The **N-Sentinel** cloud-based managed security services are designed specifically for utilities, delivering continuous cyber threat vigilance and comprehensive remediation guidance. With timely awareness and insights about cyber threats, along with actionable information and access to cybersecurity experts, customers can take action to protect their networks, data and assets from cyber risks.

The first step in protecting your utility from cyber risks is knowing how and where its vulnerable. If your utility has been the target of cyber threats or if you’re unsure about how vulnerable it may be, we have the solutions for you that work hand-in-hand as part of a comprehensive layered security strategy.

**N-SENTINEL MANAGED SECURITY SERVICES**

**N-Sentinel Monitoring /** Delivers continuous monitoring of network traffic, detecting, analyzing and alerting on cybersecurity threats, malware, and viruses. Biweekly reports offer visibility into a utility’s cyber risks, the priority in which they should be addressed based upon severity, and specific steps that can be taken to improve reduce risk. Cybersecurity experts review reports with customers and are available to assist in answering additional questions.

**N-Sentinel Vulnerability Assessment /** Provides on-demand assessment of endpoints (including servers, industrial control systems, desktops/laptops, smart phones and more) connected to a network, providing an up-to-date view of latent vulnerabilities in operating systems and applications. Daily reports offer visibility into cyber risks, recommendations and prioritization of the vulnerabilities that should be addressed and specific guidance on remediation. Alerts provide awareness of new vulnerabilities as they are discovered. Cybersecurity experts are available to review reports and answer customer questions.

**FEATURE OVERVIEW**

- 24 x 7 cybersecurity threat monitoring and alerts
- Intelligent cloud-based threat analysis & false positive reduction
- Actionable threat intelligence
- Utility community cyber intelligence
- Access to cybersecurity experts
- Secure web-based customer portal
- Helps meet NERC CIP compliance
- Affordable managed security service

**N-SENTINEL SOLUTION DETAIL**

<table>
<thead>
<tr>
<th>Threat Detection</th>
<th>N-Sentinel Monitoring</th>
<th>N-Sentinel Vulnerability Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-depth Threat Insights</td>
<td>Active</td>
<td>Passive</td>
</tr>
<tr>
<td></td>
<td>Live network traffic</td>
<td>Endpoint devices</td>
</tr>
<tr>
<td></td>
<td>Actual attacks &amp; attackers</td>
<td>Exploitable vulnerabilities</td>
</tr>
<tr>
<td>Security Policy Violations</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Malware &amp; Viruses</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Software &amp; OS Vulnerabilities</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Reconnaissance, Exploit Attempts, DOS/DDOS</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Rogue Devices</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Asset ID</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
WHY N-SENTINEL

• **Continuous operation and alerts**
  With the number and breadth of cyber threats that can impact the reliable delivery of power, 24 x 7 vigilance and awareness of vulnerabilities is essential.

• **Actionable threat intelligence**
  Visibility into cyber incidents; identification on which systems are vulnerable; guidance on specific actions to take to mitigate risks.

• **Utility community cyber intelligence**
  Threat trends are monitored across the community enabling advanced warning about attacks starting to affect some members, enabling preemptive action. Utilities can also view how their security posture is performing compared with other similar utilities.

• **Cybersecurity expert assistance**
  In-house cybersecurity experts review the cybersecurity data and guide utilities in taking timely and appropriate actions to reduce risk and improve their security posture.

Contact us to find out what cyber threats are putting your networks, data and assets at risk.

www.n-sentinel.com