FORTINET

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.[1]

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.

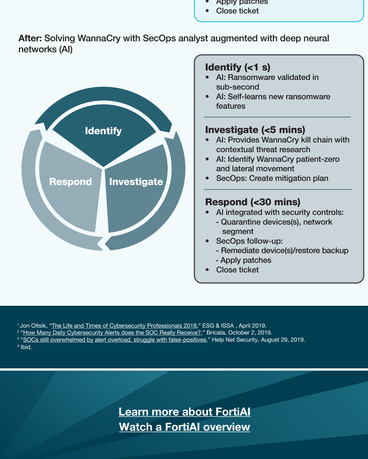
An AI-driven Virtual Security Analyst Must Learn by Itself

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.

Machine Learning		Deep Learning
Supervised	Training Model	Unsupervised
Provider Controlled Domain	AI Hosted	Anywhere Including Customer On-premises
Requires Cloud-based Updates	AI Maturity (Ongoing Training)	Self-learning. Optional Consumption of Global Learning
Weeks	On-prem Training	Pre-trained to Operate on Day 1

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

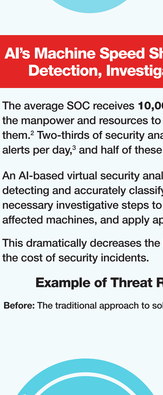
The average SOC receives **10,000 alerts per day** but only has the manpower and resources to properly handle a fraction of them.[2] Two-thirds of security analysts investigate less than 30 alerts per day,[3] and half of these are likely false positives.[4]

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



Identify (1+ hrs)
- Assume out of 100s – 1,000s of threat alerts on a SOC dashboard, threat selected happens to be ransomware, or
- Alerted directly by an affected user

Investigate (4+ hrs)
- Log into security product(s)
- Review logs/alerts
- Use built-in and external tools to validate ransomware
- Perform external research
- Log into security product(s) to search for WannaCry's lateral movement
- Create mitigation plan

Respond (2+ hrs)
- Quarantine devices(s), network segment
- Remediate device(s)/restore backup
- Apply patches
- Close ticket

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

Identify (<1 s)
- AI: Ransomware validated in sub-second
- AI: Self-learns new ransomware features

Investigate (<5 mins)
- AI: Provides WannaCry kill chain with contextual threat research
- AI: Identify WannaCry patient-zero and lateral movement
- SecOps: Create mitigation plan

Respond (<30 mins)
- AI integrated with security controls:
  - Quarantine devices(s), network segment
- SecOps follow-up:
  - Remediate device(s)/restore backup
  - Apply patches
- Close ticket

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

Learn more about FortiAI
Watch a FortiAI overview