Unsupervised Pre-trained to Process Organization’s People, Processes, and Technology

Applying AI to improve Modernize Your SOC

A deep neural network-based virtual SOC analyst can help overcome the growing skills gap and more rapidly detect and respond security incidents. Such a collaboration improves the scalability of teams, automates menial tasks, and keeps pace with protecting against evolving cyber-threat landscape.

Before:

The traditional approach to solving WannaCry with SecOps analysts only requires

Example of Threat Response Life Cycle

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

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

Machine Learning

Deep Learning

Machine Learning

Deep Learning

Provided by Fortinet

AI: Provides WannaCry kill chain with contextual threat research

AI: Self-learns new ransomware in sub-second

AI: Ransomware validated in less than 30 mins

Provider

Controlled Context

Model

Model

Process

Training

Pre-trained to Operate on Day 1

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

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

AI: 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. Two-thirds of security professionals say that the cybersecurity skills gap has impacted their organization.

Example of Threat Response Life Cycle

Below is the typical approach to solving WannaCry with SecOps analysts only

AI: Identifies WannaCry patient-zero

AI: Provides WannaCry kill chain with contextual threat research

AI: Self-learns new ransomware in sub-second

AI: Ransomware validated in less than 30 mins

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

The average SOC receives 10,000 alerts per day, but only has the manpower and resources to properly handle a fraction of them. Two-thirds of security professionals say that the cybersecurity skills gap has impacted their organization.

Example of Threat Response Life Cycle

Below is the typical approach to solving WannaCry with SecOps analysts only

AI: Identifies WannaCry patient-zero

AI: Provides WannaCry kill chain with contextual threat research

AI: Self-learns new ransomware in sub-second

AI: Ransomware validated in less than 30 mins

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

The average SOC receives 10,000 alerts per day, but only has the manpower and resources to properly handle a fraction of them. Two-thirds of security professionals say that the cybersecurity skills gap has impacted their organization.

Example of Threat Response Life Cycle

Below is the typical approach to solving WannaCry with SecOps analysts only

AI: Identifies WannaCry patient-zero

AI: Provides WannaCry kill chain with contextual threat research

AI: Self-learns new ransomware in sub-second

AI: Ransomware validated in less than 30 mins

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

The average SOC receives 10,000 alerts per day, but only has the manpower and resources to properly handle a fraction of them. Two-thirds of security professionals say that the cybersecurity skills gap has impacted their organization.

Example of Threat Response Life Cycle

Below is the typical approach to solving WannaCry with SecOps analysts only

AI: Identifies WannaCry patient-zero

AI: Provides WannaCry kill chain with contextual threat research

AI: Self-learns new ransomware in sub-second

AI: Ransomware validated in less than 30 mins

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

The average SOC receives 10,000 alerts per day, but only has the manpower and resources to properly handle a fraction of them. Two-thirds of security professionals say that the cybersecurity skills gap has impacted their organization.

Example of Threat Response Life Cycle

Below is the typical approach to solving WannaCry with SecOps analysts only

AI: Identifies WannaCry patient-zero

AI: Provides WannaCry kill chain with contextual threat research

AI: Self-learns new ransomware in sub-second

AI: Ransomware validated in less than 30 mins

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

The average SOC receives 10,000 alerts per day, but only has the manpower and resources to properly handle a fraction of them. Two-thirds of security professionals say that the cybersecurity skills gap has impacted their organization.

Example of Threat Response Life Cycle

Below is the typical approach to solving WannaCry with SecOps analysts only

AI: Identifies WannaCry patient-zero

AI: Provides WannaCry kill chain with contextual threat research

AI: Self-learns new ransomware in sub-second

AI: Ransomware validated in less than 30 mins

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

The average SOC receives 10,000 alerts per day, but only has the manpower and resources to properly handle a fraction of them. Two-thirds of security professionals say that the cybersecurity skills gap has impacted their organization.

Example of Threat Response Life Cycle

Below is the typical approach to solving WannaCry with SecOps analysts only

AI: Identifies WannaCry patient-zero

AI: Provides WannaCry kill chain with contextual threat research

AI: Self-learns new ransomware in sub-second

AI: Ransomware validated in less than 30 mins

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

The average SOC receives 10,000 alerts per day, but only has the manpower and resources to properly handle a fraction of them. Two-thirds of security professionals say that the cybersecurity skills gap has impacted their organization.

Example of Threat Response Life Cycle

Below is the typical approach to solving WannaCry with SecOps analysts only

AI: Identifies WannaCry patient-zero

AI: Provides WannaCry kill chain with contextual threat research

AI: Self-learns new ransomware in sub-second

AI: Ransomware validated in less than 30 mins

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

The average SOC receives 10,000 alerts per day, but only has the manpower and resources to properly handle a fraction of them. Two-thirds of security professionals say that the cybersecurity skills gap has impacted their organization.

Example of Threat Response Life Cycle

Below is the typical approach to solving WannaCry with SecOps analysts only

AI: Identifies WannaCry patient-zero

AI: Provides WannaCry kill chain with contextual threat research

AI: Self-learns new ransomware in sub-second

AI: Ransomware validated in less than 30 mins