INTELLIGENCE-LED THREAT MITIGATION.
BACKGROUND

As organizations seek greater situational awareness and operational efficiency, many are looking to intelligence-led approaches to augment their cyber defenses. Specialist fields such as cyber threat intelligence have emerged with both boutique firms as well as traditional players offering solutions to cater for this. Complementary data-driven approaches such as security analytics are also gaining traction. So how can organizations take advantage of these in a strategic way?

This paper presents a six-step process for building an intelligence-led threat mitigation program. It discusses the importance of having a threat model to base intelligence requirements on, the need for a platform to operationalize intelligence efficiently, security analytics for discovery of new or unknown threats, and a security dashboard to bring it all together for effective performance management.

The approaches to implementing some or all of this program will vary from organization to organization, partly due to differing levels of existing maturity and partly due to differing missions. Getting the steps of the process described here right though, whether by augmenting an existing program or building from scratch, will be a worthwhile investment for any security or intelligence team.

“...how can organizations take advantage of these in a strategic way?”
THE ROLE OF INTELLIGENCE IN MITIGATING THREATS

The attacker naturally has the upper hand in conflict situations for several reasons: they can move first, defenders need to be quick to react; they only need to be lucky once, a defender must succeed all the time; they can focus on narrow objectives, defenders need wide visibility. In cyber network defense these principles are especially true – keeping out a skilled and determined attacker over the long run is a hard task.

Security teams do have some advantages though: they can use defense in depth approaches, meaning an attacker must evade many layers to reach their goal; they can leverage broad communities of expertise, something akin to a herd defense posture; they can track attackers through digital evidence left in cyber space, even a small security lapse on the part of the attacker can link back to their identity. These approaches are complementary, and they are brought together by the field of cyber threat intelligence.

While network defense is important enough, this is not the only benefit a good intelligence program will bring. It can also provide important enrichment to the technical components of cyber attacks – for example, providing details of actor intent and potential adverse impact to individuals, business, or nations. Such threat context is a key component of security operations. It gives the network defense teams greater ability to prioritize incidents, but also gains buy-in from senior stakeholders in explaining the nature of the threats faced and how resources should be allocated to mitigating them.

The diagram below shows this in conceptual format. This contains two sets of information, a set of threat data which includes signatures for known bad entities, and a set of threat context information which provides the additional perspective on the threat.

Cyber threat intelligence is a multidisciplinary field of security. As well as hard technical skills it also requires soft skills such as having an ability to communicate complex problems in plain language. When done well it is the key linkage in translating the technology risk, with its jargon and terminology, into the business risk language understood by management and policy makers.
As former US Secretary of Defense Donald Rumsfeld put it:

“There are known knowns; these are things we know we know. There are known unknowns; that is to say we know there are things we do not know. But there are also unknown unknowns – the ones we don’t know we don’t know.”

“Their are known knowns; these are things we know we know...”

Network defenders can learn a lesson from this. Cyber threat intelligence has its limits and chief among these is the focus on the known knowns; and at best, extrapolating from these to cover known unknowns. Detecting unknown unknowns, for example an attack from a new adversary with new tools and new infrastructure, requires another approach.

Discovery of unknown threats using data is a core capability of a modern intelligence-led operation. In cyber defense, we refer to this approach as security analytics – using techniques borrowed from data-mining to detect anomalies in network and host logs which are worthy of further investigation. This complements other network defense capabilities, such as correlation engines, sandboxing, and application whitelisting, to provide enhanced visibility and ability to pick up subtly executed attacks.

In our own security operations center, where we monitor the networks of many large organizations, we detect approximately half of security incidents using threat intelligence and the rest from security analytics. The two capabilities work side-by-side: threat intelligence is used to inform the models of the security analytics, while new and previously unknown threats detected through security analytics feed the intelligence picture.

The illustration on the next page shows these approaches working together.

Building this capability requires a strategic approach to cyber security. There is no shortage of attractive looking solutions to mitigate one threat or another, however a robust security program should be based on solid foundations such as a thorough understanding of the threats faced. It should have the agility and visibility to be able to react to changes in how adversaries seek to compromise the systems and information assets we protect. The following six steps are provided as a guide on how to build such a program.
Information sharing with trusted partners

Indicators deployed to monitoring systems

Centrally managed threat intelligence repository

Ingest of structured and unstructured feeds

Contextual information available to SOC analysts

Integrated threat models for security analytics research

Threat Intelligence

Security Analytics

Investigation

Raw Data
SIX STEPS TO INTELLIGENCE-LED THREAT MITIGATION

Undertaking an intelligence-led approach to security can be broken down into several phases which build on each other. The entry point to this journey depends on the maturity of existing security operations. For some it may be that the intelligence function already exists and they are looking to security analytics and improved situational awareness. For others it will begin with understanding the threats they face and how they can collect more intelligence to mitigate these.

The process aims not only to enhance threat discovery and investigation prioritization, but also to promote greater awareness of cyber threats among senior stakeholders. This allows them to make better risk informed judgements, including those which influence resources for security operations.

This figure illustrates the six steps which are further described below.

- **Step 1. Perform threat assessment**
- **Step 2. Determine intelligence requirements**
- **Step 3. Build collection sources**
- **Step 4. Operationalize threat intelligence**
- **Step 5. Introduce security analytics**
- **Step 6. Gain situational awareness**
STEP 1. PERFORM THREAT ASSESSMENT

The goal of an intelligence program should be to reduce uncertainty in conflict – in this case defending the security of information networks from a range of adversaries. To accomplish this it is necessary to have a problem statement which guides our high-level thinking. This could be “What are the major threats to networks we defend from cyber attacks?”

The next step is breaking this problem statement down into a detailed problem definition. For this we need to build a model of the major threats which the organization faces. This can be developed through an exercise which includes input from:

- **Incident response reports:** Attackers often return to targets where they had success in the past, so understanding these adversaries is a priority. The tools, techniques, and procedures of such an attacker should inform both the intelligence picture and in turn the relevant security controls.

- **Pen-testing reports:** Penetration tests aim to reveal vulnerabilities – another component of the cyber risk equation – but they can be equally informative to the threat model by highlighting systems which may be prone to attack. For example, highlighting a publically exposed portal for an industrial control system may attract attackers which specialize in compromising these systems. Such a threat may then be captured and added to the model.

- **Security alerts:** Near misses in the form of detected and prevented attacks will be recorded in security alert data. Reviewing anti-virus alerts as well as blocked email/web based attacks can reveal patterns which are indicative of a persistent threat.

- **Advice from external experts:** Cyber threat intelligence professionals can provide an impartial view of the threat landscape as well as distil the more serious observed threats from those which are commonplace. They leverage visibility across multiple sources, privileged relationships with other security professionals, and conduct research which tracks the tools, infrastructure, and targets of the attackers.

- **Surveys of I.T. team members and business area managers:** There are likely many people within the organization with a view on the cyber threat. Not all of these will sit within security roles specifically; however developers, system admins, business area managers, legal team members, CXO executives will all have a different but equally important view. Surveying a range of members of staff with a concise questionnaire, followed by open-ended questions via phone interviews, will provide both input to the threat model and an indication of organizational maturity.

- **Workshops with key stakeholders:** Bring together internal stakeholders, external experts, and even external parties such as suppliers to brainstorm threats. This will provide a fruitful input to the threat model and can also be a useful point at which to define the scope – e.g. what counts as a cyber risk verses operational-risk, whether or not accidental insiders count as threats, etc.

The input from the various sources should be compiled into a model, as well as a report, to provide context on decisions made.

Both current threats as well as future ones should be considered. This may require input from strategy or development teams in order to gauge what the operating environment will look like in years to come. Geopolitical tensions and the rise of cyber capabilities in foreign militaries should not be underestimated as future threat sources.

It is said that all models are wrong, but some are useful. It is important to bear this in mind and resist the urge to be too complete or precise. Threats which cannot be easily categorised initially, for example new attack sources using new capability, should be captured under a placeholder with a label such as ‘emerging threats’. The model should be reviewed regularly and threats which have fallen into this last group can be given their own category as required.
STEP 2. DETERMINE INTELLIGENCE REQUIREMENTS

The next step in an intelligence-led threat mitigation program is deriving requirements from the threat model. These will drive not only the collection of threat information but also provide direction for security analytics development.

Threats should be prioritized in order of perceived likelihood of causing an incident and severity of impact caused. A gap-analysis may be conducted to determine current status of intelligence against identified threats. These two inputs then influence the creation of a set of prioritized intelligence requirements.

Individual threats can be deconstructed into smaller sub-problems in order to help guide collection. Established models can be invoked at this stage, such as kill chains or the diamond model. The former is useful in an operational context, particularly for building security analytics and detection rules; whereas the latter works well as a target model – where new threat data can be fitted in to the relevant segment of the problem.

To illustrate usage of a target model approach, we’ll use the hypothetical example of a criminal group called ‘The Digital Mob’: an organization’s threat assessment and gap analysis has determined that ‘The Digital Mob’ are a priority intelligence requirement. Using the diamond model approach, we build a target model around this group’s socio-political features and the technology they use in attacks. Breaking this down further we get a set of smaller intelligence problems focused on the group’s identity and relationships, their targets and victims, their tooling (e.g. malware) and their infrastructure (e.g. rented hosting). Each of these sub-problems becomes a component which can be analyzed separately, but directly builds into the overall intelligence picture. When a new piece of intelligence arrives the analyst can then fit this into the relevant portion of the model. Importantly, this approach helps identify gaps which can be tasked for extra collection effort.

The step of determining intelligence requirements can be done as part of the threat assessment exercise. Doing so also provides an opportunity to engage with the end customers of intelligence products within the organization. Identifying what different customers want, gains buy-in for the program and helps manage expectations. Different customers should still have a common threat model, but would receive different intelligence products.

The output of this process is a set of prioritized intelligence requirements and structured intelligence models ready for collection.

“A gap-analysis may be conducted to determine current status of intelligence against identified threats.”
STEP 3. BUILD COLLECTION SOURCES

Organizations often ask our advice on what the best place to get cyber threat intelligence is, and whether one source or another is preferred. In reality, there are many good sources available, and no single source will ever meet a full set of intelligence requirements. Some which we recommend looking into are:

**INTERNAL SOURCES**

As with the threat assessment, internal sources such as incident reports, security alerts, and research by colleagues are an excellent first source of intelligence. It is important to consider how these can be captured and saved to an intelligence store for analysts to query but also accessible to via high-level dashboards.

**OPEN SOURCE**

For many cyber intelligence problems it is likely that some information will already exist in the public domain. Depending on how specific the intelligence problem is, there might be a blogger or security vendor which publishes research relevant to the threat. Capturing this, perhaps via an RSS reader, helps to update the picture for that particular intelligence problem.

**VENDOR SERVICES**

Many security vendors now offer cyber intelligence products as part of their product and service portfolios. Some are traditional security technology companies with access to large volumes of threat data. Others are specialist firms with expertise in delivery of intelligence. There are advantages to using third-parties to supplement other sources: ready access to a leveraged pool of expert analysts; existing intelligence databases and reports; extensive networks of sources which the vendor has built up; specialist tools for mining and clustering data. Some disadvantages worth noting: intelligence products may not be tailored to your organization; biases towards particular regions or sectors may exist; some vendors don’t do their own research and merely act as aggregators. This field is still immature and we expect to see evolutions in commercial models such as price-per-report emerging to help to balance cost and relevance.

**MALWARE REPORTS**

Building an in-house automated malware analysis system for generating cyber intelligence may seem like a considerable undertaking. However with open-source technology and access to free malware feeds, the barriers to this sort of capability are much lower than they once were. Malware reports provide a supply of indicators which may be searched across logs. A database of such information also provides a useful repository for trending and intelligence exchange with partners.

**INTELLIGENCE SHARING COMMUNITIES**

In recent years communities have emerged for sharing cyber intelligence. Some of these are government led and sponsored, some are industry led, and some are run by individual researchers. All have merit for different intelligence problems and can provide the first insights into emerging threats. As these communities mature, more will offer some level of support for queries, for example via APIs. This will allow organizations to access the information in more ways and enrich their intelligence problems more quickly.

The output of this process should be a set of documented threat sources ready for integration into operations.
STEP 4. OPERATIONALIZE THREAT INTELLIGENCE

This step is critical to getting value from an intelligence-led threat mitigation program. It is where threat data is collated, processed, searched across host and network log sources, and converted into intelligence products. There are some common stages to operationalizing threat intelligence:

ACQUIRE
To efficiently take collected threat data and turn it into actionable intelligence it is necessary to have an intelligence management platform. This should allow the threat intelligence function to acquire new sources when available. New data may arrive in both structured formats as well as unstructured reports – often containing the richest threat context information.

PROCESS
Systems exist today for processing structured intelligence, through ingest of common formats and saving into relational databases. It is also possible to perform entity extraction on unstructured data, for example pulling out IP addresses, email addresses, domain names from written reports. This dramatically improves the analyst’s ability to process multiple sources such as PDF documents, emails, blog posts, and extract the relevant intelligence rapidly.

Tagging of the intelligence, enrichment using API lookups to online sources, fusion with existing threat data, and visualization all aid the analyst with the job of processing new information efficiently and updating the relevant threat model.

STORE
The processed threat data should be saved in a central intelligence store, which is fully indexed and searchable by other analysts. The threat database of contextual intelligence should be aligned to your threat model and intelligence requirements. Similarly the indicator database – from which the detection capabilities are deployed – should contain a referential link back to the contextual intelligence. This means that if analysts in future get alerts related to some old intelligence they are quickly able to retrieve the original source and review the details.

ANALYZE
To gain new insights and advance the picture of the threat, analysts need to have multiple tools and techniques at their disposal. These should be tightly integrated into the intelligence management platform. Examples of important capabilities include: sorting and filtering of data/reports, time-series analysis, document-entity graphing, histograms and basic stats charts, tagging/bucketing of intelligence, and dossier creation. To be efficient, this should be built on technology which allows fast-search and retrieval, as well as have a focus on visualization for exploring the stored intelligence. The latter is particularly important for communicating trends and complex problems to stakeholders. Strong analysis makes for deeper insights, more reliable intelligence products, and more actionable results.

ACTION
The processed intelligence may be deployed in different formats for network defense. For example, this may be in the form of firewall block rules, IDS rules, host IOC rules, etc. The ability to generate multiple formats from the same intelligence is key to making it ‘actionable’. Many organizations share intelligence with partners – thus having the ability to export relevant intelligence in common formats is vital for this capability. As part of this it is important for collected intelligence to retain information on the originator (who provided it) and what the appropriate handling instructions for it are. This enables more efficient sharing as permissions are built-in to the data.

At every stage it should be possible to link the intelligence back to the original threat model and therefore the stated intelligence requirements. This is important from the perspective of mission focus – there is no shortage of threat data available to analysts, keeping it relevant while not missing anything is the challenge which the right technology can help with.

The output of this step may include security alerts, threat reports and dossiers, indicators, and partner sharable intelligence.
STEP 5. INTRODUCE SECURITY ANALYTICS

Discovery using intelligence alone will not fully mitigate all threats as attackers develop new capabilities and change their attack vectors with ease.

Threat Intelligence helps to discover known bad, e.g. a partner has shared a signature for a command-and-control channel; an analyst can now identify that channel using logs such as network metadata.

Security analytics helps to discover unknown bad, e.g. we believe attackers use malware which polls command-and-control servers at regular intervals; running a frequency analysis algorithm over the data will reveal the traffic which is periodic in nature.

The big difference here is that where signatures only detect single instances of threats, the analytics detect the generalized behaviors. This is harder for the attacker to modify as it is part of the fundamental modus operandi of the threat. Using the example above again: changing a command-and-control IP address just requires a DNS update, but making the malware non-periodic requires a re-write in the source-code (which may not be available to the attacker).

Few analytics can be written which are binary indicators of good/bad behavior, so alerts from security analytics need to be triaged and investigated by skilled analysts. These analysts should have the ability to pivot through available log sources and then determine whether the anomaly is likely to be a new attack or a false alarm.

Creating analytics is the job of the security data scientist. These team members typically have background in data-mining techniques, as well as domain knowledge in security. Using a variety of sources, including threat intelligence, they craft new security analytics to keep up with the evolving threat and help discover the unknown unknowns.

The output of this step will be deployed security analytics – used to detect security incidents related to previously unknown or hard to detect threats.
**STEP 6. GAIN SITUATIONAL AWARENESS**

A mature intelligence program can be judged on how well it maintains a picture of the problems its customers are interested in and how it delivers this picture to them. This is the concept of ‘situational awareness’. For intelligence-led threat mitigation, it requires all the preceding steps to be effective. Situational awareness cannot be achieved without scoping the underlying threat model, building intelligence collection and detection, and having ability to discover new or emerging threats.

Once this is achieved the final step becomes performance management. This should use the threat model for deriving metrics against which effectiveness of the program can be measured. The intelligence management platform should display these metrics in a dashboard view and on-demand report format.

Returning to our hypothetical ‘Digital Mob’, an example would be:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Our threat assessment exercise has determined that mitigating ‘The Digital Mob’ is a high priority</td>
</tr>
<tr>
<td>2</td>
<td>We have built an intelligence requirement around understanding ‘The Digital Mob’, and in particular tracking usage of their bespoke malware tools</td>
</tr>
<tr>
<td>3</td>
<td>We have collected 5 reports in the past quarter related to ‘The Digital Mob’. These are saved in our intelligence repository and automatically feed our performance metric on collection</td>
</tr>
<tr>
<td>4</td>
<td>The reports have resulted in 100 distinct indicators which we have deployed and a new analytic which detects the generic behavior of their bespoke malware</td>
</tr>
<tr>
<td>5</td>
<td>Another metric shows that we have mitigated 2 attacks from this group in the same period – one using intelligence obtained in a vendor supplied report, and another from our security analytics</td>
</tr>
</tbody>
</table>

The security dashboard thus fulfils the role of providing situational awareness. Pre-defined metrics can be displayed and access given to both security analysts and management to drill into the details. For organizations which monitor multiple networks this can provide intelligence on both the current threat landscape, how effective current mitigations are, and where additional security alerts should be sent. It also becomes a focal point for engaging with multiple stakeholders and intelligence customers, again gaining buy-in to the whole intelligence program.
CONCLUSIONS

Intelligence-led threat mitigation is an approach which complements other best practices in network defense and information security. Organizations using it will still need strong technical defenses, security controls, testing, network segmentation, user training, and many more approaches to keep attackers out. However, good intelligence can augment these other areas and help to prioritize resources. It can shed light on past threats, current ones, and even help forecast future threats.

This report has presented a set of steps through which organizations can adopt an intelligence-led approach to cyber security. It is deliberately not prescriptive in terms of specific technologies or approaches, as many options are available at each step. This also allows organizations from small companies right up to national level security agencies to choose what is most appropriate to them. The steps start small in terms of required commitment at the early stages, but grow along with the maturity of the program. This should allow organizations to gain more buy-in from stakeholders over time without significant barriers to early adoption.

The tools and techniques exist today to support these steps, and expertise in cyber intelligence is growing fast. Intelligence-led threat mitigation promises both improved discovery of threats, but also the ability to bridge the technology risk and business risk divide. To achieve this it needs to evidence its successes. Having a considered strategy and approach from threat modelling to intelligence collection to dashboards for management information will help to achieve this.
ABOUT US

BAE Systems Applied Intelligence delivers solutions which help our clients to protect and enhance their critical assets in the connected world. Leading enterprises and government departments use our solutions to protect and enhance their physical infrastructure, nations and people, mission-critical systems, valuable intellectual property, corporate information, reputation and customer relationships, and competitive advantage and financial success.

We operate in three key domains of expertise:

- **Cyber Security** – helping our clients across the complete cyber security risk lifecycle
- **Financial Crime** – identifying, combating and preventing financial threats, risk, loss or penalties
- **Communications Intelligence** – providing sophisticated network intelligence, protection and controls

We enable organizations to be more agile, increase trust and operate more confidently. Our solutions help to strengthen national security and resilience, for a safer world. They enable enterprises to manage their business risks, optimize their operations and comply with regulatory obligations.

We are part of BAE Systems, a global defence, aerospace and security company delivering a wide range of products and services including advanced electronics, security and information technology solutions.

Victim of a cyber attack? Contact our emergency response team on:

UK Freephone: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

BAE Systems Applied Intelligence USA
265 Franklin Street
Boston
MA 02110
USA
T: +1 (617) 737 4170
E: learn@baesystems.com
W: www.baesystems.com/ai

www.twitter.com/baesystems_ai
www.linkedin.com/company/baesystemsai

Copyright © BAE Systems plc 2014. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.