Building Your Defensive Line: Selecting MSS to Increase Your Cyber Resilience

Greg Gray
Patrick Dalton
**What is MSS?**

- **Asset Discovery**
  Know who and what is connected to your environment at all times.

- **Vulnerability Assessment**
  Know where the vulnerabilities are on your assets to avoid compromise.

- **Intrusion Detection**
  Know when suspicious activities happen in your environment.

- **Endpoint Detection & Response**
  Continuously monitor your endpoints in the cloud and on premises to detect threats and changes to critical files.

- **Behavioral Monitoring**
  Identify suspicious behavior and potentially compromised systems.

- **SIEM & Log Management**
  Correlate and analyze security event data from across your network and respond.

- **Security & Compliance Reporting**
  Pre-built, customizable reports for regulation standards and compliance frameworks.

History of SEDC MSS

• SEDC MSS (powered by AlienVault)
  • 3 pilots in Q4 2016
  • Serving 36 utilities today
• SEDC EDR (powered by Carbon Black)
  • Serving 15 utilities today
• SEDC MFA (powered by Duo)
  • Serving 15 utilities today
Millions of Events Daily (36 Clients)
1000+ Alarms Daily (36 Clients)
DNS Reply Sinkhole (TP or FP)

- True Positive Alarm
- Malware on Android phone on corporate WiFi contacting DNS sinkhole in Portugal

DNS Reply Sinkhole (TP or FP)

• False Positive Alarm but still sketchy and requires research
• Firewall is making reverse DNS lookups to determine domain name of IP from Russia who was port scanning utility
• Domain registered by Dom Tehniki Ltd. from Russia
False Positive Alarm

<table>
<thead>
<tr>
<th>EVENT NAME</th>
<th>DATE (GMT-03:00)</th>
<th>SENSOR</th>
<th>OTX</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>SonicWALL: TCP connection dropped</td>
<td>2019-07-11 11:43:16</td>
<td></td>
<td>![Sensor Icon]</td>
<td>46.3.96.69:46456</td>
<td></td>
<td>LOW (0)</td>
</tr>
<tr>
<td>SonicWALL: TCP connection dropped</td>
<td>2019-07-11 08:34:39</td>
<td></td>
<td>![Sensor Icon]</td>
<td>46.3.96.69:46456</td>
<td></td>
<td>LOW (0)</td>
</tr>
<tr>
<td>SonicWALL: TCP connection dropped</td>
<td>2019-07-11 04:00:33</td>
<td></td>
<td>![Sensor Icon]</td>
<td>46.3.96.69:46456</td>
<td></td>
<td>LOW (0)</td>
</tr>
<tr>
<td>SonicWALL: TCP connection dropped</td>
<td>2019-07-11 02:32:09</td>
<td></td>
<td>![Sensor Icon]</td>
<td>46.3.96.69:46456</td>
<td></td>
<td>LOW (0)</td>
</tr>
<tr>
<td>SonicWALL: Initiator from country blocked: %s</td>
<td>2019-07-11 00:59:05</td>
<td></td>
<td>![Sensor Icon]</td>
<td>46.3.96.69:48098</td>
<td></td>
<td>LOW (0)</td>
</tr>
<tr>
<td>SonicWALL: TCP connection dropped</td>
<td>2019-07-11 00:13:37</td>
<td></td>
<td>![Sensor Icon]</td>
<td>46.3.96.69:48098</td>
<td></td>
<td>LOW (0)</td>
</tr>
<tr>
<td>SonicWALL: TCP connection dropped</td>
<td>2019-07-10 19:06:26</td>
<td></td>
<td>![Sensor Icon]</td>
<td>46.3.96.69:48098</td>
<td></td>
<td>LOW (0)</td>
</tr>
<tr>
<td>SonicWALL: TCP connection dropped</td>
<td>2019-07-10 02:13:28</td>
<td></td>
<td>![Sensor Icon]</td>
<td>46.3.96.69:432628</td>
<td></td>
<td>LOW (0)</td>
</tr>
<tr>
<td>SonicWALL: TCP connection dropped</td>
<td>2019-07-09 17:46:06</td>
<td></td>
<td>![Sensor Icon]</td>
<td>46.3.96.69:432628</td>
<td></td>
<td>LOW (0)</td>
</tr>
<tr>
<td>SonicWALL: TCP connection dropped</td>
<td>2019-07-09 07:51:12</td>
<td></td>
<td>![Sensor Icon]</td>
<td>46.3.96.69:52758</td>
<td></td>
<td>LOW (0)</td>
</tr>
</tbody>
</table>
False Positive Alarm

**Basic Information**

- **LOCATION:** Russian Federation
- **ASN/OWNER:** AS202984 Chernyshov Alexandr Aleksandrovich
- **FIRST SEEN:** May 27, 2019, 2:52/27/2019 2:40:33 AM
- **LAST SEEN:** Jul. 12, 2019, 8:7/12/2019 8:02:56 AM

**Threat Summary**

- **THREAT SCORE:** 2 (out of 7)
- **OBSERVED ACTIVITY:** Malicious Host
- **Actively Malicious**

**External Sources**

- ☰ Whois
- 🔄 VirusTotal

**Observed Malicious Activity**

<table>
<thead>
<tr>
<th>Show 10 entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>FINDING</td>
</tr>
<tr>
<td>46.3.96.69 hostile</td>
</tr>
</tbody>
</table>
## The Importance of Threat Intelligence

<table>
<thead>
<tr>
<th>THREAT</th>
<th>DISCOVERED</th>
<th>AVAILABLE FOR ALIENVault CUSTOMERS</th>
<th>TIME TO DETECTION ABILITY IN USM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meltdown / Spectre</td>
<td>January 3, 2018</td>
<td>January 4, 2018</td>
<td>1 day</td>
</tr>
<tr>
<td>“Petya” / NotPetya</td>
<td>June 27, 2017</td>
<td>June 27, 2017</td>
<td>Same day</td>
</tr>
<tr>
<td>WannaCry</td>
<td>May 12, 2017</td>
<td>May 12, 2017</td>
<td>Same day</td>
</tr>
<tr>
<td>Samba CVE-2017-7494</td>
<td>May 25, 2017</td>
<td>May 25, 2017</td>
<td>Same day</td>
</tr>
<tr>
<td>EternalBlue</td>
<td>April 14, 2017</td>
<td>April 18, 2017</td>
<td>4 days</td>
</tr>
<tr>
<td>WordPress Content Injection</td>
<td>February 1, 2017</td>
<td>January 26, 2017</td>
<td>6 days BEFORE</td>
</tr>
<tr>
<td>Adobe 0-day (CVE-2015-0311)</td>
<td>January 22, 2015</td>
<td>November 16, 2014**</td>
<td>3 months BEFORE</td>
</tr>
</tbody>
</table>
SEDC SOC - Atlanta, GA

SEDC MSS (Managed Security Services)
Why SEDC MSS?

• SEDC MSS is Cost Effective
  • Under SEDC umbrella, utility gains Security Operations Center (SOC) experts at a fraction of the cost
• 24x7 monitoring
  • of your network so you don’t have to...
• PCI-DSS
  • Satisfy 37+ of the most challenging PCI-DSS requirements while improving the security of your network
Sign up with SEDC MSS!

Please contact techsales@sedata.com or cri@sedata.com