AI's Machine Speed Should Accelerate Threat Detection, Investigation, and Response

The WannaCry outbreak and its lateral movement emphasize the importance of deploying AI in a virtual security analyst role to help handle cyber threats quickly and efficiently. This ransomware outbreak was identified and responded to in sub-second time frames, dramatically reducing the time required for investigation and response.

### Before:

- **Identify**: 1+ hrs
- **Investigate**: 4+ hrs
- **Respond**: 2+ hrs
- **Close Ticket**: 30+ mins

### After: AI Integrated with Security Controls:

- **Identify**: sub-second
- **Investigate**: <5 mins
- **Respond**: <30 mins
- **Close Ticket**: <5 mins

### Example of Threat Response Life Cycle

<table>
<thead>
<tr>
<th><strong>Phase</strong></th>
<th><strong>Before</strong></th>
<th><strong>After</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>1+ hrs</td>
<td>sub-second</td>
</tr>
<tr>
<td>Identify</td>
<td>&lt;5 mins</td>
<td>&lt;30 mins</td>
</tr>
<tr>
<td>Respond</td>
<td>2+ hrs</td>
<td>&lt;30 mins</td>
</tr>
<tr>
<td>Close Ticket</td>
<td>30+ mins</td>
<td>&lt;5 mins</td>
</tr>
</tbody>
</table>

### Key Features of AI for Threat Response:

- **Self-learning**: AI can learn from previous threats and improve its accuracy over time.
- **Fast response**: AI can react in real-time to threats, reducing the time to respond.
- **Efficiency**: AI can automate tasks, freeing up human analysts to focus on more complex threats.

Al's Machine Speed Should Accelerate Threat Detection, Investigation, and Response

Solving WannaCry with SecOps analyst augmented with deep neural networks helps mitigate the effects of this skills gap and more rapidly detect and respond security incidents. After: deep learning virtual security analyst using deep neural networks can help overcome the growing skills gap and more rapidly detect and respond security incidents. An AI-based virtual security analyst can expedite the process of detecting and accurately classifying potential attacks, perform the necessary investigative steps to identify the source of the threat, and half of these are likely false positives.

The average SOC receives 10,000 alerts per day, but only has the manpower and resources to properly handle a fraction of them. Such a collaboration improves the scalability of teams, automates menial tasks, and keeps pace with protecting against evolving cyber-threat landscapes.