Tailoring Intelligence for Automated Response

Overworked and understaffed IT security teams are trying to integrate threat intelligence into their detection, response, and protection processes -- but not very successfully. IT teams need fewer intelligence alerts and more visibility into external threats that matter to their enterprises. SANS Analyst Sonny Sarai discusses his experience reviewing IntSights' Enterprise Threat Intelligence and Mitigation Platform under simulated attack, detection, and remediation scenarios.

Copyright SANS Institute
Author Retains Full Rights
Cyber threat intelligence (CTI), when used correctly, provides visibility into attacks and threats, according to the 2017 SANS CTI survey. There are many challenges to using and implementing CTI, however; the top two issues are not having adequately trained staff and having little to no funding, according to the same survey.

Specifically, security analysts are dealing with too many sources of intelligence. They aren’t able to correlate and narrow all these sources of intelligence to those events and vulnerabilities that really matter. The SANS CTI survey states that organizations can accept and utilize up to 10 threat indicators a week, yet most are receiving between 11 and 100 threat intelligence feeds per week. This is causing information overload and causes more confusion for practitioners. What is noise? To what do IT staff really need to pay attention?

To that end, SANS conducted a functional review of IntSights’ threat intelligence platform, which reduces the load on security administrators and responders by collecting external and internal threat intelligence tailored to an organization’s environment.

The IntSights Enterprise Threat Intelligence and Mitigation platform is primarily a cloud-based service module that monitors millions of sources across the deep, dark and clear web for threat information that can be used against the organization or may indicate a cyber threat. This allows IntSights’ platform to provide tailored feeds, alerts and reports to the organization. For internal detection and response, the platform integrates easily with on-premises security systems such as firewalls, web

---

proxies and Active Directory, to automatically inform security teams about internal threat intelligence and align with automated remediation capabilities.

This ability to connect the dots between what is going on outside the organization (on the clear and dark web) and what’s happening inside the organization (internal data from security devices, networks, systems, devices and users) eliminates the need for extensive staff training and deeper understanding across the entire security and response team.

During our review, the interface and pivot capabilities were user-friendly and intuitive. There are a number of feeds and IoCs that IntSights takes in for the customer, but it is important to enter your critical company assets into the interface in order to further tailor the service to your specific organization. Overall, we felt that these and other enhanced features should reduce the stress on overworked, under-informed security analysts and responders, while also increasing the accuracy of detection and response.

**Product Overview**

In this functional review of the cloud-based IntSights Enterprise Threat Intelligence and Mitigation service, we utilized a mock environment hosted in the cloud. It included pre-populated data showing actual alerts and reports from other investigations.

We started by applying intelligence to the digital footprint we set up, and then implementing an automated workflow. Our goal was to see how IntSights gathers intelligence (including from the dark web), sorts it for relevance and enables responders.

IntSights’ platform is primarily a cloud-based SaaS service, with one component we used on-premises to help with automation across internal devices that the service would be working with. This on-premises component, discussed later in the paper, is a virtual machine that integrates with an organization’s internal security devices, such as a firewall or a web proxy.

When a customer becomes active, the IntSights team provides it with login information into the cloud service. This login is protected, by default, with two-factor authentication. In addition, using the information provided by a customer, IntSights’ patented artificial intelligence capabilities and cyber reconnaissance algorithms generate millions of additional customer-specific asset variations to ensure an exhaustive, yet tailored, information-gathering process.

**IntSights’ Enterprise Threat Intelligence and Mitigation Platform: Key Features**

- **Tailored threat intelligence.** The system’s monitoring service scans the surface, deep and dark web to detect external risks and early-stage indicators of attacks on an enterprise’s digital footprint and/or brand. These are known as pre-indicators of attack.

- **Aggregated data feeds.** IntSights aggregates external threat data (from sources such as malicious web addresses, social media pages, IP addresses, malicious domain lists, and even dark-web activity) that would help threat actors target systems and people within an organization. It also aggregates internal system data collected about threats, as well as data from open-source and industry threat feeds to correlate and enrich the data feeds used by investigators and detection systems.

- **Prioritized alerting.** IntSights’ platform includes reliable mechanisms for prioritizing and scoring potential risks and sending alerts.

- **Dark-web research.** IntSights gathers and maintains an emerging threat database from the dark web and other sources, including malware, threat actors, tools and techniques, and active campaigns, and applies additional relevant context to the threat intelligence mix.

- **Multiplatform workflow.** IntSights enables workflow across platforms for incident response and automated remediation of internal threats (such as leaked credentials, exposed employee lists, etc.) and external threats (such as the takedown of malicious IPs, mobile applications and paste sites).

**Sourcing from the Dark Web**

The term dark web refers to overlay networks that operate on top of the Internet and commonly host malicious hackers as well as software communities that tend to share information that intelligence providers can use to identify threats. Dark-web sources include, but are not limited to, black markets and malicious forums.
Customization

We began by defining the assets specific to our mock review environment. These assets include, but are not limited to, our “mock” organization’s domains, IP addresses, company names and social media pages. IntSights’ platform scours the web looking for any threat information related to the identified assets. It then reports and alerts on this information. These alerts and reports provide the user with a high level of assurance that the threats are real.

Asset Population

IntSights uses the asset information for deep customization and to narrow search filters so that they look only for and alert only on vulnerabilities and threats related to the organization’s systems. This greatly reduces the noise coming from the organization’s other security devices and provides actionable intelligence to the user.

A screenshot of the asset inventory page is shown in Figure 1. This is where we added our mock company-specific assets to facilitate tailored CTI. We added our sample assets manually, but users can import them from a file, which makes things easier when dealing with a long list of assets. Adding the assets manually took a trivial amount of work in our mock review environment, but in a real-world deployment, we definitely would import the assets from a list.

Dashboard and Drilldown

The dashboard provided a tremendous amount of threat intelligence tailored to our mock organization and presented in an easy-to-digest format. The dashboard has two panes. The top pane contains threat information found on the clear web that indicates potential future attack attempts against the organization. When threat information appears in the dashboard, this is a good indicator that the organization is being targeted.

Clear web

The part of the Internet that is searchable by well-known search engines such as Google, Bing and Yahoo. It includes public domains and IP addresses, social media sites, public company websites, paste sites and other locations from which attackers can gather data on their targets before initiating an attack.

Please Do Overshare

Our mock environment had 150 attributes reported to IntSights for customization; the full IntSights platform allows up to 10 million assets to be added. The more assets listed, the more tailored the intelligence will be. Listing domain names, for example, allows the platform to alert on any leaked login credentials and email address information. Some examples of other asset information that can be added into the platform include:

- Company names
- Domains owned by the organization
- IP addresses that should be monitored
- VIP email addresses, such as those of an organization’s senior management team
- Brand names associated with the organization
- Official social media pages
- Mobile and browser apps
- Technologies in use, such as Chrome or Microsoft Office
- DLP indicators
- Login pages for any of the company’s websites
From the dashboard, we saw a summary count of attack indicators that IntSights had discovered relating to data leakage, phishing and exploitable data. An example of this is shown in Figure 2.

We also saw attack pre-indicators from external threat sources, including those with the potential to harm or damage the brand and those that posed threats to company VIPs. Then we drilled down to get more detailed information about the attack types.

An example of an alert revealing that company employees had been discovered on a target list is shown in Figure 3.

**Severity Rankings**

Alerts contain severity rankings that help users focus on the highest-risk threats. They also recommend the next course of action. In this example, the alert recommended notifying the targeted employees. As part of its external threat-takedown functionality, the platform also provides the option to assist with removing the malicious page with a single click of the “remediate” button.

**Remediation and Workflow**

We were not left to fend for ourselves once an issue was reported. We drilled down on the compromised usernames and passwords to gain more context on this incident.

Two alerts occurring one day apart in our mock scenario are shown in Figure 4.

The email addresses of company employees appeared on a target list on July 3. Then, on July 4, a large number of passwords and usernames of employees was leaked. This indicated that attackers took advantage of the target list and immediately began using social engineering or phishing attacks to uncover employee credentials.
**Remediation Assistance**

On our initial alert page, as shown in Figure 3, we had additional remediation options in the tabs to the right of the alert.

1. The first option is **Mail**, which the investigating team can use to send an email alert to other team members or to an external forensics team.

2. The next option is to use **Ask the Analyst**, which sends an inquiry to a live IntSights analyst on any topic related to the alert reported in the dashboard, including how to handle and remediate a threat.

3. The next option is to **Remediate** the alert. This is known as **external takedown**. The team at IntSights, with the customer’s approval, will take action on the customer’s behalf. In this case, the IntSights team will contact the owner of the site hosting the leaked list and request its removal. This removes a significant burden from the organization’s security team.

4. The **Whitelist** option prompts the IntSights team to categorize the alert as a false positive so that it won’t be flagged as a potential incident in the future.

5. To **Archive** an alert is to remove it from the list of current alerts. A user might do this if IntSights is working on an external takedown for the user’s organization, for example; the user archives that alert and is left with a view of only those alerts on which no action has yet been taken. (Archived alerts can be viewed periodically to determine status.)

6. The **Investigate** tab provides great value. It presents a timeline showing all alerts with similar severity. This can tell the customer’s investigation team a story of what has occurred by showing things such as leaks and last alert in the timeline. It may be possible, using this feature, to conclude that all threat activities are related.

**Dark Web**

We can also get perspective from other external threats tailored to the organization found on the dark web. The layout is the same as the clear-web interface, but the threat sources are different. Examples of dark-web sources are shown in Figure 5.

These sources include, but are not limited to, black markets, malicious forums and paste sites.

---

*The attack timeline presents a story of what happened before the phishing attack started, providing a deeper understanding of the attack progression, timing and techniques—all of which we can use to quickly detect and block attacks at the onset of a phishing campaign.*

---

*Figure 5. Tailored Intelligence from Scanning the Dark Web*
Finding tools or solutions to comb the dark web is a challenge. This is especially true when it comes to putting into context the information found in the dark web. Utilizing a service such as IntSights’ that scour the dark web looking for suspicious activity related to a company’s specifically defined assets is a significant value in terms of time and providing actionable intelligence.

Each individual attack type can be clicked on to see more detail. When we examined data leakage, as shown in Figure 6, we saw that the company’s database was for sale on the dark web.

It showed the seller’s handle along with the website on which the database was being sold. We also searched for any employee login credentials that may have been leaked. The IntSights Enterprise Threat Intelligence and Mitigation Platform discovered that login credentials were leaked on the dark web. This is a straightforward task that a security analyst could perform daily. It takes minutes, if not seconds, to run the search. The alert description provides the right level of detail for a user to quickly understand what occurred. See Figure 7.

This may not have been discovered for months without the dark-web and clear-web scan results provided by IntSights services.

**Reports**

From the reports tab, we ran an Executive Summary report showing the severity of reported threats. We scrolled through the Executive Summary to determine the threat sources. The report is useful to demonstrate to executives how severe the threats against the company are.

Now that we know our database is for sale on the black market, we can respond to the external threat and shut it down, rather than discover this information late from outside sources, such as attacker and malware forums, complaints from customers and clients, or the media.

Someone in a senior management role can read the Executive Summary and understand the level of attack severity and the threats against the organization that exist on both the clear and dark webs.
Apart from the Executive Summary, the report tab has a number of options that users can run either on a scheduled basis or on demand. A severity report broken down by quarter is shown in Figure 8.

The information in this report describes the sources that revealed the threat and the top three alerts discovered on both the clear and dark webs against which analysts should take action.

**IoC Management**

The IoC dashboard, shown in Figure 9, provides a high-level summary of any IoCs.

The summary breaks out this information into severity levels and IoC types and includes IP addresses, domain names, URLs and hashes. A big challenge with IoCs is their varying reliability and a lack of context, which can leave analysts without the confidence they need to take action. To address this, IntSights has developed an IoC confidence level to indicate the level of legitimacy the intelligence has. Higher confidence levels are given to IoCs that have been corroborated by multiple sources, confirmed by other independent sources and analyzed to determine that the threat is real.

We could also drill down on a specific IoC type, as shown in Figure 10.

Clicking on “IP addresses” in the graph took us to another window, which displays malicious IP addresses. From there, we could either search by a particular IP address or retrieve a list of malicious IP addresses within a specific date. We could then use that information to search for any connection made to those IP addresses from our internal security devices, such as a firewall or web proxy.

*IntSights enriches IoCs by associating them with known malware, indicating whether they are part of a malicious URL link, enumerating the online scanners such as VirusTotal that flagged them as suspicious and more.*
After seeing an IP address of interest, we entered it in the Investigation pane to retrieve more information, as shown in Figure 11.

By noting the malicious characteristics found when searching for the suspect IP address, we could create a more refined IoC to use when searching our environment. This helps in reducing false positives.

**Threat Feeds**

IntSights has built its own cyber threat feeds for use by its customers. These CTI feeds are based on research conducted by IntSights’ analysts, as well as cyber threat alerts and reputable blacklists showing malicious domain names and IP addresses. An example of such a feed is shown in Figure 12.

IntSights' platform takes information from reputable third-party sources for its threat feeds, including any services to which the customer subscribes. This aids in adding more high-fidelity data to the overall product suite.

In this case, IntSights’ Enterprise Threat Intelligence and Mitigation Platform allows us to configure well-known private feeds. One example is FS-ISAC, a service used by the financial industry to research cyber and physical threats and to share intelligence. See Figure 13.

IntSights also includes threat feeds from retail-specific forums, as shown in Figure 13. These types of sources are used by retailers to share threat information and best security practices for their industry, including safeguarding customers’ personally identifiable information.
**Internal Threat Detection and Remediation**

The IntSights Enterprise Threat Intelligence and Mitigation Platform helps automate remediation tasks by integrating with security devices, user directories and other sources to consume and push intelligence information. This is known as internal threat remediation. IntSights integrates with internal tools, such as Active Directory, firewalls, web proxies, endpoint security solutions and SIEMs, using a virtual machine that can be downloaded from IntSights’ portal and kept on-premises. It communicates with the IntSights platform in the cloud and the customer’s on-premises security devices. The tool supports integration with products from numerous reputable vendors that are commonly used today.

**How does it work?**

1. Place an IntSights virtual appliance on the company’s network. This can be on-premises or in the cloud, but it must communicate with IntSights’ Management service in the cloud.
2. The customer’s IntSights service continues to collect intelligence on activities that could indicate threats.
3. IntSights assesses these activities against its intelligence database to validate that these are threats to the customer.
4. The virtual appliance (on-premises) consumes these enriched IoCs, which are retrieved from IntSights’ cloud-based platform.
5. The virtual appliance sends these IoCs information, such as malicious domains or IP addresses, to a customer’s security appliances.
6. The security appliances can then enforce these IoCs in their defenses and potentially stop any attacks involving them.

How a virtual appliance automatically pushes this type of intelligence (for blacklisting domains, IPs, etc.) to an on-premises security device is shown in Figure 14.

As you can see in Figure 14, some well-known security vendors support this push method.
Security devices can also be used to “pull” the IoCs from IntSights through this virtual appliance. An example of this is shown in Figure 15. This information can be added to a user’s malware and malicious domain blacklists.

**Internal and External Intelligence Combined**

Integrating the virtual appliance with Active Directory helps complete the intelligence circle. When IntSights detects compromised or leaked accounts on the web, it automatically cross-references those accounts with a user’s Active Directory contents. This is how it identifies and then alerts a user that its employees are being targeted for phishing well before an actual phishing attempt can be launched. It also provides recommendations to remediate the threat potential, such as to immediately change passwords for each targeted account. See Figure 16.

This is a valuable service, especially in today’s threat landscape. IntSights’ platform scours the web—dark, deep and clear—for compromised or leaked accounts for those domains specified in the assets page. This type of due diligence can be challenging for an organization to execute because it may lack the knowledge, tools and appropriate resources.

**Internal IoC Remediation**

During a security incident, blocking an attempted attack in a timely manner is paramount to minimize any potential damage.

In one use case, IntSights Enterprise Threat Intelligence and Mitigation Platform discovered malicious command-and-control IP addresses, then pushed that information to our virtual appliances. The appliances subsequently sent the IoC information to the integrated security appliances (our firewalls, directories, etc.), thus blocking any attacks involving those IP addresses. It can, if configured and tested properly, complete these tasks without human intervention.

**TAKEAWAY:**

Had this been a manual effort, the IoC may not have been discovered until much later, after the attack succeeded.
Conclusion

According to the CTI survey, 41% of respondents feel that CTI is maturing. Most feel it is a necessary tool for response teams. It still has its challenges, however. Some of the biggest barriers to implementing CTI are a lack of appropriate staff skills and the inability to handle large amounts of intelligence information and to apply the appropriate context to this intelligence.

Many of these issues have been addressed by the IntSights Enterprise Threat Intelligence and Mitigation platform, through its tailored and actionable intelligence, internal remediation, external remediation and IoC management capabilities.

The most effective way to utilize the IntSights Enterprise Threat Intelligence and Mitigation Platform and all its capabilities is to, first, fully identify all assets that must be protected. This allows the IntSights Enterprise Threat Intelligence and Mitigation Platform to tailor its intelligence more successfully based on what it knows about your organization.

Leverage the tool’s internal remediation component by integrating the IntSights virtual machine with your security systems. If it is too early to turn on prevention, then use this capability to detect malicious behavior. It is a good strategy to leverage IntSights’ automation to more rapidly prevent or detect malicious activity.

About the Author

Sonny Sarai, SANS GIAC Advisor, has more than 10 years’ IT experience, seven of them in an information security capacity. He now works in the Retail industry and is responsible for data governance, compliance, penetration testing, digital forensics and incident response. Sonny holds a degree in forensic investigation, specializing in computer crime. He holds a CISSP and industry-leading certifications from SANS in advanced digital forensics (GCFA), network intrusion detection (GCIA) and security essentials (GSEC). Sonny has an extensive lab dedicated to research, development and analysis, where he continually hones his skills and enhances his capabilities.

Sponsor

SANS would like to thank the sponsor of this product review.

INTSIGHTS
Threat Intelligence Realized.
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Melbourne 2018</td>
<td>Melbourne, AU</td>
<td>May 14, 2018 - May 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA Reston Spring 2018</td>
<td>Reston, VAUS</td>
<td>May 20, 2018 - May 25, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam May 2018</td>
<td>Amsterdam, NL</td>
<td>May 28, 2018 - Jun 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Atlanta 2018</td>
<td>Atlanta, GAUS</td>
<td>May 29, 2018 - Jun 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Rocky Mountain 2018</td>
<td>Denver, COUS</td>
<td>Jun 04, 2018 - Jun 09, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training 2018</td>
<td>Austin, TXUS</td>
<td>Jun 07, 2018 - Jun 14, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud INsecurity Summit - Washington DC</td>
<td>Crystal City, VAUS</td>
<td>Jun 08, 2018 - Jun 08, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud INsecurity Summit - Austin</td>
<td>Austin, TXUS</td>
<td>Jun 11, 2018 - Jun 11, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Milan June 2018</td>
<td>Milan, IT</td>
<td>Jun 11, 2018 - Jun 16, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Europe Summit and Training 2018</td>
<td>Munich, DE</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2018</td>
<td>Manila, PH</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Crystal City 2018</td>
<td>Arlington, VAUS</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Oslo June 2018</td>
<td>Oslo, NO</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Minneapolis 2018</td>
<td>Minneapolis, MNUS</td>
<td>Jun 25, 2018 - Jun 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Vancouver 2018</td>
<td>Vancouver, BCCA</td>
<td>Jun 25, 2018 - Jun 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cyber Defence Canberra 2018</td>
<td>Canberra, AU</td>
<td>Jun 25, 2018 - Jul 07, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Charlotte 2018</td>
<td>Charlotte, NCUS</td>
<td>Jul 09, 2018 - Jul 14, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cyber Defence Bangalore 2018</td>
<td>Bangalore, IN</td>
<td>Jul 16, 2018 - Jul 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Malaysia 2018</td>
<td>Kuala Lumpur, MY</td>
<td>Jul 16, 2018 - Jul 21, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Riyadh July 2018</td>
<td>Riyadh, SA</td>
<td>Jul 28, 2018 - Aug 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pittsburgh 2018</td>
<td>Pittsburgh, PAUS</td>
<td>Jul 30, 2018 - Aug 04, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Boston Summer 2018</td>
<td>Boston, MAUS</td>
<td>Aug 06, 2018 - Aug 11, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2018</td>
<td>OnlineCAUS</td>
<td>May 11, 2018 - May 18, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>