In our global economy where everything is connected to the internet, data is our most valuable currency.
AT&T’s approach to cybersecurity

- **24x7 global situational awareness**
  Near real-time analysis of security indicators

- **Operate largest IP/MPLS Core Infrastructure**
  Real time global situational awareness
  Integrated management and response capability

- **Embed security capabilities into the network**
  Security enforcement nodes
  Enterprise protection/managed services
Providing value-deep visibility, analytics, and response

**Extensive visibility**
- 62.6 Petabytes of data traffic passes through the AT&T Network on an average business day

**Robust security analytics**
- Hundreds of millions of events reduced to hundreds of actionable alerts daily

**Expert threat response & mitigation**
- 24x7 redundant Security Operations Centers
- Approximately 2000 security experts

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo and other marks are trademarks of AT&T Intellectual Property.
Identifying the anomalies

Normal patterns of behavior emerge...

...and the anomalies quickly stand out
Source Information Useful to ISPs – Tangible/Contextual

<table>
<thead>
<tr>
<th>Tangible</th>
<th>Contextual</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IP address, 1.2.3.4</td>
<td>• Attacker group, e.g. Anonymous, APT1</td>
</tr>
<tr>
<td>• Domain name, <a href="http://www.baddomain.com">www.baddomain.com</a></td>
<td>• Botnets, e.g., ZeroAccess</td>
</tr>
<tr>
<td>• URL</td>
<td>• Incident, e.g., DDoS attack on 2014-Jan-8 @ 0100 UTC</td>
</tr>
<tr>
<td>• Email address, <a href="mailto:badguy@gmail.com">badguy@gmail.com</a></td>
<td>• Threat advisory, e.g., FBI flash 00034</td>
</tr>
<tr>
<td>• File hash</td>
<td>• Exploit example, e.g., Heartbleed exploit</td>
</tr>
<tr>
<td>• SSL certificate IDs</td>
<td>• Attack trends, e.g., protocols used in distributed reflection DoS</td>
</tr>
<tr>
<td>• Network detection signatures</td>
<td>• Activity pattern, e.g., reverse web behavior</td>
</tr>
<tr>
<td>• ASNs networks with frequent problems</td>
<td>• Algorithm/code, e.g., domain name</td>
</tr>
<tr>
<td>• Hosting provider</td>
<td>• Campaign, e.g., operation confusion</td>
</tr>
<tr>
<td>• MSISDN/IMEI – Phone number/Identifier of</td>
<td>• Named actors, e.g., John Smith a.k.a. JohnSmith</td>
</tr>
<tr>
<td>compromised or vulnerable device type</td>
<td></td>
</tr>
<tr>
<td>• SMS short code - spam or malware link</td>
<td></td>
</tr>
<tr>
<td>source</td>
<td></td>
</tr>
</tbody>
</table>

Note: These are examples of information that may be used by network service provider cyber practitioners to detect cyber threats. This is not intended to imply that this information is shared with third parties which requires a different analysis including of the privacy implications involved with sharing.
AT&T global security nodes, botnet illustration
Evolution of threat management

Traditional approach

- Monitor traffic in and out of perimeter
- Compare against known signatures
- Generate alerts to SOC for investigation

The traditional approach is changing

- What’s the perimeter?
- Threats evolving at increasing rate
- Overwhelming amounts of data from many sources across complex environments

Effective threat management must...

- Aggregate data from multiple sources
- Turn data into information
- Respond real-time with changes to policies and filtering
Perimeter security?

70% of threats go undetected by anti-virus software

29% work from multiple locations, using multiple devices and apps
Evolution to Simple, Efficient Network Environment

Protection in the Network Across Wireline & Wireless

- Network Based Firewall
- Email & Web Security
- DDoS Protection
- Policy Controls
Current Policy Issues

- President’s Information Sharing Executive Order (Issued 2/13/15)
- Information Sharing/Data Breach/CFAA Reform Legislation
- NIST Framework
- FCC Communications Security, Reliability and Interoperability Council