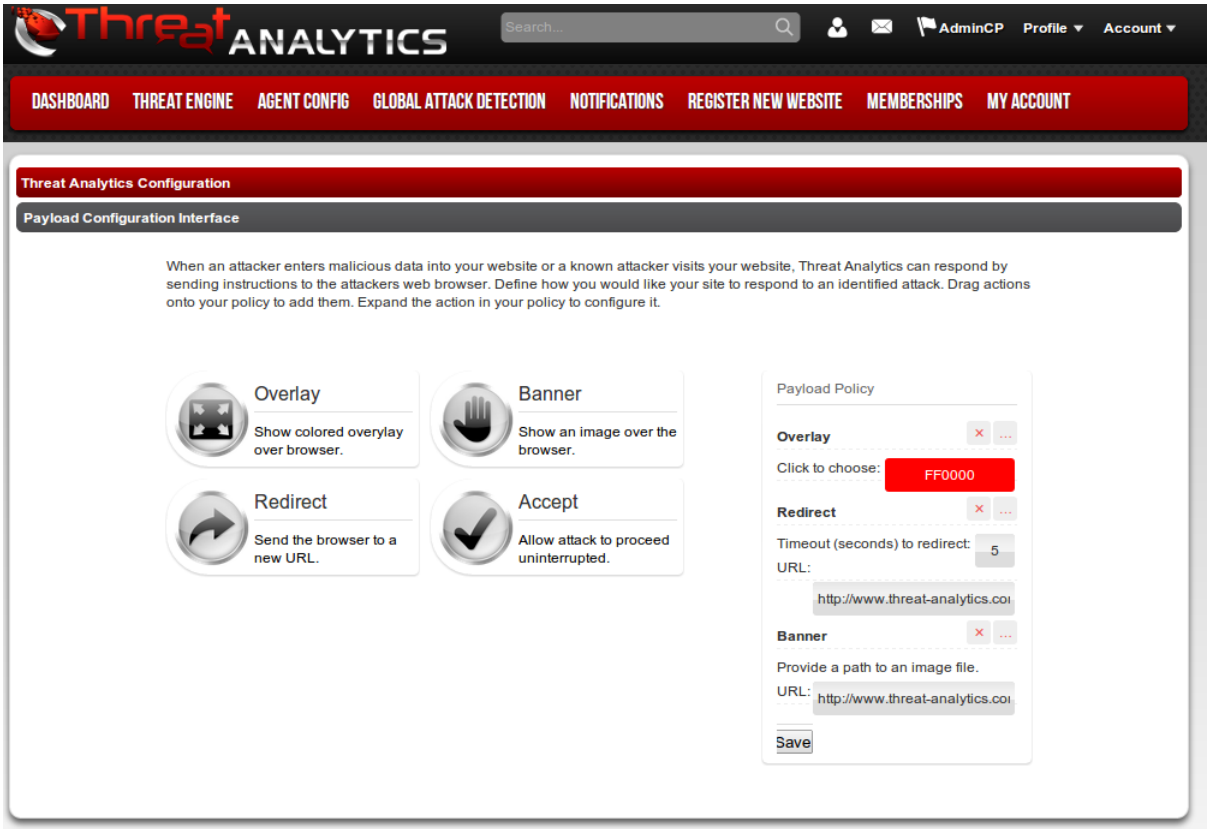


Figure 3 - Threat Analytics Agent Counter Intelligence configuration

6.6 Internal Intelligence

Since a large number of security breaches occur via phishing attacks, your employees are often the gatekeepers to your internal network, and unfortunately, are often the most vulnerable. If your employees are trained up in being able to identify phishing emails and social engineering attacks, as well as also know who to contact when a suspicious email is identified, then your employees are a valuable piece of intelligence within your internal environment.

Threat Intelligence has found that performing a Social Engineering Penetration Test that includes a phishing component is a very effective Security Awareness education exercise. This type of engagement doesn't go without upsetting a few people, but as long as this is expected and managed, your employees will experience an actual attack and can see the devastation that results.

In our experience, we have found that the number of employees that fall victim during subsequent annual phishing engagements can drop to as little as 10%. This dramatically reduces the attack surface of your organisation and reduces the risk of your internal network becoming remotely compromised.

SIEM solutions are another great source of Internal Intelligence. Traditional SIEM solutions aren't intelligence products; however, they typically host a lot of useful information that

intelligence can be extracted from. Unfortunately, SIEM solutions are often found to be missing a lot of data, or simply just don't exist within many organisations.

Searching your network for Indicators of Compromise is also a source of Internal Intelligence, since any findings provide you with visibility into potential security breaches, non-standard activity, and potential threat actors within your internal environment.

Internal Honeypots can also provide an insight to internal malicious activity, just as they are used on the Internet to identify and profile hackers to gather intelligence.

7 Threat Analytics

7.1 Threat Analytics Overview

Although this section is named “Threat Analytics”, it isn’t referring to our product Threat Analytics, but to the general analysis of threats.

At this stage, you have successfully correlated and aggregated your intelligence sources so that you have threat data for both external and internal threats. You now need to turn this data into actual intelligence through analysis.

A few of the components that you need to take into account when analysing your threat data includes:

- Reputation Services
- Hacker Profiling
- Internal Threats
- Intelligence Sharing
- Threat Intent

This list is aimed at providing you with an insight into the range of intelligence analysis techniques and areas that you need to consider and should be customised for each organisation based on the type of data that has been gathered, the supporting intelligence systems and features, as well as the types of systems or applications that are being protected.

7.2 Reputation Services

Reputation Services, also commonly referred to as Intelligence Feeds, provide you with an insight into whether the connecting IP address is likely to be trustworthy or not.

During your Intelligence Aggregation phase, you have pulled together a number of sources of intelligence to base your decisions. A few questions that are likely to arise very quickly include:

- Which Intelligence Feed do you trust when one feed says that the IP address is trustworthy and another feed says that it is malicious?
- What if the IP address has rotated its ownership and is now owned by a trusted user but the IP is being marked as malicious?
- What if the malicious user has changed IP addresses or is using various techniques to hide their IP address, and is now being marked as trustworthy?
- Is it the IP address that is malicious or is it the user?

- Have you aggregated enough intelligence feeds to make an accurate informed decision to make these distinctions?

This comes down to analysing the various intelligence sources to identify what they claim to provide, their strengths and weaknesses, and why they are classing the IP address as malicious.

In many cases, it is safe to assume that if the IP address is marked as trustworthy or "low risk" then the source of the Intelligence Feed has simply not come across that IP address before, or at least not in a while.

This doesn't mean that you can trust the IP address. It may be an indicator that you don't have sufficient intelligence sources to make an informed decision.

To demonstrate this concept, Threat Intelligence obtained a sample of hosts that Threat Analytics detected as being malicious, and manually confirmed them to be malicious via our Threat Engine. A comparison was performed to identify if these hosts were known to a commercial Intelligence Feed. It was found that none of the known malicious hosts were flagged as malicious by the commercial intelligence feed.

Now, this doesn't in any way mean that the commercial feed isn't of a high quality. What it means is that the two feeds have different purposes and techniques of identifying malicious hosts or users. This simply demonstrates the need for multiple Intelligence Feeds, or ensuring that you select feeds that are designed to identify threats detailed in your Intelligence Strategy and that are relevant to your business.

If the IP address is marked as malicious, then you need to understand why it is being marked as malicious:

- Is it a TOR node?
- Is it a part of a botnet?
- Is it a known open proxy?
- Is it a host that is known to be infected with malware?
- Is it a web server running a phishing website?
- Is it a host that uses peer-to-peer file sharing?
- Is it because the connection is originating from a high risk region within a high risk country?
- Is it an IP address that is previously unknown but the user has been mapped to a known hacker?
- Is it an internal IP address doing malicious activity on a DHCP network, and has the DHCP lease expired meaning that the IP may no longer be allocated to the offending host?

Depending upon the system or application that is under threat, each of these cases may or may not require intervention.

7.3 Hacker Profiling

Many Reputation Services use IP addresses as a primary key. In some cases this is valid, and in other cases it produces incorrect data and threat levels that lead to false-positives or false-negatives.

Hacker Profiling allows you to proactively gather information about the attackers, and in the case of our online Threat Analytics product, it can actually track the hackers around the Internet using a number of proprietary techniques.

This allows you to break out of the restriction of classifying IP addresses, and allows you to enter into tracking malicious users across a range of IP addresses. If an attacker connects to your website via TOR, then their actual IP address is hidden. Not only that, their requests may also exist out of a large number of TOR exit nodes with their own unique IP addresses.

Threat Analytics allows you to track the hacker and create a more accurate profile within the scope of what Threat Analytics was designed to do. This information can then be correlated with other Intelligence Sources to get an even more accurate picture of the actual threat against your organisation from this user.

7.4 Internal Threats

Many organisations believe that their internal users are a more critical risk than external attackers, and therefore, Internal Intelligence is a key component to identifying threats against your organisation.

This is completely justified when you realise that a technically skilled internal attacker is able to escalate their privileges from a standard user through to Domain Administrator access within a day. This provides them with the ability to dump and crack every person's password within your company in order to gain access to any other system, device, application or database.

When you identify a technically skilled attacker who also has detailed knowledge of how your business processes operate, then you have come up against a primary target that has the capability to defraud your company and bypass any security checks that will get them caught. In this case, you need to either hope that they never turn rogue, or tune your intelligence gathering to capture Indicators of Compromise (IOC) so that you can contain any security breaches or fraudulent activities.

A common security breach that occurs internal to organisations is when a contractor turns rogue because they have had their contact cancelled in a manner that they deem unfair or were simply unhappy with the circumstance that it happened. This often leads to administrative passwords being changed to prevent your company from accessing your own systems and applications, or even more malicious where virtual machines are simply deleted to cause an immediate and significant impact to your organisation.

This circumstance tends to lead to the requirement of a digital forensic investigation to determine if the rogue employee or contractor has left any backdoors within the internal systems, and to identify if they have performed any other actions.

7.5 Intelligence Sharing

At this point you have a significant amount of intelligence data and threat analysis internal to your organisation. If you think about it, other organisations that are maturing their Intelligence-Based Security controls will also have a significant amount of data and experience. Discussing and sharing this information with each other can be quite beneficial to both parties.

But how much data do you want to share, and with whom? You almost certainly do not want to publish your data on the Internet for everyone to see; however, if no one shared any data then the amount of intelligence available to your organisation and other similar organisations will be more limited.

You may want to base each decision on how sharing the data will affect the value of the data. If you suddenly disclose that you have detected a malicious IP address or user, and that information gets published, then you may tip off the attacker who you are trying to investigate.

Similarly when submitting malicious code to third party websites for analysis, you need to be mindful of what happens after you have submitted that piece of malware. Often the malware is sold to anti-virus vendors who then create a signature to mitigate against infections. If the attacker's malware suddenly starts getting caught by anti-virus before your investigation has completed, then you may find that they create a variant, which may hinder your investigation efforts.

Sharing information with CERTs, law enforcement, Governments, and ISPs is common practice, especially when you need their help to shut down an ongoing attack.

7.6 Threat Intent

The analysis of the intelligence data should also attempt to gain an insight into the intent of the attacker. Based on the intelligence that has been gathered, you may want to ask yourself questions such as:

- Does it appear that the attacker tends to probe for vulnerabilities for a bit of fun, or is this the beginning of a larger attack?
- Does it appear that the attacker tends to exploit vulnerabilities within organisations, and then publish their successful breaches on publicly available defacement archives, which can lead to reputational and financial damage?

- Does it appear that the attacker is a known cyber-crime offender who is after credit cards or large amounts of personally identifiable information (PII)?

The results of this analysis will determine if further actions should take place.

8 Operational Intelligence

8.1 Operational Intelligence Overview

Once you have performed an analysis of your intelligence data, whether via automated and/or manual techniques, you now need to create Operational Intelligence that produces actions that should be taken to close down the threat.

A few of the components that you need to take into account when creating Operational Intelligence include:

- Cyber Kill Chain
- Course of Action
- Threat Dissemination
- Proactive Defence

This list is aimed at providing you with an insight into what each stage involves at a high level and should be customised for each organisation.

8.2 Cyber Kill Chain

A "Kill Chain" describes the phases of an attack. When talking about cyber-attacks, we refer to this as the "Cyber Kill Chain", which was a concept put forward by Lockheed Martin (http://www.lockheedmartin.com.au/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf). By understanding the Cyber Kill Chain, we can gain an insight into the indicators that we must look for in order to identify a pending attack.

The phases of a common Cyber Kill Chain are detailed below. It should be noted that not every attack follows this path, and therefore, indicators for each phase may not exist.

- Reconnaissance
- Weaponization
- Delivery
- Exploit
- Installation
- Command & Control
- Actions

The further an attacker is allowed to progress through the Cyber Kill Chain, the more information they have about your organisation and the target system, which ultimately increases their exploitation success rate, and subsequently increases the impact on your organisation.

This means that the earlier that we can detect a threat the less likely they will be successful in compromising your organisations systems, applications or data.

As an example, a port scan across your network border may be an indicator of an attack that is currently in the "Reconnaissance" phase. This attack may then progress to performing vulnerability scans against your infrastructure or spider your website to extract information such as email addresses of employees.

The next set of phases will depend upon the information that was able to be gleaned during the Reconnaissance phase. If critical vulnerabilities within your external systems or content management systems were identified, then you may find that exploitation attempts will be performed, else it is likely that phishing attacks may be chosen.

If you are aware of the public information that your company has on the Internet, including the information contained within your employees personal online and social networking accounts, as well as the state of your systems' and applications' security, then you should have a descent idea of how the next phases of the Cyber Kill Chain will progress.

8.3 Course of Action

Once you have identified a threat, whether that is through Cyber Kill Chain indicators or through Intelligence Feeds, you need to now determine a course of action to dissolve the threat.

To free up limited resources and to increase the value of your new Intelligence-Based Security Framework, many of these actions would ideally be automated allowing your team to focus on locating other threat indicators and identify trends in the threats.

Unfortunately, this depends upon the type of threat that you are facing, your confidence in the intelligence sources, and the supporting intelligence systems and architecture that you have in place.

Your courses of action will evolve over time as your Intelligence Strategy matures, your intelligence systems mature, and your intelligence capabilities mature.

8.4 Threat Dissemination

Threat Dissemination is where you inform relevant parties to a pending threat. This may be your incident response team, the executive team, business partners, or across all of the employees in your organisation.

Let's say that you have been able to identify that there is a higher than normal threat level of a phishing attack. This may be because indicators have been revealed due to an attacker brute forcing a list of email addresses from your corporate website, or because your intelligence processes have revealed that a phishing site relating to your organisation or industry has been located.

Your course of action may be to disseminate information to all of your employees that there is a higher than normal threat level for a phishing attack, and that all employees should keep an eye out for suspicious emails. If a phishing site exists, then a screenshot of the site may also be provided so that it can be easily recognisable.

This Threat Dissemination is an attempt to dissolve the threat before it begins.

8.5 Proactive Defence

Depending upon your Intelligence Strategy, you can automatically block threats or increase the security associated with threats for some circumstances.

This may be through automatically injecting new firewall rules to block untrusted IP addresses from connecting for 24 hours, or similarly inject new IPS or WAF rules.

Intelligence can also be integrated into web applications to increase their security, and reduce risk and fraud. For example, a web user may be attempting to perform a financial transaction within your eCommerce application, but their IP address is known to be infected with malware. This increases the risk associated with fraudulent activity within their account, and therefore, you may hold the transaction for further analysis, or inject a two-factor authentication control to increase the trust associated with the transaction.

Advanced Persistent Threats (APTs) are typically carried out over a period of time, meaning that locating these threats will be an ongoing process to identify, track, and react to recurring threats. In this case, your proactive defence will be a combination of both manual and automated means. As you continue to close down threats and attacks, APTs will use new techniques or target different systems in your organisation to achieve their end goal.

9 Managed Intelligence Summary

9.1 Summary

Intelligence-Based Security arms you with a wide array of defence techniques that are not available with traditional security systems. Some of these include:

- The visibility of pending threats against your organisation,
- The ability to proactively shut down threats before they have even been launched,
- The ability to track hackers and malicious IP addresses so that you can control who is accessing your systems, applications and data,
- The visibility of threats internal to your organisation and the ability to mitigate devastating attacks,
- The intelligence data required to identify threat trending so that your organisation is equipped to protect itself against emerging threats and attack techniques,
- The integration of business systems with intelligence data in order to prevent business specific risks, such as eCommerce fraud.

To successfully integrate intelligence into your security program, your Intelligence Strategy should be developed so that it contains a roadmap that details the systems you plan to protect, the intelligence techniques you plan to implement, the capabilities that you plan to develop, and the timeframes of when each technique will be implemented.

Intelligence sources should be identified, aggregated and validated, and should provide intelligence data that is related to the types of threats that you have defined in your Intelligence Strategy.

Once data is being gathered from your intelligence sources, they should be analysed to identify threats to your organisation, the validity of these threats, and what the intent is of each threat. This analysis is then turned into threat protection actions that may be to disseminate information about the threat or to implement protection mechanisms to close down the threat before an attack has been launched.

This “Managed Intelligence Life Cycle” then feeds back into itself again to mature your Intelligence Strategy and controls, as well as morph them to prepare for the next generation of threats.

Threat Intelligence can help you define and execute an Intelligence Strategy specific to your organisation. Contact us on 1300 809 437 or email us at info@threatintelligence.com.

10 Managed Intelligence Enquiries

10.1.1 Enquire Now

To discuss Managed Intelligence Services and the development of an Intelligence Strategy for your organisation, please contact Threat Intelligence on 1300 809 437 or email us at info@threatintelligence.com.

We thank you for the opportunity to provide our specialist security experience to help you protect your business.