

# Use an AI-based Virtual Security Analyst to Modernize Your SOC

**Artificial intelligence (AI)** has the ability to identify patterns in massive amounts of data, enabling it to detect trends and make threat classifications much more rapidly than humans. An AI-based virtual security operations center (SOC) analyst using deep learning such as deep neural networks can help overcome the growing skills gap and more rapidly detect and respond security incidents.

**74%**

of security professionals say that the cybersecurity skills gap has impacted their organization.<sup>1</sup>

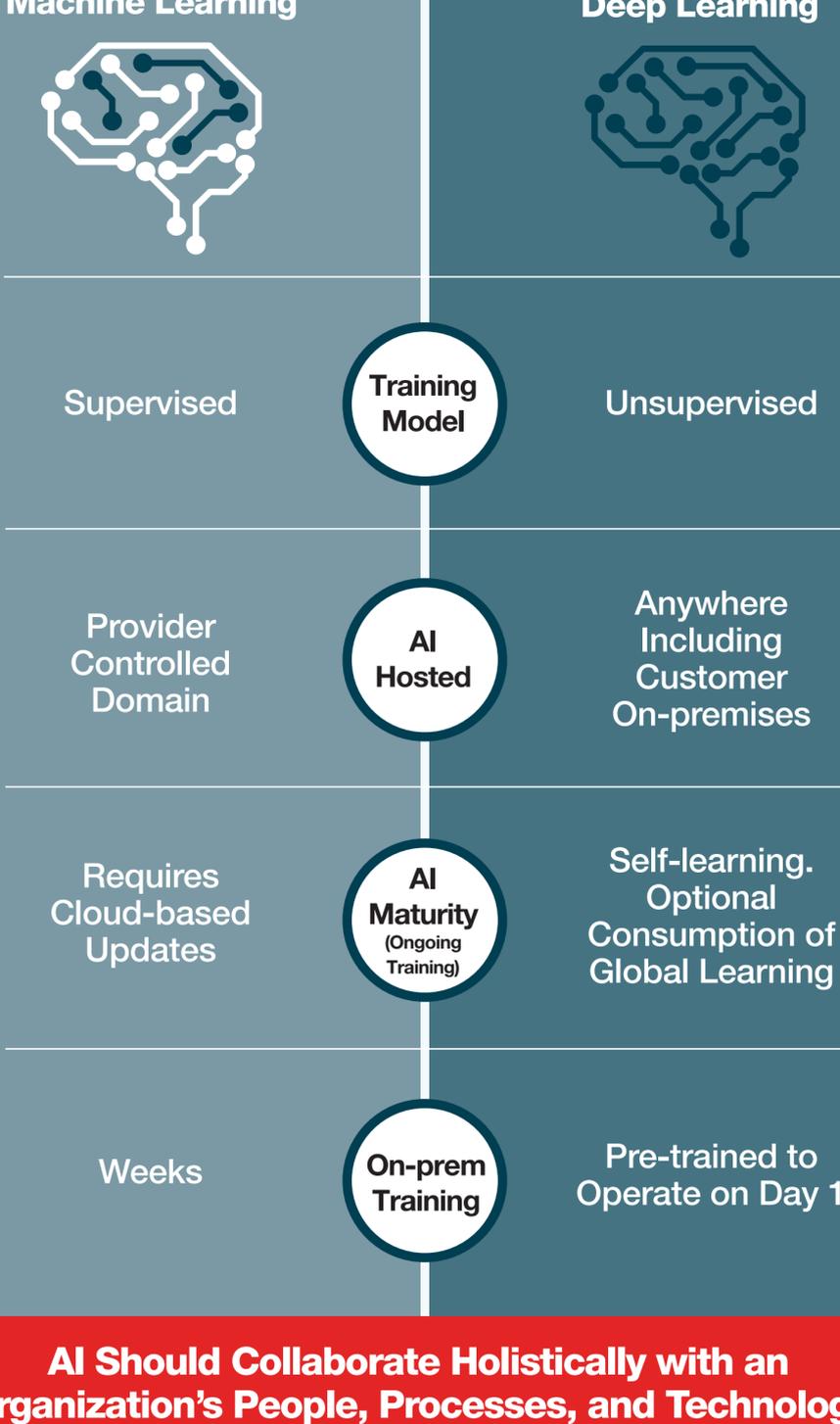
A deep neural network-based virtual SOC analyst helps mitigate the effects of this skills gap by helping to perform low-tier tasks and assisting human analysts, enabling them to operate at a higher level.



An AI system must have certain characteristics to be successful.

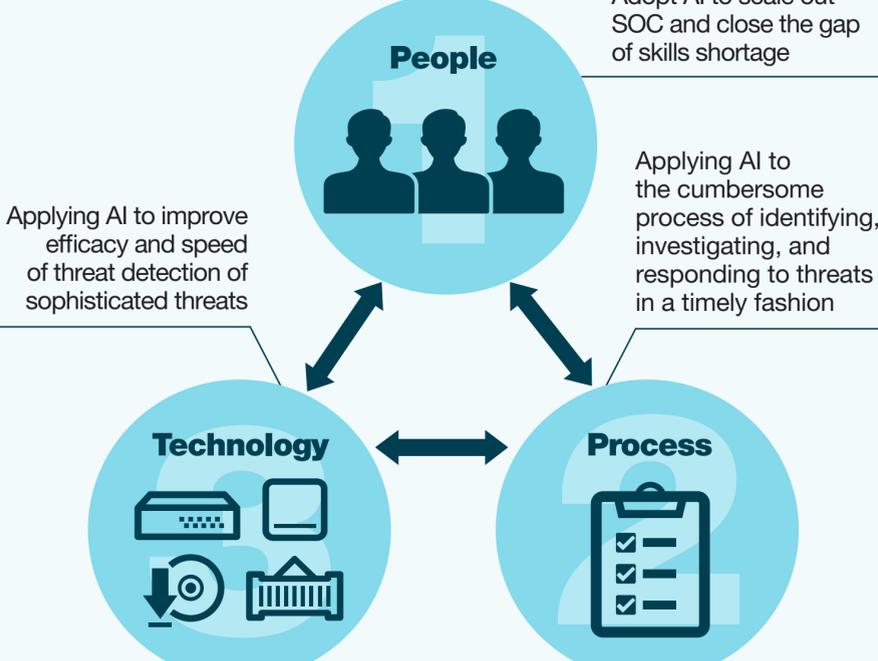
## An AI-driven Virtual Security Analyst Must Learn by Itself

When it comes to commonly used **machine-learning algorithms**, a virtual security analyst based on deep learning that can operate in unsupervised mode without initial training on-premises is a boon to lean SOC teams, which rely on its ability to adapt to the evolving cyber-threat landscape.



## AI Should Collaborate Holistically with an Organization's People, Processes, and Technology

Such a collaboration improves the scalability of teams, automates menial tasks, and keeps pace with protecting against sophisticated threats.



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

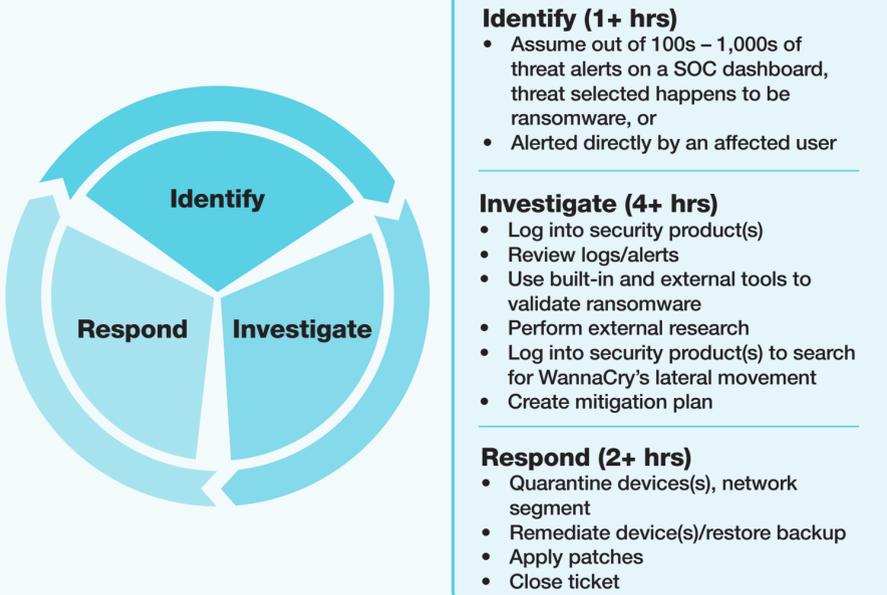
The average SOC receives **10,000 alerts per day** but only has the manpower and resources to properly handle a fraction of them.<sup>2</sup> Two-thirds of security analysts investigate less than 30 alerts per day,<sup>3</sup> and half of these are likely false positives.<sup>4</sup>

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, affected machines, and apply appropriate remediation.

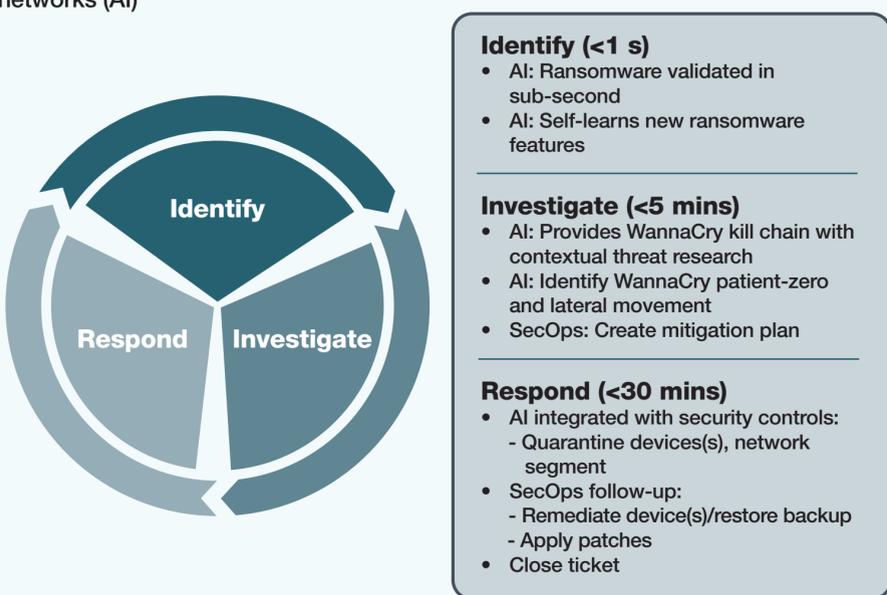
This dramatically decreases the load on security staff and reduces the cost of security incidents.

### Example of Threat Response Life Cycle

**Before:** The traditional approach to solving WannaCry with SecOps analysts only



**After:** Solving WannaCry with SecOps analyst augmented with deep neural networks (AI)



<sup>1</sup> Jon Oltsik, "The Life and Times of Cybersecurity Professionals 2018," ESG & ISSA, April 2019.  
<sup>2</sup> "How Many Daily Cybersecurity Alerts does the SOC Really Receive?," Bricata, October 2, 2019.  
<sup>3</sup> "SOCs still overwhelmed by alert overload, struggle with false-positives," Help Net Security, August 29, 2019.  
<sup>4</sup> Ibid.