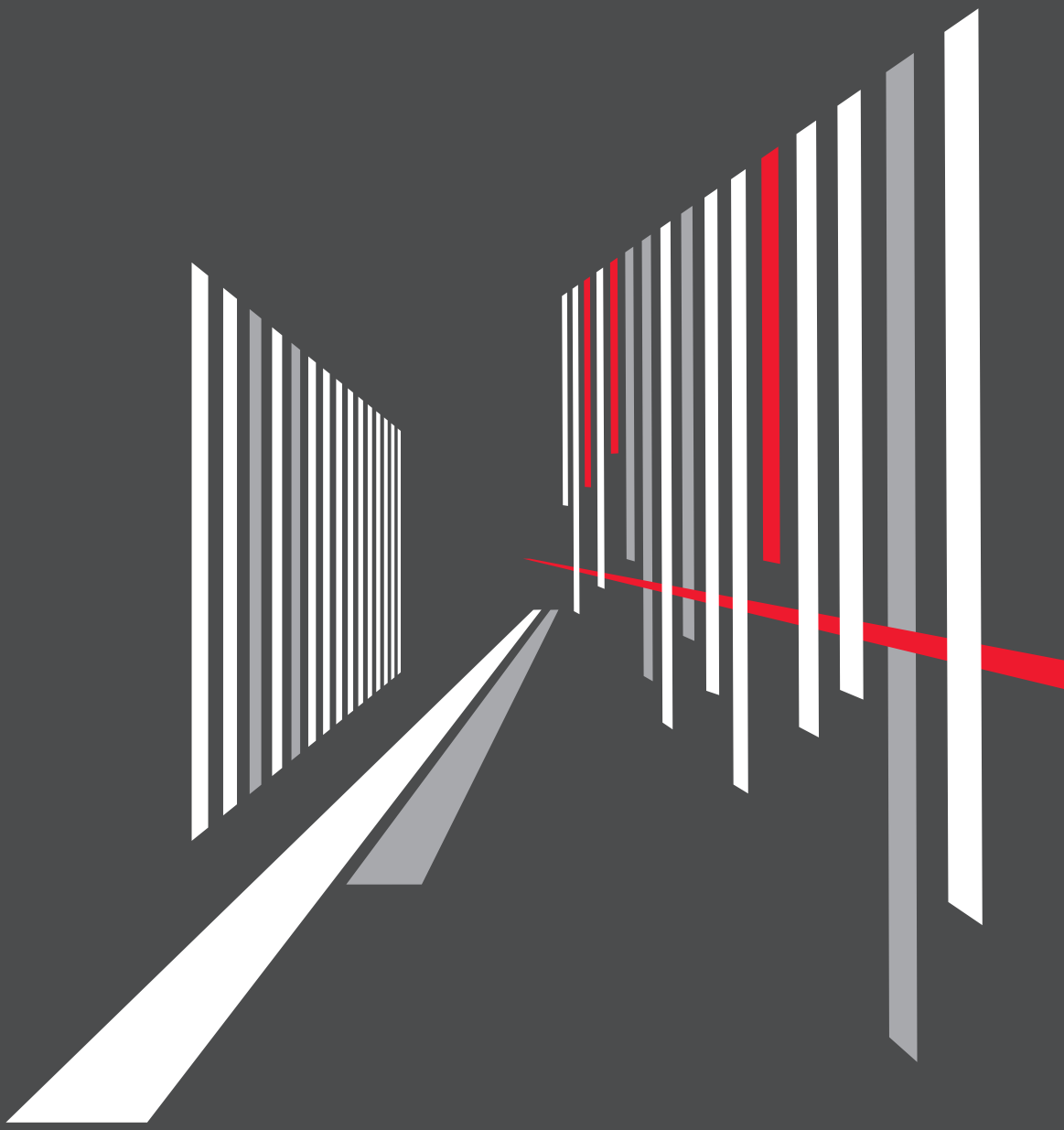
context



Integrating Threat Intelligence

Defining an Intelligence Driven Cyber Security Strategy

Supported by:

CERT-UK

CPNI®
Centre for the Protection of National Infrastructure

CONTEXT would like to acknowledge the help and support of CPNI and CERT-UK in researching this topic and producing the accompanying products.

Contents

1 Executive Summary

The purpose of this report is to provide guidance on integrating threat intelligence into cyber defence activities within your organisation. It will discuss the steps towards developing an intelligence driven security strategy, which will include: data acquisition, consumption, analysis, and distribution.

In solitude, conventional procedures, like producing attack signatures, are no longer sufficient in assisting security teams to prevent threat actors from gaining access to networks. This is because the tactics, techniques, and procedures used by sophisticated threat actors are evolving quicker than ever before.

Threat intelligence provides the context which allows us to better understand the motives and overall capabilities of the adversary. If utilised and implemented properly, through the development of a clear strategy, threat intelligence can help us to predict and prevent future attacks, whilst better defending us against existing ones.

But threat intelligence is only as good as the data that feeds it. It is important to implement a strategy within your organisation for the effective deployment of network devices and host applications that will collect this data.

In order to enhance data collected internally, an important step toward better protecting your network is to consume and act upon threat intelligence obtained via a third-party. The ideal is to integrate this intelligence with traditional security devices and applications within your network. However, this is an emerging area. Considerable effort is being made in the standardisation of threat intelligence formats and increasing collaboration across the security community will help drive this forward.

The continued sharing of threat intelligence and collaboration within the security community or, more specifically, within a trusted community will make an attacker's objectives increasingly harder to achieve. Attackers will be required to expend more resource and time reinventing their techniques in order to continually bypass intrusion detection systems. This extra effort required by attackers may deter their activity entirely or significantly slow the process of obtaining or re-establishing access.

Being able to interpret threat intelligence and how it relates to your organisation specifically is the ideal. In order to achieve this, a security team that is able to conduct their own analysis of threat intelligence obtained from both internal and external sources is required. This will benefit the organisation through the provision of tailored actionable intelligence relevant to your industry sector, geographical area or supply chain.

2 Introduction

> ***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.***
> ***Source:*** *Gartner, Definition: Threat Intelligence, 2013*

Threat intelligence is a term used to describe a product that can be acquired by an organisation and also an analytical practice that can be followed.

In simple terms, a threat intelligence product is akin to how anti-virus software monitors activity on a computer. For anti-virus software to detect malicious activity, it regularly downloads definitions distributed by the provider that specify what malicious activity to look for. If malware is found on a computer an alert is presented to the user, along with the malware's name and ways to remove it.

Threat intelligence similarly defines what malicious activity to look for, but its scope and use is much broader. Expanding the concept to the wider network, threat intelligence can be applied not just to a computer but to other security devices, such as firewalls and intrusion detection systems, to block or detect malicious activity across the organisation.

Where threat intelligence differs significantly from traditional products like anti-virus is the context in which the intelligence is held. Any definition of malicious activity is built around a higher-level concept, such as who the attacker was or what previous hacking campaigns the malware has associations with.

2.1 The Threat

A deep understanding of the threat helps to better protect an organisation. Any credible threat must have three attributes[1]:

- Intent;
- Opportunity; and
- Capability.

The intent will depend on the type of actor. For example, hacktivists may seek to disrupt a web service in order to send a politically motivated message. An organised crime group may pursue credit card details for financial gain, or a foreign intelligence service may seek to acquire intellectual property in order to strengthen its economy.

The opportunity defines the availability of an entity for exploitation. For example, an actor may identify a vulnerable server on a victim network, or use an upcoming event to increase the likelihood of an employee opening a spear-phishing email.

The capability describes the resources available to an actor in order to achieve their goal. These resources include the availability of finances, skill and people.

Whilst there may be many threat actors with the intent to attack, without the appropriate level of capability and the right opportunity they will be unlikely to succeed.

2.1.1 Threat Actors

A threat actor, also described as an adversary, is an individual or group with the intent to conduct attacks against a target. Some threat actors may have a large target base and conduct attacks indiscriminately, whilst others may seek to target specific individuals, organisations, industry sectors, or geographical areas.

Collectively, the threat that all actors pose is often referred to as the "threat landscape". Below is an outline of the most prominent threat actor groups that make up the threat landscape.

Hacktivists

Individuals or groups who use computers in an attempt to achieve political change. Activities include attacking websites or illegally accessing a computer network.

Hacktivists have proven that even relatively uncoordinated groups with only a basic level of technical capability can cause significant disruption to major services.

Hacktivists predominantly seek to further their cause through disruption of popular online services.

[1] Also referred to as *motive, opportunity and means*

Organised Cybercrime Groups

Specialist criminal groups who target individuals, small businesses and large corporate networks to steal information in order to profit from the compromised data[2].

Cyber criminals are becoming increasingly advanced, now employing tools and techniques once used exclusively by nation state actors. Whilst the National Infrastructure may not be a specific target, an organisation may become a victim through the actor's wide and indiscriminate targeting.

State-sponsored

State-led or state-directed attacks against an organisation, be that public or private.

An increasing number of states see the benefit of conducting cyber espionage to acquire highly-valuable foreign intelligence and intellectual property, often with few repercussions. Those nations who do not have the technical capability can now purchase commercial offensive services.

Insider threat

Current or former employees or associates whose level of authorised access and trust is misused in order to obtain access to systems and information for the purpose of espionage, sabotage or other objectives.

The insider threat poses one of the greatest risks to all organisations, including those that are part of the National Infrastructure. Either co-opted (most likely by one of the groups above), self-motivated or unwitting, there are numerous examples that have resulted in compromise.

2.1.2 Attribution

Attributing a compromise to a threat actor can be a difficult task. Threat actors may use a multitude of techniques to help anonymise their activity. This may include the use of compromised third party infrastructure to route communications between the attacker and victim machine (or machines) across the globe. There may also be political or commercial sensitivities surrounding the disclosure of the attribution.

The case for and against the efforts to attribute activity is a much-debated subject, with some in the security community arguing that it serves little benefit. The key point, however, is that any intelligence resulting from the analysis of malicious activity, both past and present, should be grouped and related where possible to help provide context and to better understand attacker capability and motives.

If this analysis leads to attribution then this can only assist in helping the defender better understand attacker characteristics and potential intent. It can also help inform an organisation's strategy for dealing with a particular threat group. Moving beyond

[2] Taken from the National Crime Agency definition

this, law enforcement agencies seek attribution for prosecution purposes, but while there has been decisive attribution and accusations made across the threat landscape toward foreign states; a successful prosecution has yet to be realised.

2.2 The Threat Intelligence Model

Threat intelligence as an analytical practice is suitable for organisations with mature security processes and an appropriate level of resources, such as people, skills and technology.

There are elements of threat intelligence that have existed for some time within the security community. For example, malicious indicators are recorded as part of traditional incident response practices following a network compromise.

An indicator, one type of threat intelligence, is a piece of information associated with a malicious event. For example, an analyst may derive an indicator from a malware sample found when responding to an incident. It may be possible to characterise the malware sample through its filename and where it is installed on a victim's computer, at the most simple level.

An indicator may not necessarily be malicious itself but relate to the use of a legitimate system, resource or technology by an actor to achieve their goals.

A threat model can represent attack patterns or behaviour, as shown in Figure 1 below. A threat actor will employ a series of steps to achieve their goal of compromising a network. An individual step in itself may appear legitimate, but collectively they form an attack pattern. A series of indicators may be required to define the activity and an alert will only be raised if all or a number of these are detected.

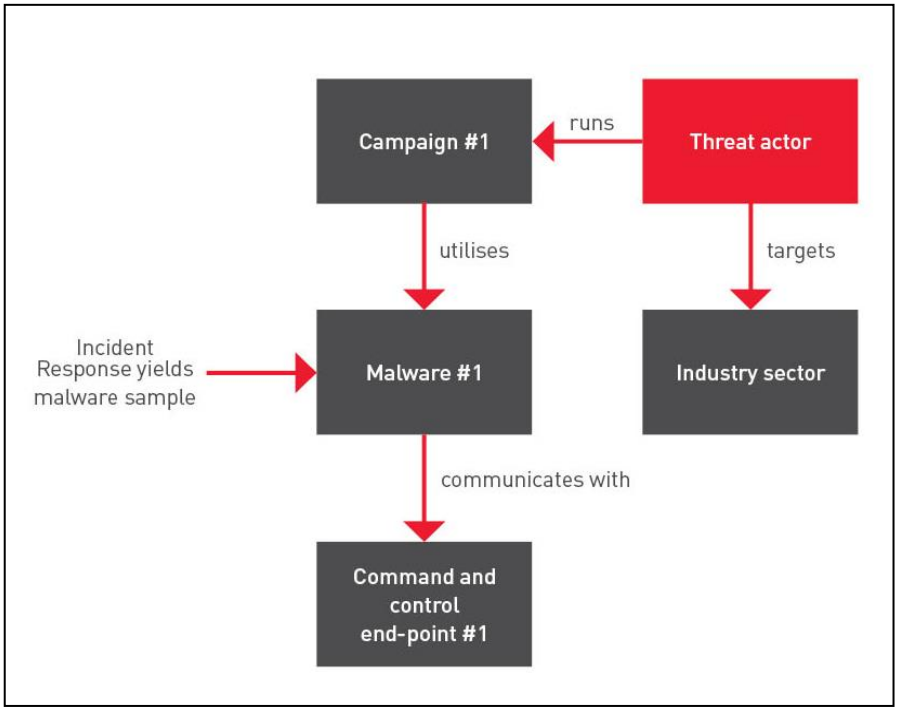


Figure 1 Example of a threat intelligence model

An indicator can be translated into a format that can be understood by traditional security appliances and used to prevent or detect the same activity in the future. For example, an analyst may discover the domain used by a malware sample to communicate back to an attacker. This indicator can be translated into a firewall rule to block access to the malicious website from computers within the organisation's network.

These indicators have traditionally been stored informally in formats such as tickets, documents or spreadsheets and have remained within the scope of the specific incident in which they were identified. As a result, a subsequent attack by the same attacker may not be linked to a previous compromise and any response may only remediate the specific malware rather than understanding that it is part of a wider campaign.

Threat intelligence is an evolution of this process. It takes from and is influenced by many security disciplines, from risk assessment to remediation. It defines a new construct from which intelligence relating to threats affecting an organisation can be built upon and shared. It provides context of a compromise in relation to an attacker or campaign. However, the intelligence needs to be actionable, meaning that it needs to be relevant to the security controls and risk posture of an organisation. This can help track compromises and potentially predict, detect and defend against future attacks.

2.3 Types of Threat Intelligence

Threat intelligence can cover a wide range of attributes that define a threat or threat actor. It can describe an actor's tactics, techniques and procedures (TTPs), their historic campaigns, linked threat groups, the vulnerabilities that they utilise in order to exploit a system, and much more.

Threat intelligence can be subcategorised into being either tactical or strategic. However, this is only one representation of intelligence and there are other models that can be followed. The definitions presented in this section describe the most commonly used amongst the security community.

The *actionable timeframe* field within each section below describes the timeframe in which the intelligence is able to describe an aspect of an actor's activity and provide a realistic window within which one is able to act upon it. For example, knowledge that an actor made use of a particular Command and Control endpoint may be short-lived as they seek to hide their tracks. However, knowledge that the actor's motives are to acquire intellectual property from a particular industry sector is more likely to be applicable long-term.

2.3.1 Tactical intelligence

Overview	Tactical intelligence is a collection of indicators in the context of a threat actor, threat type or campaign. Where possible, an indicator should be given context to help build awareness of how it features in the wider campaign, relates to the threat type or helps identify the threat actor. Tactical intelligence can be used to describe observable behaviour of a process or actor during a compromise, often conveyed via indicators of compromise or documented attack patterns.
Produced by	To produce intelligence requires some level of interpretation by an analyst[3]. For example, an analyst may produce tactical intelligence following a compromise through forensics within the context of an actor's campaign.
Actionable timeframe	Some threat actors are more concerned than others about their operational security (OPSEC). A threat actor who maintains good OPSEC is one that changes their capability frequently so as to help evade tracking and detection. For example, as the same sample of malware is used against multiple victims, analysts are able to build a pattern of activity to track and defend against future attacks. As a result, actors, especially those who are more advanced, will seek to modify attributes of their capability frequently to help prevent detection. This may change with each campaign or even with each victim. For example, by changing the Command and Control infrastructure to which a sample of malware beacons, may help the malware evade a firewall where blocks have already been put in place. As a result, the actionable timeframe for this type of intelligence may be short.
Used by	Tactical intelligence can: • Feed into security devices to provide real-time alerting, defence and monitoring; • Feed into a security information and event management (SIEM) tool to enrich and correlate log data from security devices; • Build an awareness of a threat actor, threat types or campaigns that may affect an organisation as part of an intelligence gathering and analysis process; and • Determine trends of an attacker to build into strategic intelligence.

[3] Some security devices can create unanalysed threat data automatically through a heuristic-based approach. Here, security devices look for and flag up suspicious activity. However, this data still requires analysis to validate and provide context before producing intelligence.

Listed in the table below (Figure 2) are examples of the tactical intelligence that could be obtained from a threat intelligence feed or from analysis during an incident:

Network	• Email address used in a spear-phishing campaign; • URL used to host an exploit and malware; • IP address of Command and Control infrastructure; or • Network signature of malware communication (e.g. beaconing).
Host	• MD5 hash of malware or associated files; • File location of malware; • Registry key used to run malware at system start-up; or • Vulnerability used to exploit a web browser.

Figure 2 Examples of tactical threat intelligence

A distinction is made between tactical threat intelligence and threat data. Threat data is tactical threat intelligence stripped of its context. Threat data can be fed into security devices such that if malicious activity is detected, an association can be made back to the tactical intelligence from which it was derived.

2.3.2 Strategic Intelligence

Overview	Strategic intelligence can cover an actor's: • Social, political, economic and cultural motives; • Historic campaigns and targeting trends, such as industry focus; and • Technical capabilities.
Produced by	Open source information such as; geo-political reporting, industry whitepapers. In addition, trends and patterns inferred from tactical intelligence.
Actionable timeframe	While the tactical nature of attacks by a threat actor may change frequently, the motives that drive a threat actor and their capabilities will change less frequently.

Used by	Security teams to: • Develop a deeper understanding of their adversary; • Proactively plan defence strategies; and • Influence risk-based decision-making based on known attack vectors and sensitive business operations and data.
	Strategic intelligence may include: • Information that an actor is targeting a particular sector for the purpose of intellectual property theft; • Use of malicious links within a spear-phishing email; • Use of a particular exploit; or • Use of a particular malware toolset.

Figure 3 Examples of strategic threat intelligence

2.4 Proportionality

The integration of threat intelligence into a security process should be appropriate to the organisation's risk posture, factoring into account the size of the organisation and the value of the assets it possesses. To build an understanding of the risk posture requires:

- A risk assessment of an organisation's systems, assets and information; and
- An assessment of which threat actors target an organisation's industry sector or geographical area.

For more information on risk and threat assessment, refer to section 4 Assess and prepare.

2.5 Use Cases and Benefits

The use cases and benefits of threat intelligence are particular to the situation in which it is applied and its quality. In general, however, threat intelligence can benefit many areas within information security, including:

- **Threat assessment and modelling:** A threat assessment is a process to identify which threats and attack types should be considered when hardening network devices, systems or implementing new security controls. Intelligence of a particular actor and their preferred technique for gaining access to a type of system can be used to bolster defences against similar attacks, such as employing two-factor authentication on sensitive systems;

- **Prevention:** Threat intelligence can help prevent or disrupt an attack by blocking malicious access to particular resources within the internal network or attempted communication with Command and Control infrastructure. For example, security devices, such as firewalls, can ingest threat data to monitor and block an attempt by malware to connect to an IP address known to be a threat actor's Command and Control endpoint. Within the internal network, it may be known, for example, that a threat actor installs a specific malicious toolset on a host to enable lateral movement around the network. Indicators that suggest its presence on a host, such as its unique file hash, can be added to a known bad list to prevent installation;
- **Detection:** Similar to the use case for Prevention, threat data can be applied to security devices in order to detect and alert on malicious activity, such as intrusion detection systems, firewalls and proxy servers;
- **Incident response:** Threat intelligence can help many aspects of the incident response process. For example, an analyst may uncover an indicator during incident response which they find to be associated to a particular threat actor by using their threat intelligence sources. The actor is known to use specific tools and techniques once they have compromised the network. The analyst can search for these indicators of the actor's wider tradecraft to determine the scale of the compromise. Intelligence can provide guidance on mitigation and remediation. Security events can be enriched with threat intelligence to provide context for security alerts. For example, if an email is found to be the initial infection vector for an incident, indicators in the email such as the sender's email address can be used to determine which threat actor or campaign it may originate from. The threat model for the actor or campaign can provide additional indicators that should be searched for and may provide mitigation or remediation procedures;
- **Research and analysis:** Broader threat intelligence gathering and analysis can discover and relate campaigns to build a deeper understanding of relevant threats. This activity is conducted internally and can produce more comprehensive indicators of relevant threat actor's TTPs; and
- **Exchange:** Exchange of threat intelligence within a trusted community can provide a wider view of actionable and relevant intelligence. Indicators found during incident response can be shared amongst the community.

2.6 Summary

Threat intelligence seeks to relate threat data, such as malicious IP addresses found during an incident, to intelligence of attack behaviour or patterns; on-going campaigns and ultimately, a threat actor. Without this end-to-end context, it can be difficult to track and understand the motives behind a compromise and the overall capabilities of the actor. This makes taking action to predict, prevent and defend against the success of future attacks extremely difficult.

Following a compromise, conventional incident response involves producing signatures for the detection and prevention of a similar attack in the future. This will only prevent the threat actor from regaining a foothold in the short-term. This is because they may only need to adjust their attack vector or malware slightly in order to regain access to

the target network, immediately circumventing the efforts of the defending organisation.

Utilising an intelligence model of a threat actor, or at least association to a series of campaigns, can provide an insight into their intent, opportunity and capabilities. As this intelligence is shared and awareness increases, the actor is forced to reinvent their techniques to continually bypass intrusion detection systems, and this extra effort can deter or significantly slow the process of regaining a foothold.

The remainder of the report is intended to assist information security professionals looking to develop an intelligence driven cyber security strategy, including; how threat intelligence can be sourced, stored, exchanged and utilised.

3 The Steps to an Intelligence Driven Strategy

In order to realise the full benefits that can be obtained from threat intelligence, a clear strategy is needed to determine the type of intelligence required; and where and how it should be applied. The high-level strategy shown in Figure 4 provides guidance for integrating threat intelligence into an organisation's security practice:

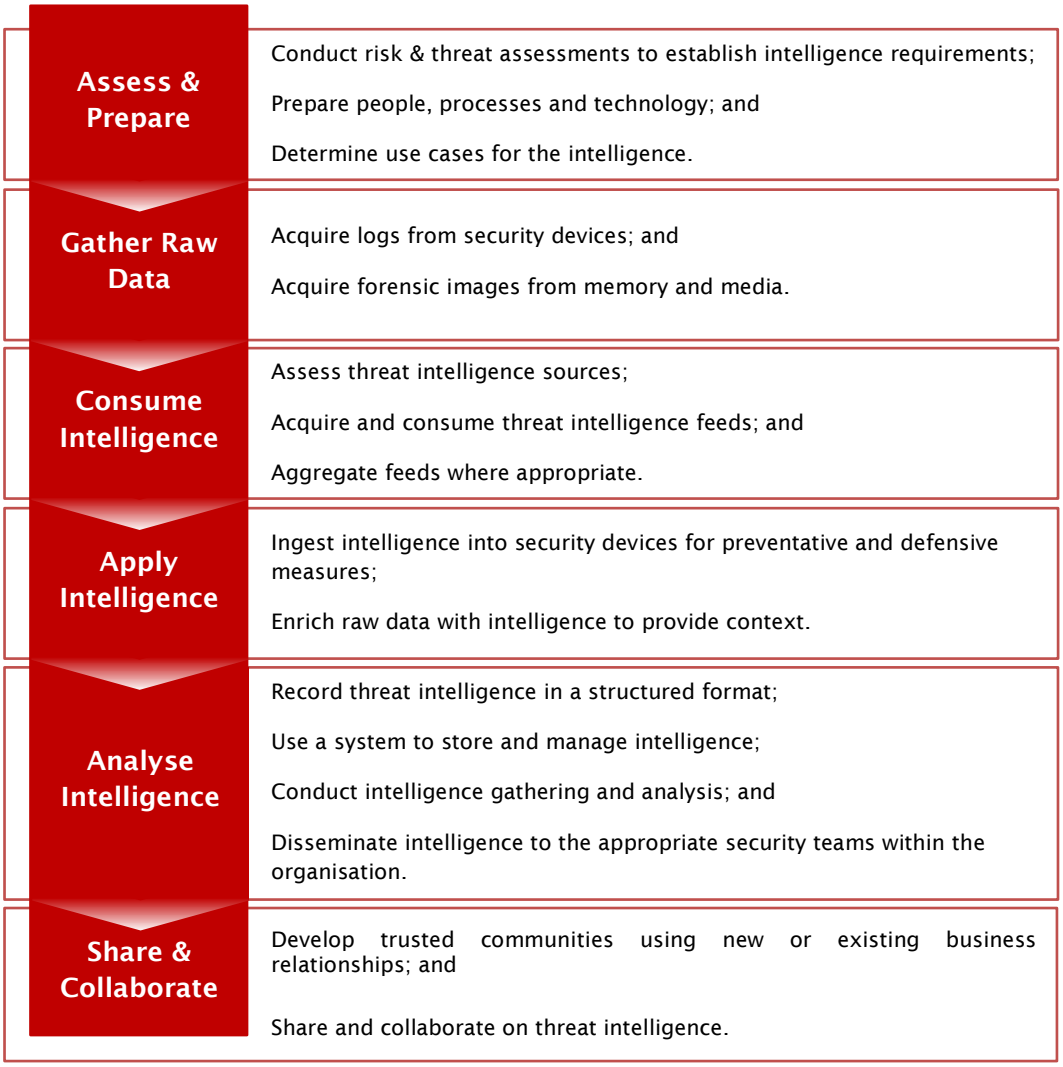


Figure 4 Intelligence Driven Strategy

The stages may occur concurrently and each stage may iteratively feed into others. For example, the intelligence analysis stage may identify a new threat type which helps to develop the threat assessment.

An organisation may not have the maturity, resources, or risk posture to achieve or require all stages. Guidance on each stage is given for a range of organisations and intelligence objectives.

4 Assess and prepare

4.1 Key Points

To accurately define the strategy, an assessment should be made of an organisation's risks and threats, the maturity of the security process, and the resources available.

Preparation should ensure that the correct people, processes, and technology are in place to integrate threat intelligence into an existing security strategy.

4.2 Risk and Threat Assessment

A risk assessment will help identify security gaps and vulnerabilities, and provide recommendations for threat mitigation and remediation.

A threat assessment will help identify the threat types and attack vectors against each asset.

OWASP[4] provide details on a number of commonly used risk models. CPNI provides recommendations on conducting risk assessments through the Critical Security Controls guidance[5] and Business Continuity Planning[6].

4.2.1 Inventory of Assets

It may not be feasible or appropriate to protect every asset in an organisation. An asset inventory should be conducted alongside the risk and threat assessment. The asset inventory should allow prioritisation of the deployment of security devices for logging, defence, and protection.

4.3 Preparation

Threat intelligence alone cannot provide benefit to the organisations security practise without support from the right team of people, appropriately integrated processes, and suitable technology. Preparation is required to ensure that the organisation is ready to receive, analyse, and act upon threat intelligence.

4.3.1 People

An organisation may seek to build an internal threat intelligence team or incorporate the duties into existing roles.

A typical Cyber Threat Intelligence Team will combine the following responsibilities:

- Malware reverse-engineering;
- Forensics;
- Management of threat intelligence;
- Intelligence gathering, analysis and distribution of threat information;

[4] http://www.owasp.org/index.php/Threat_Risk_Modeling
[5] http://www.cpni.gov.uk/advice/cyber/Critical-controls
[6] http://www.cpni.gov.uk/Security-Planning/Business-continuity-plan

- Threat assessment; and
- Collaboration with all information security teams within an organisation.

4.3.2 Processes

Most information security processes can benefit from threat intelligence. The organisation should identify processes that require input from threat intelligence and understand how the intelligence should be best presented for that purpose.

For example, an information assurance team can use intelligence on known threat types to help develop a defence-in-depth strategy[7]; an incident detection and response team can search for patterns derived from threat intelligence across the enterprise to detect and defend against malicious activity.

Understanding the audience for threat intelligence across the entire organisation requires in depth analysis. An organisation may use a Managed Security Service Provider (MSSP) who can provide recommendations on threat intelligence integration. Additionally, CPNI provides recommendations for incident response through the Cyber Incident Response service pages[8].

4.3.3 Technology

Fully utilising threat intelligence requires effective use of producers and consumers of data and intelligence:

- **Raw data producers:** Devices or systems that monitor activity and produce log files or packet captures, such as firewalls or proxy servers;
- **Threat data consumers:** Devices or systems that ingest threat data for the prevention or detection of malicious activity. A consumer may include a firewall with rules to block incoming connection attempts from malicious IP addresses, a proxy server to block outgoing access to a malicious web site or an intrusion prevention system to block activity related to a piece of malware;
- **Threat intelligence consumers:** A local or remote management platform for managing threat intelligence, for example a SIEM tool; and
- **Threat intelligence producers**: Threat intelligence feed or collaborative platform.

Threat intelligence can be used to bolster the defensive capability of security devices. This can be achieved by translating threat intelligence into threat data and feeding it back into security devices in order to define what malicious activity to look for. Security devices should be deployed strategically throughout the network to protect sensitive assets. While devices deployed to the perimeter of a network can prevent some attacks, an organisation needs to assume these preventative measures can and will be defeated by an attacker. Deploying devices throughout the organisation can significantly reduce an attacker's ability to evade detection for long periods. The effort required to compromise a target or remain hidden would need to increase with each layer of defence.

---

[7] https://www.nsa.gov/ia/_files/support/defenseindepth.pdf
[8] http://www.cpni.gov.uk/advice/cyber/cir/

An organisation should seek to automate the process of consumption and distribution of threat data and intelligence to these defences where possible. As the threat intelligence process matures and increases in size, manual handling of data and intelligence will negatively impact on their effectiveness.

Areas relevant to automation include:

- Use of standard formats.[9]
- Subscription to a structured threat intelligence feed.[10]
- Use of a threat intelligence platform.

[9] Refer to section 10 Standards and Specifications
[10] Refer to section 11 Intelligence Analysis Models

5 Gather Data

5.1 Key Points

Effective utilisation of threat intelligence requires access to a quality data set acquired through strategically deployed network devices and host applications.

Advanced malware may remove or disable logging to prevent its activity being recorded on a particular system. As such, it is important to have access to data from disparate sources across the network.

Data should be aggregated on a central logging system to enable automated and manual analytics and enrichment.

5.2 Network

To help an analyst build an awareness of the overall network environment, log files and alerts from each security device can be sent to a centralised logging system, such as a SIEM tool. Here, the logs are aggregated to allow an analyst to conduct queries over the entire dataset.

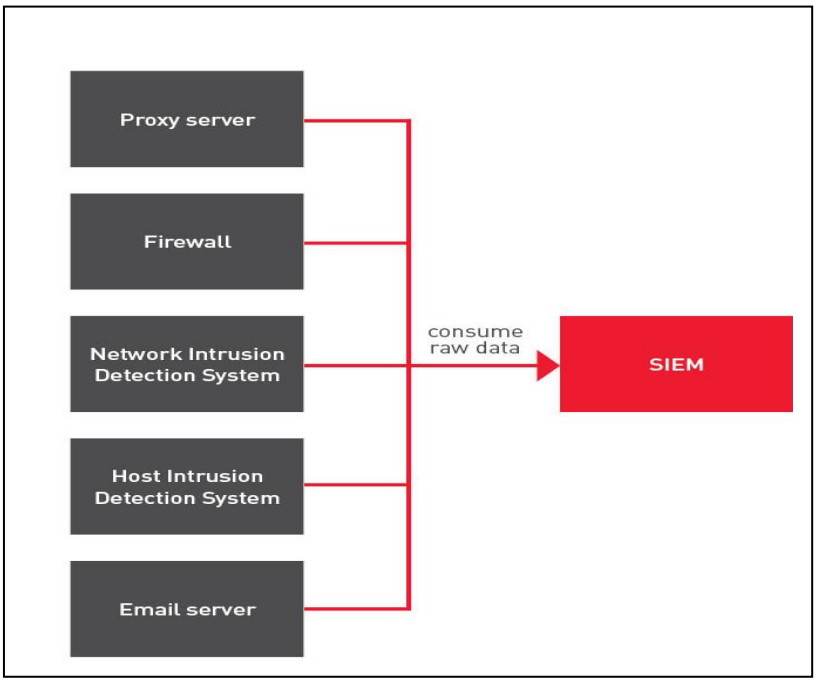


Figure 5 Examples of data that can be sent to a centralised logging system

The substantial amount of data received from the security devices can be overwhelming and finding malicious activity can be difficult. Threat intelligence can be fed into a SIEM to enrich the log events received and direct the analysis work. Here, threat intelligence is used for *Detection* purposes - for monitoring networks and highlighting malicious activity, rather than to prevent it. Please refer to section 6 Consume Intelligence for more information.

Security devices can log activity regardless of whether it is malicious or legitimate. For example, a proxy server can log all web traffic activity that passes through it; a Host Intrusion Detection System can monitor all activity on a computer, such as the opening of applications or use of a USB drive. A thorough record of activity can help build a timeline of a compromise during an incident response investigation process. Refer to the Effective Log Management[11] guidance for more information.

Network traffic can be captured to help verify malicious activity. It can provide access to the raw data that contains evidence of the attack. However, security teams should be mindful that attackers are expert at hiding crucial elements of an intrusion through the use of encryption or operating cautiously over a protracted timeframe. A SIEM tool typically provides integrated visualisation tools to help with analysis.

5.3 Host

While threat intelligence is most commonly used to search for malicious activity on a network, it can also be used to detect malicious activity on a host, through ongoing monitoring or post-compromise.

Host Intrusion Detection Systems, also known as host agents or sensors, can provide a very granular log of activity, as shown below. In addition, they can provide alternate data that is not present in network traffic. Similar to network devices, the activity can be sent to centralised consoles or a SIEM for further analysis.

- **Applications:** Open and closed applications, processes and their actions;
- **System modification:** Windows Registry and installation or removal of applications;
- **Network:** Communication over the network or open network connections; and
- **External devices:** Use of external media, such as an external hard drive or USB drive.

A host agent installed on a computer sends a log of system activity to a centralised logging system, such as a SIEM tool. The SIEM tool aggregates these events and searches for malicious activity using threat intelligence.

Following a compromise, forensic images can be taken from memory or media. These images are raw unanalysed data from which malicious activity can be found and intelligence derived. Threat intelligence can be used to search over the raw data to find indicators of compromise.

A virtual machine or sandbox can be used to gather threat data. This can be achieved either manually through analysis of the malware by an analyst, or run automatically with the behaviour dynamically recorded. Detected behaviour can be represented in a structured format for use in other tools.

[11] https://www.cpni.gov.uk/advice/cyber/Log-File-Management/

6 Consume Intelligence

6.1 Key Points

Threat intelligence should be consumed into existing security and network devices for the purposes of enhancing network protection.

Each intelligence source should be chosen to help mitigate the specific risk or threat posed to an organisation. It is unlikely that one feed will provide sufficient coverage. As such, it is important to assess what sources are available. Beyond commercial vendors, there are an increasing number of initiatives specific to industry sectors that bring their own unique and actionable intelligence. The evaluation of the effectiveness of intelligence sources should be carried out regularly and further sources acquired or removed where appropriate. Aggregation of threat intelligence sources will ensure that you have the best possible coverage of existing and emerging threats.

The use of standards will aid in the description, utilisation and sharing of threat intelligence, not only within your organisation but across the security community. Get the most from threat intelligence by ensuring that tools and frameworks are available to manage feeds and content.

6.2 Intelligence Sources

There are several threat intelligence sources, including:

- Government and industry initiatives;
- Commercial vendors;
- Open source;
- Informal business relationships;
- Collaborative and exchange platforms; and
- Internal intelligence gathering and analysis.

The characteristics of each source will differ considerably. For example, the content of one source may focus on detecting attacks relating to a particular industry sector, whereas another may focus on a particular threat type, such as spear-phishing. As such, it is important to evaluate each source to identify how and where it can benefit an organisation.

Threat intelligence is described in a variety of formats. Where possible, the source of the intelligence should be described in a structured format to assist with consumption and exchange. Refer to section 10 Standards and Specifications for more information on threat intelligence formats. Utilising the intelligence using an unstructured format requires a level of human interaction that can slow the process and potentially miss the detection or prevention of an attack.

6.2.1 Government and Industry Initiatives

Joint efforts between industry and UK Government enable the sharing of information on cyber-attacks. These mechanisms allow experiences to be shared while ensuring the organisation's confidentiality.

The Cyber Security Information Sharing Partnership[12] (CiSP), part of CERT-UK, is a joint industry government initiative to share cyber threat and vulnerability information. The main objective of this is to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business.

There are government initiatives in the United States that provide threat intelligence. For example, the Industrial Control Systems Cyber Emergency Response Team[13] (ICS-CERT), managed by the Department for Homeland Security in the United States; they produce alerts, advisories and other products[14] that can be used to supplement intelligence sources.

6.2.2 Commercial Vendors

An organisation can acquire tactical and strategic threat intelligence from a commercial vendor. Vendors typically provide a threat data feed that an organisation can subscribe to and ingest into the appropriate security devices. The Service Level Agreement (SLA) provided by the vendor should be reviewed as part of the assessment process. The vendor may provide a delivery mechanism to help automate the process.

Commercial vendors may offer a range of services beyond the feed itself, as shown in 6.3, Considerations for Selecting Intelligence Sources. The decision on which additional services are required is dependent on how the organisation intends to utilise the intelligence and the resources available.

Commercial vendors may also publish free intelligence reports covering particular threat actors or attack vectors. These reports can include indicators of compromise that can be harvested by an analyst to prevent or detect the activity. While these reports can provide good intelligence, they may be less timely and comprehensive as those supplied through an intelligence feed.

Most threat intelligence vendors produce intelligence through their own threat research and analysis as well as through processing and enriching aggregated third party feeds. Vendors have formed alliances within the industry to share intelligence. Vendors within these alliances differentiate themselves through the additional services they offer. An organisation may work with a vendor to produce intelligence derived from a compromise.

Some commercial vendors prevent their feed data from being exported outside of their own product or appliance ecosystem and make use of proprietary formats. For example, a feed may be delivered solely for the purpose of ingesting into a vendor's own security appliance. This may be due to intellectual property sensitivities or to encourage sales of the appliance, which is often their primary commercial offering.

There are commercial vendors and exchange platforms who have started collaborating with the producers of traditional security devices to help with the integration process. For example, a firewall manufacturer would collaborate with a commercial threat intelligence vendor to allow malicious IP addresses to be automatically extracted from the intelligence feed and fed into the firewall.

---

[12] http://www.cert.gov.uk/cisp/
[13] https://ics-cert.us-cert.gov/
[14] https://ics-cert.us-cert.gov/Information-Products

6.2.3 Open Source

An organisation can subscribe to open source threat data feeds[15], although the delivery mechanism may not be as mature as commercial vendors. There are open source frameworks to help automate delivery and aggregate feeds[16].

Open source feeds typically focus on a particular threat type, such as botnet infrastructure or spear-phishing emails. The security community produces the threat data typically on a best endeavours basis and offers no SLA.

Ingestion of open source feeds into security devices will be assisted by their increased reliance on open threat intelligence formats and no sensitivities regarding intellectual property. Some open source feeds are already in a format that a device can ingest automatically. For example, one open source feed provides signatures that can be applied directly to an intrusion detection system. As previously discussed, however, care should be taken when automatically ingesting feeds into a device with no upfront analysis or validation of its quality.

While open source feeds may offer an attractive, low cost approach to acquire threat data, the data may be less actionable than that from commercial providers. For example, an attack may be successful due to the slower development and deployment of indicators. Open source feeds may better serve as a passive monitoring technique rather than as a blocking mechanism.

6.2.4 Collaborative and Exchange Platforms

Key to the successful exploitation of threat intelligence is the platform or series of interoperable platforms that underpin the storage and sharing of this knowledge. A new requirement for the enterprise is a system that facilitates this collaboration and exchange locally for incident responders and network defenders within the organisation. And, externally to customers and counterparts in kindred organisations or threat researchers who may enrich this knowledge, in return for access to incident specific data to assist their investigations.

[15] Refer to Section 12.1.2 Open source, for a list of open source feeds
[16] Refer to Section 10 for more information

6.3 Considerations for Selecting Intelligence Sources

Figure 6 provides some considerations when choosing a threat intelligence provider. These should be used in addition to the evaluation criteria discussed in 6.4, Evaluating Intelligence Sources. The considerations are discussed in further detail below:

Types of intelligence	• Tactical and/or strategic intelligence.
Data management	• Cloud-based intelligence; • Appliances; • Management platform or portal; • Exchange platform; and • Security and compliance.
Support services	• Managed Security Services; • Support and maintenance; • Malware and forensic analysis; • Incident response support; and • Integration professional services.
Cost	• Pricing model and subscriptions.

Figure 6 Commercial vendor evaluation criteria

6.3.1 Types of Intelligence

Vendors may offer strategic and tactical intelligence beyond the threat data provided in the feed. The provider may produce threat actor profiles or malware analysis reports as part of the service, or for an additional cost.

Tactical: Malware analysis report	**Strategic: Threat actor profile**
Analysis of a piece of malware, including its capability, how it communicates and the indicators that can be used to prevent and detect the activity. Indicators may be provided in the form of host and network detection signatures.	An in-depth analysis of a threat actor's historic campaigns, their intent and capability, TTPs and associated actors. A profile may be formally defined or in free-form text.

6.3.2 Cloud Based Intelligence

A provider may offer a *cloud-based* threat intelligence feed that may consist of one-way or two-way information exchange.

- **One-way:** an organisation downloads threat intelligence from the internet; and
- **Two-way:** In addition to the one-way data exchange, an organisation uploads network telemetry to the provider. In some cases this exchange is optional; in others it is fundamental to the design of the service or the linked appliance. The organisation can choose the level of granularity and how the data is anonymised. The two-way exchange will benefit the wider security community as it increases the visibility of threat actor activity and the provider's ability to infer trends and produce actionable signatures. However, there may be implications regarding the nature of data sent into the cloud as well as anonymity and security.

6.3.3 Appliances

A vendor may offer a threat intelligence enabled appliance to supplement traditional security appliances.

6.3.4 Support Services

An organisation may choose to outsource their whole or partial network security monitoring to a MSSP. A MSSP can provide a range of services including penetration and vulnerability testing, security monitoring and incident response. A provider can help install and maintain network security appliances, along with the integration of threat intelligence. MSSPs may offer a good solution for organisations that lack resources. They are particularly pertinent to industry sectors that have regulatory requirements to abide by.

6.3.5 Pricing Model and Subscriptions

A provider may use a pricing model structured around the types of intelligence on offer, the number of users with access, whether an appliance is installed or if it is part of a wider Managed Security Service.

6.4 Evaluating Intelligence Sources

An organisation should evaluate an intelligence source to ensure it meets their security requirements. Figure 7 outlines recommended assessment criteria, followed by details of each criterion in 6.4.1, Information and intelligence and 6.4.2, Integration into the environment.

Certain criteria, such as the quality of the feed, will be difficult to evaluate and quantify. As such, a security team should trial a feed within their operational environment where possible. The wider security community will be able to provide feedback on its reputation. Once installed, the feed should be reviewed regularly to ensure that it continues to meet the intelligence requirements:

Information and intelligence	• Intelligence scope; • Context; • Data source; • Quality and quantity; • Timeliness; and • Priority and criticality.
Integration into the environment	• Query, customise and filter; • Format and delivery; and • Confidence.

Figure 7 Evaluation criteria and considerations for threat intelligence feeds

6.4.1 Information and intelligence

Intelligence Scope

Feeds may focus on particular threat actors, threat types and attack vectors, or geographical and industry sectors. The risk and threat assessment will help determine which areas are relevant.

Context

The context helps associate an indicator found through analysis of a network compromise with a particular threat actor, threat type or campaign.

Data source

Threat data can be acquired from a variety of sources, including a provider's own intelligence analysis or aggregation of third party feeds. It is important to understand where a provider sources their intelligence as part of assessing the overall intelligence coverage.

Quality and quantity

A feed should provide a sufficient number of indicators to provide appropriate coverage of malicious activity. The threat data should receive a sufficient level of vetting and intelligence analysis to ensure accuracy to prevent false positives or false negatives.

Timeliness

Threat actors can modify their malware and infrastructure frequently. As such, the time window for actionable intelligence can be small. A feed should provide timely delivery of actionable threat data. An organisation needs to ingest the threat data at a similar rate.

Priority and criticality

The severity of an indicator allows an organisation to give priority to its response.

6.4.2 Integration into the environment

Query, customise and filter

Intelligence should be tailored to meet the organisation's security requirements. An intelligence source and associated framework should allow the client to remove inaccurate or duplicate data; particularly relevant for multi-source feeds.

The ability to query the intelligence significantly increases its usefulness. Example use cases include:

- Enrichment of data;
- Tools built around the data;
- Ability to translate intelligence into a format that can be ingested by a SIEM, network monitor, IDS/IPS, firewall;
- Association of a piece of threat data to the higher level intelligence;
- Association of an indicator with a previous incident; and
- External analytics.

To enable these analytics, an Application Programming Interface (API) may be provided. An API provides a programmatic method for an organisation to manage and manipulate the raw threat data.

Format and delivery

The delivery mechanism for each feed will differ and require an organisation to adapt their systems accordingly. Commercial providers may offer an appliance which can manage the delivery and update process.

The threat data will typically be delivered in a formal and structured format, known as Machine Readable Threat Intelligence (MRTI). The specific format of the intelligence will affect the ease in which it can be consumed by security devices, such as a firewall or SIEM, or aggregated with other feeds. Feeds can use open or proprietary formats. Providers may allow the client to choose the format.

To allow a security device to ingest a threat intelligence feed requires an analyst or automated process to translate the data into a format the receiving device understands. The ease in which this is accomplished will vary depending on how the feed is delivered and the format it is in. The same considerations apply when looking to ingest feeds into SIEM tool. It is certainly a worthwhile exercise as it can provide a far more enhanced and enriched view of network and host activity, providing the appropriate log data is captured. For example, attack patterns described by threat intelligence can be translated into SIEM rules to enable threat detection. Refer to section 10 Standards and Specifications for more information.

Confidence

Confidence tends to be supplied in terms of correctness how likely would detection of activity by the indicator represent a true positive case. Or in terms of attribution how confident is the source of the indicator that the activity represented here relates to the threat actor or attack tool ascribed in the indicator metadata.

7 Apply Intelligence

7.1 Key Points

To consume and act on threat intelligence from a third-party is an important step toward better protecting a network. The intelligence can help alleviate the pressure on a security team to exclusively build a deep understanding of relevant threats to their network.

The integration of threat intelligence into traditional security devices and applications is still an emerging area. However, there is considerable effort being made in the standardisation of threat intelligence formats and increasing openness and collaboration amongst the security community will help and enable automation.

7.2 Intelligence Application

The application of threat intelligence acquired from a third-party or derived internally can prevent compromises and enrich raw data to provide the context in which a malicious event occurs. Threat intelligence can help to detect and prevent malicious activity on a host, either as a preventative measure or post-compromise. Examples of how to apply intelligence are discussed throughout this report. A few examples of how intelligence can be applied are listed below.

Threat assessment and modelling	• To identify specific threats and remediation strategies against a system; and • To provide guidance on security architecture for hosts and networks.
Prevention and detection	• To block malicious activity through ingestion of threat data into security devices; • To detect and alert on malicious activity through ingestion of threat data into security devices; and • To enrich events within a SIEM tool.
Incident response	**Forensics:** Following a compromise, threat intelligence can be used to search forensic images taken from host media or memory. Threat intelligence may need to be translated into the appropriate format before use. **Scope of compromise:** During a live incident, analysts can leverage threat intelligence, in combination with other sources like open source and third party data, to assist in highlighting further indicators of compromise across the wider network.

8 Analyse Intelligence

8.1 Key Points

A security team that conducts their own analysis will benefit from tailored actionable intelligence. It can enable an organisation to acquire highly relevant intelligence on threat actors and campaigns that impact their community directly, such as the industry sector or geographical area.

Threat intelligence analysis falls into two main categories, reactive and proactive:

Reactive intelligence analysis is triggered following a compromise. During incident response, an analyst will collect indicators of compromise. These indicators can be used to find associated activity using other intelligence and data sources, such as open source.

Proactive intelligence analysis is performed as an on-going task to seek out relevant threats before they materialise. The goal here is to build an understanding of the threat landscape and build situational awareness surrounding which threats need to be considered and prioritised.

The intelligence can be aggregated with that already acquired from other sources. The process requires dedicated analysts and investment in tools and systems.

8.2 Intelligence Cycle

The Intelligence Cycle[17] shown in Figure 8 can be applied to threat intelligence and used to set the strategic direction for intelligence analysis:

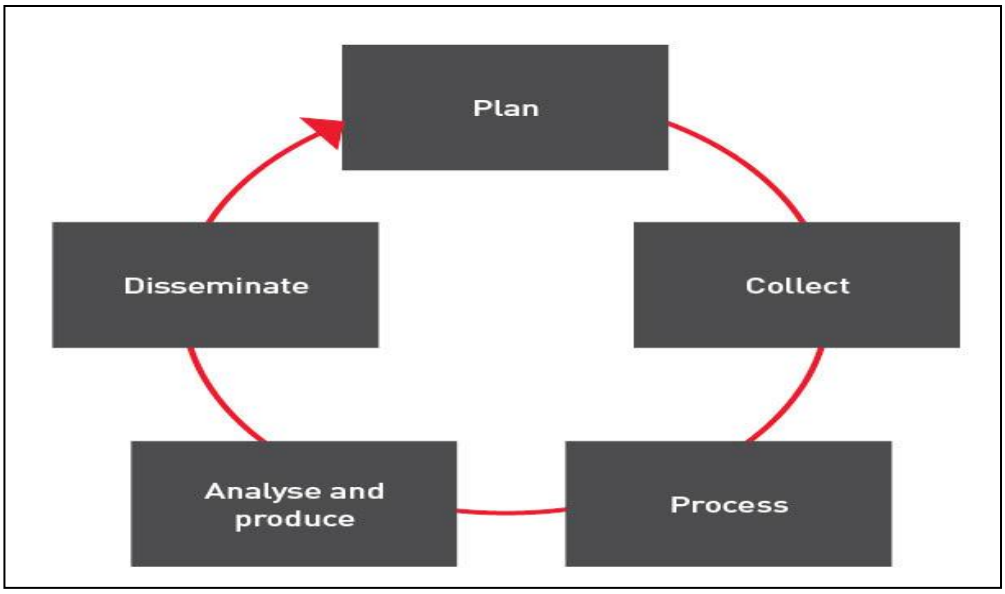


Figure 8 Intelligence Cycle

- **Plan:** This involves assessing the intelligence requirements for the organisation;
- **Collect:** The ability to utilise internal data in combination with intelligence gathered via open source and third-party relationships;
- **Process:** In order to ensure effective processing of threat intelligence it is important to ensure that it is recorded using a formalised and structured format;
- **Analyse and produce:** To fully incorporate threat intelligence into a security process human intelligence analysis of raw data is required to derive both tactical and strategic intelligence; and
- **Disseminate:** The delivery of the analysis product to feed back into intelligence process through sharing and collaboration.

8.2.1 Plan

The potential scope of an investigation into which threats affect an organisation is vast. There are many threat actors that could target an organisation – the difficulty is in knowing where to focus effort and when to move on. As such, the direction and benefit of the analysis should be continually evaluated. An analyst should not be hesitant to drop a line of analysis if it is not producing sufficient or relevant intelligence.

Intelligence should be corroborated against other data sources and vetted by other analysts where possible. A confidence rating should be given on the certainty of an association and the process detailing how the analyst reached their conclusion should be documented.

[17] JP 2-0, Joint Intelligence, dtic.mil/doctrine/new_pubs/jp2_0.pdf 22 October 2013

An analyst covering another analyst's work should be able to clearly understand how a decision was made. Quite often in intelligence analysis, an incorrect assumption is made upon which further assessment and lines of investigation are based. This can result in incorrect groupings and set the direction of analysis that may not be relevant to the organisation's security posture.

The overall intentions of the intelligence gathering and analysis should be established early on. For example, the intention may be to obtain open source malicious indicators (though arguably not intelligence analysis) or to build an awareness of threat actors and campaigns.

8.2.2 Collect

In addition to the data acquired from section 5 Gather Data, analysts should seek data and intelligence from open source, such as forums and malware reports. Data should be processed, filtered and aggregated.

8.2.3 Analyse and Produce

An intelligence analyst gathers raw data and derives intelligence through analysis. For example, identifying indicators and the associated context can produce tactical threat intelligence. Patterns and trends that an analyst identifies can contribute to strategic threat intelligence. The intelligence can build new or contribute to historical investigations.

A technique called pivoting is the process of analysing data to branch out from an already known indicator or piece of intelligence to identify new campaigns, threat actors or attack types. For example, analysis of a command and control website in open source may find other pieces of malware that can be defended against.

Intrusion analysis models such as the Diamond Model[18]and Cyber Kill Chain[19] can assist in describing an actor's capability and TTPs. Refer to section 8, Analyse Intelligence, for more information.

DNS can provide a rich source of data for an analyst to help track a threat actor's campaign. When a domain name is created, there are mandatory fields that are supplied by the registrant. These fields include the name, location and email address. While these details can be falsified, a threat actor may use the same false details for all of their domains. These details are publicly available via WHOIS databases and can be queried to search for similar details. A threat actor may also divide their campaigns or targets across sub-domains. For example, one target may have *organisation1.my_bad_domain.com* where another has *organisation2.my_bad_domain.com*.

---

[18] Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, "Diamond Model of Intrusion Analysis," Center for Cyber Threat Intelligence and Threat Research, Hanover, MD, Technical Report ADA586960, 05 July 2013. http://www.activeresponse.org/the-diamond-model/

[19] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In L. Armistad, editor, International Conference on Information Warfare and Security, volume 6, pages 113–125. Academic Conferences International, Academic Publishing International Unlimited, 2011. http://www.lockheedmartin.co.uk/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html

Malware platforms can help detect and track malicious campaigns. If an analyst suspects a file to be malicious, it can be uploaded and scanned against multiple anti-virus products. Threat actors also use these platforms to determine whether their malware will evade detection. When a file is uploaded, it becomes available to other users of the platform, with metadata extracted from the file, such as the creation time or the exploit used. This metadata can be queried, which is a highly valuable technique, for analysts to find similar malware used by the same actor. For example, threat actors will often sign a file with the same certificate or use the same exploit. This technique can start to build an awareness of the actor's capability. Since the specific malware an actor uses will vary per target or campaign, it may be possible to generalise the signatures so they can detect variants of the malware. The quantity and complexity of potentially malicious events can become unmanageable. Information security has become a big data problem due to the increasing size and complexity of networks. Big data technologies can be used to help manage the data and visualise events. An analyst can use visualisation tools to query and analyse multiple data sources, discover attack patterns, model threat actors, their infrastructure and capability. To enable this requires access to data acquired through log collection and access to threat intelligence for enrichment.

A Knowledge Management System (KMS) can help manage threat intelligence. A KMS provides analysts with the capability to record intelligence on threat actors, their campaigns, and related TTPs. These systems typically provide both the client application, typically web based, and server side processing and storage. A commercial vendor may provide a platform or portal that allows threat intelligence to be captured, processed and shared. The capability of a typical KMS includes:

- **Pivoting:** Ability to search across multiple fields types to identify related activity;
- **Structured content:** Intelligence recorded in a structured manner to assist with data export and exchange;
- **Data management:** Ability to update or remove historical or inaccurate data; and
- **Protective marking:** Ability to apply protective markings to ensure sensitive data is not shared with unsuitable parties.

8.2.4 Disseminate

Intelligence acquired through analysis should be distributed to the appropriate customers. Some examples are shown below:

- **Incident Response Team:** the incident response team will be able to use indicators from the intelligence to better protect and monitor for malicious activity;
- **Community:** the intelligence should be shared with the community where appropriate; and
- **The Board:** significant threats should be briefed to the board (where appropriate) to ensure that sufficient resources are in place.

9 Share and Collaborate

9.1 Key points

An organisation should share and collaborate on threat intelligence within a trusted community formed through existing or new business relationships with organisations in the same industry sector, geographical area or supply chain.

9.2 Benefits

To share and collaborate will benefit an organisation through the exchange of:

- Awareness of relevant threats;
- Proactive defensive strategies;
- Best practice incident response procedures; and
- Technical capability such as tools to convert between threat intelligence formats or to decode malicious network traffic.

A community built around related organisations, whether through industry sector, geographical area or supply chain, can provide intelligence on more relevant threats.

9.3 Implications

Before intelligence is shared it may be necessary to remove sensitive information, such as Personal Identifiable Information (PII) or how the data was captured. This should be redacted or sanitised as necessary.

It may be necessary to agree on how to handle compromises believed to originate from certain actors, such as nation states.

Intelligence obtained through a commercial provider will typically authorise its use solely at the client site, preventing sharing amongst a community.

9.4 Types of Shared Intelligence

The table below shows some the types of intelligence that can be shared:

Tactical	• Malicious IP addresses and URLs; • Network signatures for detecting malicious activity; • Filenames and computed hashes of malicious files; • Registry keys created by malware; and • Malicious email addresses used in spear-phishing.
Strategic	• Threat actor profiles; • Historical campaigns; and • Malware reports.
Security	• Threat advisories; and • Incident response strategies.

9.5 Sharing Intelligence

Typically, intelligence is shared via a manual or automated process.

Manual exchange can be made using unstructured formats such as emails, documents, portals or forums. This can transfer all types of intelligence but is not scalable or practical long-term.

Automated exchange is enabled through the representation of intelligence in a standard format and an agreement of how to share the intelligence between third-party organisations. The most commonly used methods for sharing intelligence is either through the use of a centralised platform, as shown in Figure 9a, or through an ad-hoc network as shown in Figure 9b.

A centralised platform, also known as collaborative or exchange platforms provide a service to upload, aggregate and vet threat intelligence in a community. Commercial, government and open source bodies have developed platforms based on this architecture.

Organisations can share their intelligence in public or private communities. A public community is one in which any organisation can join and share intelligence. A private community is one in which only selected organisations can join. A private community could be created through existing relationships with other organisations, such as those in the same industry sector or supply chain. One benefit of a private community is that it may provide more relevant intelligence due to the related organisations within it.

Intelligence may also be shared through an ad-hoc or peer-to-peer network as shown in Figure 9b. Here, individual trust relationships and exchange agreements are established. The disadvantage with this architecture is that the exchange mechanism will need to be developed for each partner and the intelligence may have received less vetting by others.

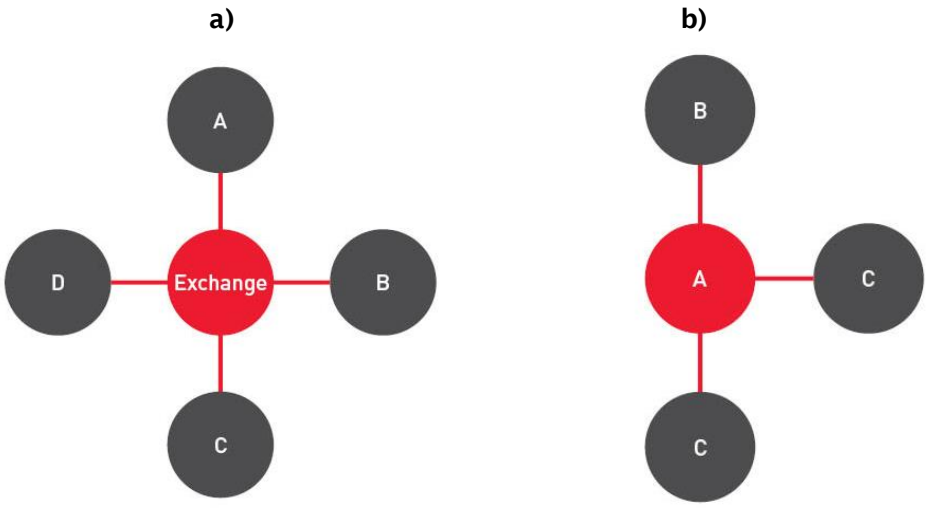


Figure 9 a) Centralised exchange b) Ad-hoc network

An agreement on how the data will be structured and the types of intelligence shared will need to be made. Refer to section 10 Standards and Specifications for more information on the formats that can be used. A disadvantage of using an automated and structured approach may be that the one format does not provide sufficient scope to record the intended intelligence. An organisation can develop extensions for some formats if required. While this can be a useful capability, it requires that all recipients support this extension. An organisation may choose to record their threat intelligence and track incidents using a proprietary format and convert to a non-proprietary format when it is shared.

9.5.1 Exchange Platform Considerations

Data handling classifications	Data handling classification schemes are used to indicate how intelligence may be distributed between individuals, organisations or communities. The Traffic Light Protocol[20] (TLP) is a commonly used scheme. The classification is chosen by the originator of the material. Organisations should also maintain an awareness of potential protective markings used on intelligence from government sources and ensure handling caveats are adhered to at all times.
Information security[21]	Confidentiality, Integrity, Availability, Accountability, Auditability, Authenticity/Trustworthiness, Non-repudiation and Privacy. Evaluate the level of security, access controls and data retention policies.
Intelligence coverage	The intelligence coverage of an exchange platform is dependent on the contributions from its members. Typically, smaller communities encourage stronger trust relationships and therefore increased willingness to share relevant and more comprehensive intelligence.
Format	Consideration should be given to the format used in order to exchange threat intelligence. To assist with the exchange process, a platform should support at least one open threat intelligence format such as those discussed in section 10 Standards and Specifications.
Automation	An exchange platform should allow the automated exchange of intelligence.

[20] https://www.us-cert.gov/tlp
[21] Proposed extension to the CIA-triad of information Assurance and Security principles. Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," Availability, Reliability and Security (ARES), 2013 Eighth International Conference on , vol., no., pp.546-555, IEEE, doi: 10.1109/ARES.2013.72, 2–6 September 2013l

10 Standards and Specifications

There are currently several competing standards for the formatting and exchange of threat data and intelligence, with differing levels of maturity and industry adoption. The relative merits of these standards are discussed in this section.

With a clear choice for industry standard yet to be established, an organisation's decision on which format to adopt both for internal use and exchange is subjective and will depend on several criteria:

- Standards differ in the scope of recordable information and intelligence;
- Tools used to work with the various formats differ in availability, functionality and whether they are open or closed-source;
- Several formats may be required to cover all required use cases; and
- Some formats allow others to be nested within them. This can be useful in the situation where a primary format is used but another provides more granularities for the intelligence to be recorded.

The formats discussed in this section are:

- OpenIOC;
- IODEF/IODEF-SCI;
- VERIS; and
- Mitre framework: STIX/TAXII.

We use the following structure to describe each format:

Overview	A brief overview of the format.
Developer	The developer of the format can influence the adoption rate and the level of development.
Tools and systems	Describes the support and availability of tools and systems; and Knowledge Management Systems.
Format	The underlying format, such as XML or JSON. This can influence the ease in which the data can be converted or extended; and A format may allow others to be nested.
Use cases	Describes the use cases covered by the format.

Figure 10 Field descriptions

10.1 Formats

10.1.1 OpenIOC

Overview	OpenIOC[22] provides a mechanism for describing malicious host and network based activity. An Indicator of Compromise (IOC) as defined by OpenIOC contains metadata, references and a definition. The metadata describes non-technical aspects such as the IOC title, free-form description and author. The references section is used to associate the IOC to an investigation and define the maturity of the indicator and associate with a threat group and category.
Developed by	Mandiant http://www.openioc.org
Tools and systems	OpenIOC Editor (Mandiant, closed source) Redline (Mandiant, closed source)
Format	XML with the ability to extend the framework with additional or customised fields, and supports nesting of other XML-based formats.
Use cases	Indicators of compromise (IOCs) may be recorded following an incident, including: • Specific hash files; • A specific entity in memory (process information); • A specific entry in registry; • Grouping of indicators to search for behaviour of malware; and • Creation of whitelists. IOCs can be associated with a threat group and category. IOCs can be grouped using Boolean logic to build scenarios, such as: • Service name is 'Internet Services'; and (filename is 'svch0st.exe' OR 'scvh0st.exe'). OpenIOC does not explicitly provide an exchange mechanism, but it can be embedded into formats such as STIX/TAXII to enable transport.

[22] http://www.openioc.org/

10.1.2 IODEF/IODEF-SCI

Overview	The Incident Object Description Exchange Format[23] (IODEF) provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. An extension is under development entitled *IODEF for Structured Cyber Security Information* or IODEF-SCI[24]. There are several open source implementations of IODEF that cover anti-phishing and e-crime. The *Collective Intelligence Framework*[25] aggregates several open-source feeds and can help with the ingestion into security appliances.
Developed by	Managed Incident Lightweight Exchange (MILE) Working Group (RFC 5070) https://www.rfc-editor.org/rfc/rfc5070.txt
Tools and systems	IncMan NG (DFLabs – closed source) ArcSight Products (closed source) Foundstone XORCISM Real-time Inter-network Defence[26] (RID) agents (open-source implementations in Java[27] and Python[28] exist)
Format	XML
Use cases	Historical incidents can be used to build better defensive networks. Open-source tools are available to convert between IODEF and the appropriate format for the appliance, such as IP blacklists or signatures for an Intrusion Detection System, such as Snort rules. An incident may be described through attack patterns, vulnerabilities, weakness and events. Events describe the systems that were involved in the attack, either the originator or those targeted, an assessment of the techniques used by the actor, the organisational impact, and forensics evidence. Real-time Inter-network Defence (RID) can enable exchange of IODEF.

[23] http://www.ietf.org/rfc/rfc5070.txt
[24] http://www.ietf.org/rfc/rfc7203.txt
[25] http://code.google.com/p/collective-intelligence-framework/
[26] http://www.ietf.org/rfc/rfc6545.txt
[27] https://github.com/RSAIntelShare/RID-Server
[28] https://github.com/MITRE-RID-Agent/MITRE_RID_Agent

10.1.3 VERIS

Overview	*Vocabulary for Event Recording and Incident Sharing*[29] *(VERIS)* is a standard for describing and sharing incident information. Primarily focussed on incidents and strategic intelligence. VERIS does not provide the ability to record different types of indicators. VERIS provides a relationship model to associate activity to actors along with their motives. The VERIS framework is divided into four main areas to capture the different aspects of an incident: • **Demographics:** the entity affected including industry sector, size and region • **Incident classification:** series of events that make up the incident • **Discovery and mitigation:** series of events following the incident, including how the incident was discovered, what resources were used, how control measures were defeated; and • **Impact classification:** impact of the compromise in terms of direct loss, such as stolen data and response costs, indirect loss, such as brand damage and legal costs, impact estimation and impact qualification, such as how the compromise has been perceived.
Developed by	Verizon http://veriscommunity.net
Tools and systems	The availability of tools and platforms that use VERIS is limited. Verizon have made their framework available in the open source community, so tools can be developed to support it.
Format	JSON XML
Use Cases	Indicators are structured in a simple array containing the indicator and associated comments. Other formats should be considered if the recording of indicators is the main use case. VERIS does not explicitly provide an exchange mechanism, but it can be mapped into STIX/TAXII to enable transport.

[29] http://veriscommunity.net/

10.1.4 Mitre Framework

Overview	The Mitre framework[30] provides a broad spectrum of storage and exchange capability. Mitre provides standards for describing both strategic and tactical intelligence. The framework is built on the CybOx format. The Mitre framework provides the following threat intelligence formats: • **CybOx:** Cyber Observable framework which underpins STIX, TAXII, MAEC and CAPEC • **STIX**: Structured Threat Information Expression • **MAEC**: Malware Attribute Enumeration and Characterization captures detailed malware information. Primarily used by malware analysts. MAEC can be embedded into STIX • **CAPEC**: Common Attack Pattern Enumeration and Classification; and • **TAXII**: Trusted automated exchange of Indicator Information. The framework provides a comprehensive relationship model that allows indicators to be associated with higher-level concepts such as threat actors and campaigns.
Developed by	Mitre - an organisation funded by the Department of Homeland Security in the United States. http://www.mitre.org
Tools	Several vendors have adopted Mitre as the underlying format for their threat intelligence platforms and tools.
Format	XML As the standard is language-independent it is expected other implementations to be developed, such as JSON. Formats, such as Yara and SNORT, can be embedded to allow them to be used natively with existing tools without having to generate the signatures from higher-level concepts.

[30] https://stix.mitre.org/

Use cases	A threat actor may be characterised by their sophistication, intent and desired effects. The relationship model allows an actor to be associated with TTPs, campaigns and related threat actors. STIX defines a campaign as a set of incidents carried out by a threat actor using specific TTPs. Intelligence can be translated into Open Indicators of Compromise (OpenIOC) to search for malicious activity. An incident may be characterised by the impact of the compromise on systems and information, the timeline, points of contact and additional metadata. Incidents can be related to threat actors, courses of action for remediation and mitigation and indicators that were used to detect the activity or discovered through the incident response. A Course of Action conveys information about incident response actions or preventative measures associated with an attack. TAXII provides an exchange mechanism for exchanging STIX

11 Intelligence Analysis Models

11.1 Cyber Kill Chain

The anatomy of an attack can be described in a variety of models. One such model is the Cyber Kill Chain®[31] which describes the process of attack over several stages as shown in Figure 11. It can be described formally through structured formats or informally through threat profile documents. The Cyber Kill Chain helps build an understanding of the threat actor and their TTPs and provides a framework in which to develop mitigation strategies. The premise of the Cyber Kill Chain is that a successful compromise can be prevented if just one stage is mitigated.

Reconnaissance	Threat Actor conducts research into a target, such as employees or network infrastructure. Identify sources the actor may have used to build an understanding of the organisation; this could include research of open source information and external network scanning. In order to protect against reconnaissance organisations should seek to review their online footprint, where appropriate. The scanning of an organisation's network to identify the services it uses and potential vulnerabilities can be logged at the perimeter of the network. Analysis of these logs can help identify the source of the scanning and begin to build an awareness of threat actor infrastructure. To protect against external network scanning, ensure that security devices such as firewalls are configured to prevent in depth reconnaissance like scanning.
Weaponisation	Threat Actor develops a malicious payload to execute within the target network. The payload will typically contain an exploit to bypass security restrictions and a piece of malware, such as a remote access Trojan, to control actions on the victim's computer. During this phase, tactical threat intelligence such as the type of exploit used or malware details (filename, hash etc.) would help build the intelligence picture surrounding the Threat Actors TTPs.

[31] Developed by Lockheed Martin: http://www.lockheedmartin.co.uk/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Delivery	Actor delivers payload, for example through a spear-phishing or strategic web compromise. Using spear-phishing as an example, threat data such as the email address; subject line and the victim email address can be used to enhance the intelligence picture. Mitigations that could be employed at this stage of the Cyber Kill Chain (using spear-phishing as an example) include; blocking the email address on the email server and utilising an intrusion detection system to detect the presence of the email subject line or malicious link.
Exploitation	Payload executes within target network. At this stage of the Cyber Kill Chain, system indicators discovered through the execution of the exploit are useful in building the intelligence picture.
Installation	Payload installed within target network, either as a permanent or temporary presence. Threat intelligence of use during this phase of the model include: system modifications made by the malware, such as the install location, registry changes, network activity and processes created.
Command and Control	At this stage, the payload communicates with actor to enable remote control. Recording this activity, for example through reverse engineering the malware, is useful for several reasons. If you signature the network traffic of the malware these can be deployed to the intrusion detection system. In addition, blocking the IP address of the Command and Control infrastructure may stop communication between the implant and the attackers.

Action on objectives	Actor carries out objectives, such as data egress or lateral movement. This phase of the attack will be dependent on Threat Actor motives. However, threat intelligence that will aid in building the intelligence picture may include; the technique used to get access to breached systems, details of any compromised accounts, the scope of the compromise (number of systems affected and data stolen). Possible mitigations at this stage of the Cyber Kill Chain include: use of two-factor authentication, encryption of data at rest and increasing the granularity of logging on sensitive systems.

Figure 11 Cyber Kill Chain®

11.2 Diamond Model for Intrusion Analysis

The Diamond Model for Intrusion Analysis[32] provides a framework to discover, develop, track, characterise and counter a threat actor or attack vector. The four basic elements of a compromise that the model considers are:

- A threat actor, or adversary, who carries out the attack;
- A technical capability to carry out the objectives, such as an actor's TTPs;
- Infrastructure on which to send commands or receive egress; and
- A victim.

In short, an adversary utilises a capability over an infrastructure against a victim. The Diamond Model can be illustrated as shown in the below diagram:

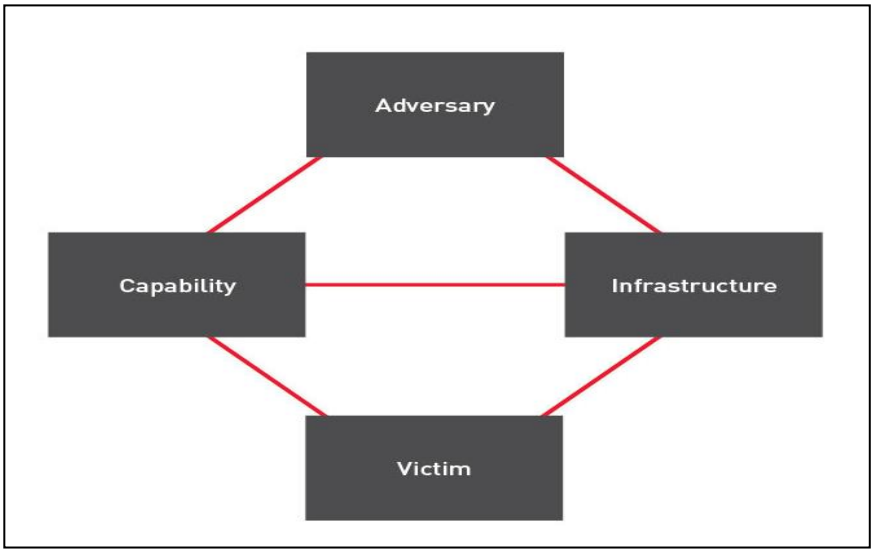


Figure 12 Diamond Model

[32] http://www.threatconnect.com/files/uploaded_files/The_Diamond_Model_of_Intrusion_Analysis.pdf

A compromise can be defined in a series of events, from an initial spear-phishing email to the eventual egress of intellectual property. Each event can be described in terms of the four elements.

By describing events using these elements allows compromises to be grouped or associated. For example, while the adversary may be unknown, common infrastructure used across several spear-phishing campaigns can be grouped together into an activity group.

The model can help formalise the process of intrusion analysis and encourages an analyst to consider each basic element through the compromise lifecycle.

12 References

12.1 Sources

The sources listed here give an indication to the availability of threat data and intelligence. It is not an exhaustive list:

12.1.1 Government

CPNI Information exchanges	http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges	Sharing of information about the risks facing networks is beneficial to both government and industry. CPNI facilitates 'information exchanges' which allow one company to learn from the experiences, mistakes and successes of another, without fear of exposing company sensitivities.
Cyber-security Information Sharing Partnership (CiSP)	https://www.cert.gov.uk/cisp	The Cyber-security Information Sharing Partnership (CiSP), part of CERT-UK, is a joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business. CiSP allows members from across sectors and organisations to exchange cyber threat information in real time, on a secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information.

12.1.2 Open source

abuse.ch	http://www.abuse.ch	Provides feeds to block or detect activity relating to a range of malware including Zeus, SpyEye and Palevo.
Emerging Threats	http://www.emergingthreats.net	A provider of open source and commercial threat intelligence.
ShadowServer	https://www.shadowserver.org/wiki	Provides intelligence on a variety of malicious indicators, such as malware and botnets.
Composite Block List	http://cbl.abuseat.org	Provides a list of known IP addresses used to distribute spam or malicious content.
Nothink	http://www.nothink.org	Provides a list of known malicious IP addresses.
CleanMX	http://support.clean-mx.de/clean-mx/viruses	Provides a list of known malicious URLs.

+44(0)207 537 7515
www.contextis.com