Dashboard

Dashboard is fully customizable. Widgets can be reordered or deleted into a workflow that best matches analyst needs. Each widget or module has a level of interactivity appropriate for that widget and what it seeks to accomplish. A CSV or PDF file can be downloaded from each.
At a Glance

At a Glance has a petri dish visual representation; blue dots are representative of active cases within the portal; red dots are “AT&T Threat Intellect Cases.” The appearance of red dots signifies the need for an analyst to intervene and contact the customer for further exploration/mitigation/remediation.
Log Security Health

Log Security Health has 3 criteria to assess a customer’s security posture at any point in time:

Case Management – the frequency with which customers touch the active cases
Case Resolution – how many cases have closed within the last 48 hours, and how long it is taking to close cases overall
Case Posture – expands on Case Resolution to look at a 7-day period

You can also see the letter grade customers are given based on this performance for today as well as for the six days prior.
Customers can do a simple keyword search, or use the “Advanced” button to build Custom Searches. Once a Custom Search is built, it can be saved for personal use or to be used within the organization. These can be accessed in the “Advanced” tab.
Custom Search

This is where a Custom Search is built. These can be developed to search Events, Alerts, and Cases. Lines can be added to any query.
Alerts

Within Alerts, you can filter the data to reduce the dataset you're looking for. You can click on the severity levels to showcase only those Alerts that fall into a particular category. In the top right, you can download these Alerts in a CSV file format, which will be available in the Message Center.
Cases

Within Cases, the interface looks strikingly similar to that of Alerts. The same functionality exists for both. Clicking into a particular Case will show more detail.
Case Details

Clicking on the Case number hyperlink will show the details above which are entered by AT&T SOC Analysts and can be edited by the customers themselves.
Case Alerts

When the “Alerts” tab is clicked, all of the Alerts associated with this particular case are populated.
Some additional ideas that a security analyst may want to explore relative to this APT event. *A PT* file archive type is typically used to bundle files and documents for exfiltration with respect to this APT activity. An analyst should look for any file ending in .apt especially if that type of archive isn’t used much within your enterprise. They might find other information that has been or will be exfiltrated. *In some instances, our analyst team has observed the initial infection vector to begin from a carefully crafted spear-phishing email which is sent to only a small set of targeted victims in the company. The context of the email is usually on top and relevant to the target victim’s industry and may be spoofed to appear to come from someone that the victim communicates with. Usually inside the email is a link or attachment containing a malicious payload. Sometimes this is buried inside an Excel spreadsheet, PDF, or some other seemingly innocent file format. Based on this, an analyst may want to look at log files for messages from outside the company that went to all of those affected users especially if it had attachments. This might indicate an initial infection time if there were other recipients, they might be infected also. * We observed in previous cases that the attackers often try to compromise the company email servers directly and add additional malware to periodically harvest email from the email server for specific individuals in the company. A thorough analysis of your email server’s logs would be warranted. If Mitigation failure often recommended that victim companies audit their DNS logs if possible for DNS lookups to the “malicious domain” for their company. This could uncover additional compromised assets. Also, where possible some customers have taken action to block these malicious domains and even the entire second-level domain (which are usually uncommon dynamic DNS domains) to a singlehole server in their organization. The singlehole server could be monitored for incoming activity for victim workstations inside the company and may uncover more compromised systems. 3. Law Enforcement Notification Finally, we recommend contacting the FBI in regard to this activity. FBI has been investigating related events. They likely will be able to provide more information and provide advice on remediation steps. If you are working with a local field office, please have the investigating agent contact either of the agents below. This would help ensure that the information and guidance you can get information on other aspects of the investigation, (503) 535-9299/2975, [AgentSmith@]@agentSmith.com Special Agent FBI Number One, Happy Street TX 553-55S-2933 [HappiJ@]@ScMithHand@agentGanger.gov

I was informed we blocked the outbound DDS. I am not 100% sure of the status of the desktops but action was taken to have a program on them. Are you still seeing this activity or similar activity? Are we sure that they are the malware does not go to another target? If this DDS is blocked also that IP is registered to a K/T in North Carolina so are they just a compromised actor?

Were you able to identify the system in your network? We are categorizing this activity as Critical and recommend that you block the destination IP on the firewalls. Please contact me or the SETA SOC (877-757-7368) if you need additional support.

Thanks but we need to know specific firewalls. Our business is distributed worldwide, and NaNed IP addresses may frequently be reused. Example: There might be a 10.159.999 assigned to different machines in China, Canada, New York and Florida. The name and IP of the firewall can immediately tell us what location were dealing with.

It appears you are the victim of a Trojan that is intended to exfiltrate (also) information from within your private network. The security team at AT&T identified this in the course of identifying and tracking malicious Internet activity, which includes some activity that is highly suspicious of data theft. Several flows of traffic were identified to a suspected drop server on the Internet from your network. The activity from your network came from address (193.149.203.193) predominantly between the times and dates indicated in the table below. The traffic was to the address 193.42.58.45 on port 9443 (S4A), which is a suspected drop server for data theft activity. AT&T can be as hands on as the customer prefers.
Documents
The Documents repository is where customers will upload information such as their Network Topology Diagram, Incident Response Plan, Contact Names and Phone Numbers, etc. This feature is included to allow Threat Manager to be a completely out-of-band way for customers to communicate with the AT&T SOC Analysts.
## Reports

Threat Manager provides customers with basic Reports they can generate to be available for download within the Message Center. In addition, if a certain report is not available, AT&T Security Consulting will be available (during service turn-up) to build custom reports on an as-needed basis.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Generate</th>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Severity by Day</td>
<td>Alert severity and the number of alerts that were opened in the selected time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alerts Summary by Destination IP</td>
<td>Overall alerts summary by Destination IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alerts Summary by Severity</td>
<td>Overall alerts summary by Severity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alerts Summary by Source IP</td>
<td>Overall alerts summary by Source IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case Severity by Day</td>
<td>Case severity and the number of cases that were opened in the selected time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case Summary</td>
<td>Overall cases summary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events Summary by Destination IP</td>
<td>Overall summary of events by Destination IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events Summary by Device Class</td>
<td>Overall summary of events by Device Class</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events Summary by Event Type</td>
<td>Overall summary of events by Event Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events Summary by Hostname</td>
<td>Overall summary of events by Hostname</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events Summary by Source IP</td>
<td>Overall summary of events by Source IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events Summary by User</td>
<td>Overall summary of events by User</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Rows Per Page: 20
Message Center

The Message Center is where collaboration happens between customers and AT&T. This is also where customers can download reports once they are generated.