AI FOR SECURITY OPERATIONS CENTER

Fort
Cybersecurity
Stronghold

CONTENTS

01 Introduction

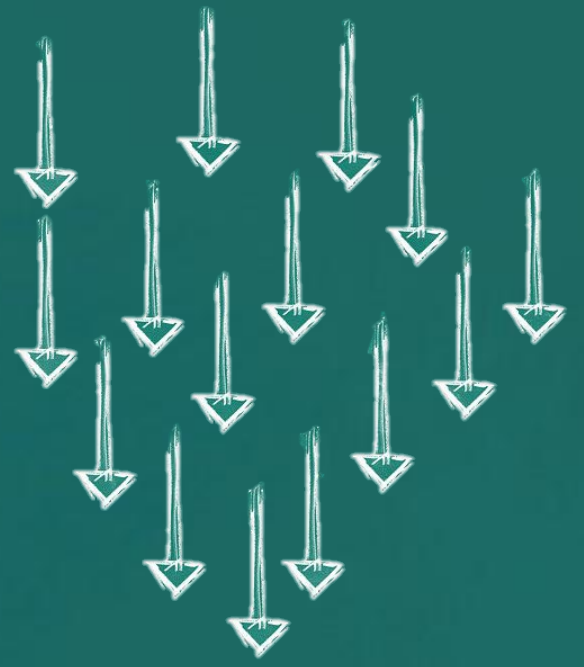
02 Artificial Intelligence

03 Machine Learning and Pattern Recognition

04 Natural Language Processing

05 Blueprint

06 Q&A



01

Introduction

Who am I?

Vladimir Ghiță (Vlad)

15+ years IT Experience

7+ years Managing CyberSecurity

Cybersecurity CEO @ Fort

Cloud and AI enthusiast

- **Who is FORT?**

Fort is one of the most dynamic company in the field of cybersecurity, proudly part of the renowned Bittnet Group. At Fort, we are dedicated to providing cutting-edge cybersecurity solutions and services to safeguard your digital assets and empower your organization against evolving cyber threats.

The world has changed

Cybersecurity requirements have increased,
especially a demand for improved detection of,
and response, to security incidents

What is the fundamental aim of a SOC?

Being analysts:

- Evaluating alerts as they come in;
- Identifying where the threats are;
- Hopefully clean them up;
- Tell the CISOs what the story is.

AI can give us automation.

Time back in the day to work.

So, what can an implementation of AI in a SOC look like?

Artificial Intelligence – A quick history

1950 – Turing Test
Method for determining the intelligence of a machine

1955 – AI
The term Artificial Intelligence is first used

1966 – Eliza
One of the first chatbots, simulates conversations as a psychotherapist.

1997 – Deep Blue
Chess AI wins against world champion Garry Kasparov

2017 – AlphaGo
Google's AlphaGo wins against world champion Lee Sedol.

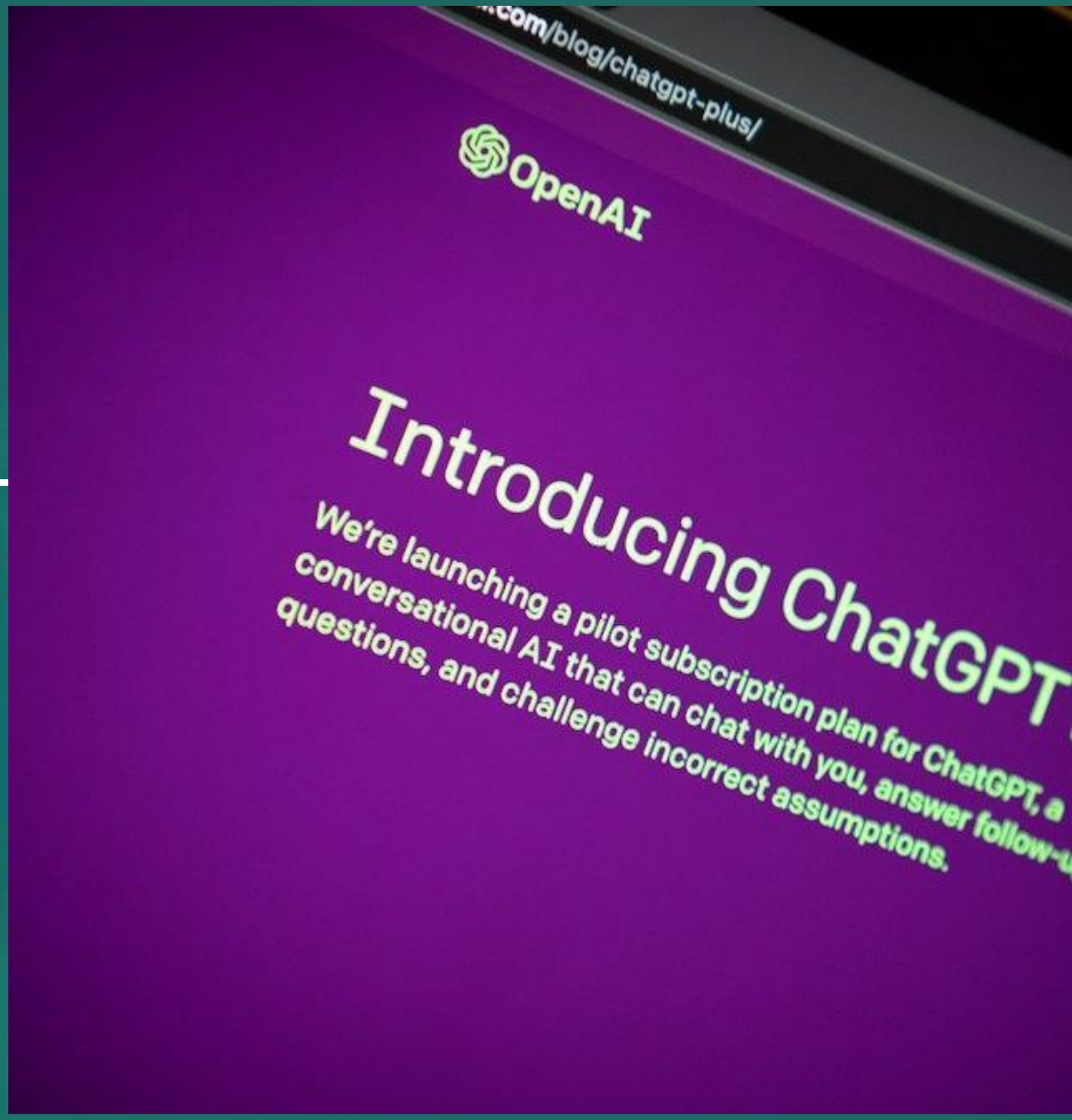
2022 – ChatGPT
Free to use OpenAI

ChatGPT

Changed the game

Much like the iPhone it wasn't fundamentally different than its predecessors, but it came at the right time in a complete package of **free**, **accessible**, **user friendly**.

Just like after the launch of the iPhone we are now in a race to see how far we can take this mode.



AI in cybersecurity at large

- Creation of realistic phishing emails to train employees;
- Creation of synthetic data such as malware for use in security testing;
- Reverse engineering malware;
- Battling bots – identifying good bots (i.e. Google*), bad bots and humans;
- Even end-to-end penetration testing.

Cybercriminals ab**use AI as well**

Social engineering schemes

Password hacking

Deepfakes

Data poisoning

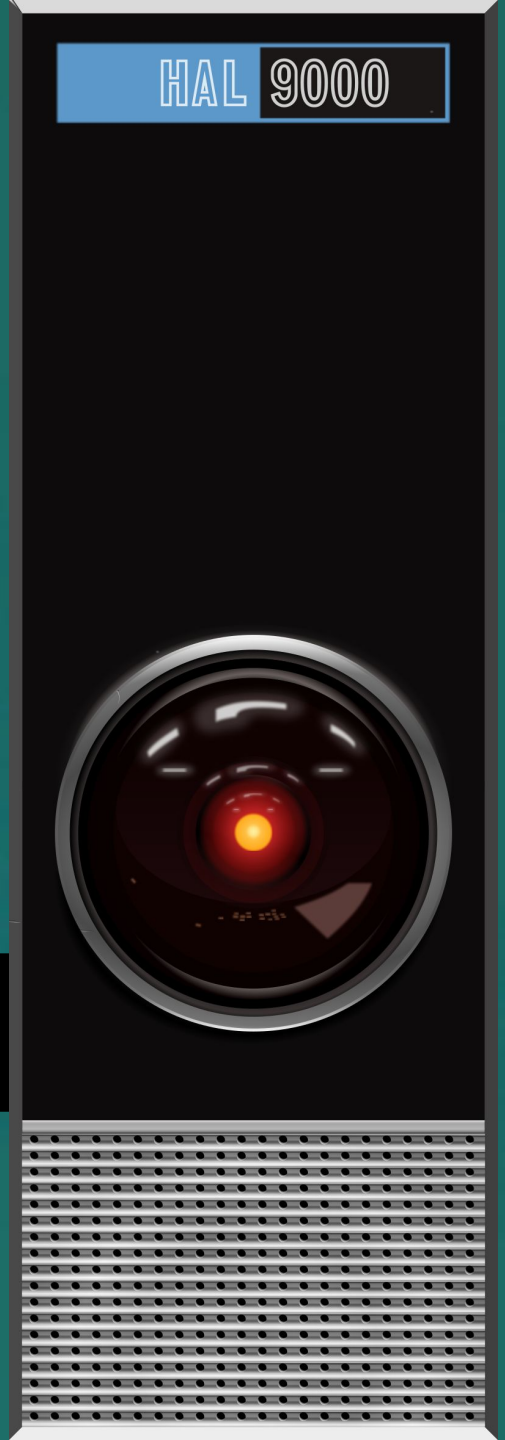
02

Artificial Intelligence

Main AI branches used for SOC

Machine Learning and Pattern Recognition

Natural Language Processing



2D depiction of the interface prop used by Stanley Kubrick in his 1968 movie "2001: A space Odyssey" to represent the Artificial Intelligence named **Hal**.

SOC Pains – What's AI good for?

- Alert fatigue – too many alerts to review and incidents to investigate;
- Analyst fatigue due to mundane and repetitive boring tasks;
- Incident investigations take too long;
- Lack of skilled analysts – takes too long to train new staff.

First task of a SOC analyst is to triage alerts.

AI can help.

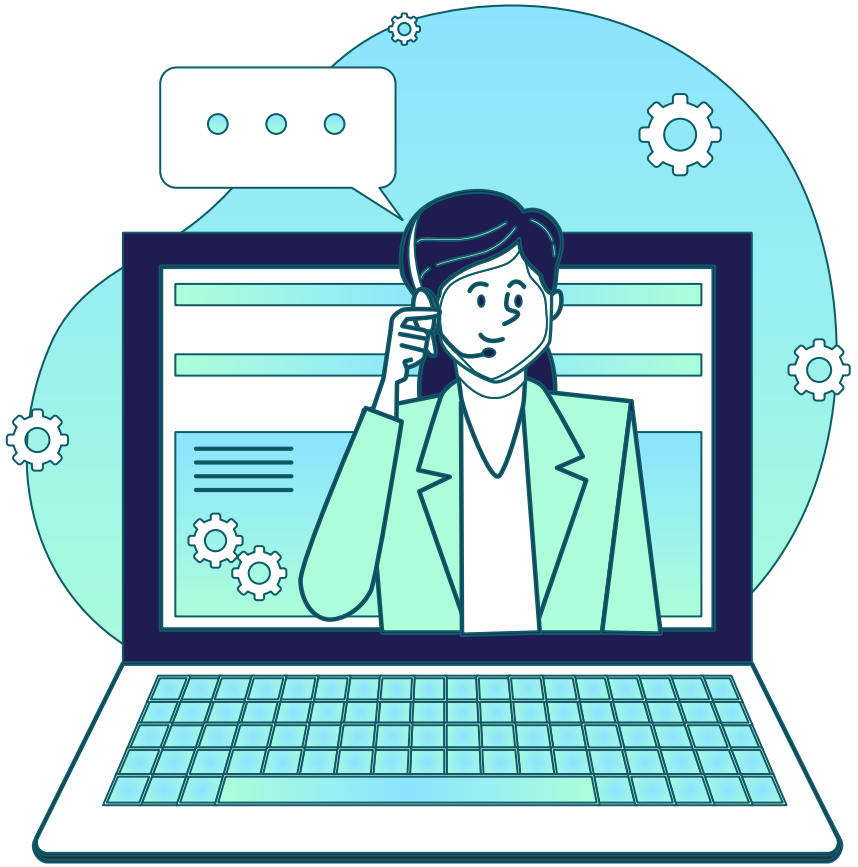
AI can help a lot.

But at the end of the day – it takes a mind to hunt a mind

Machine Learning and Pattern Recognition

Data aggregation, normalization, enrichment

- Collects information about normal user and entity behavior from system logs;
- It applies intelligent statistical analysis methods to interpret each dataset and establish baselines.



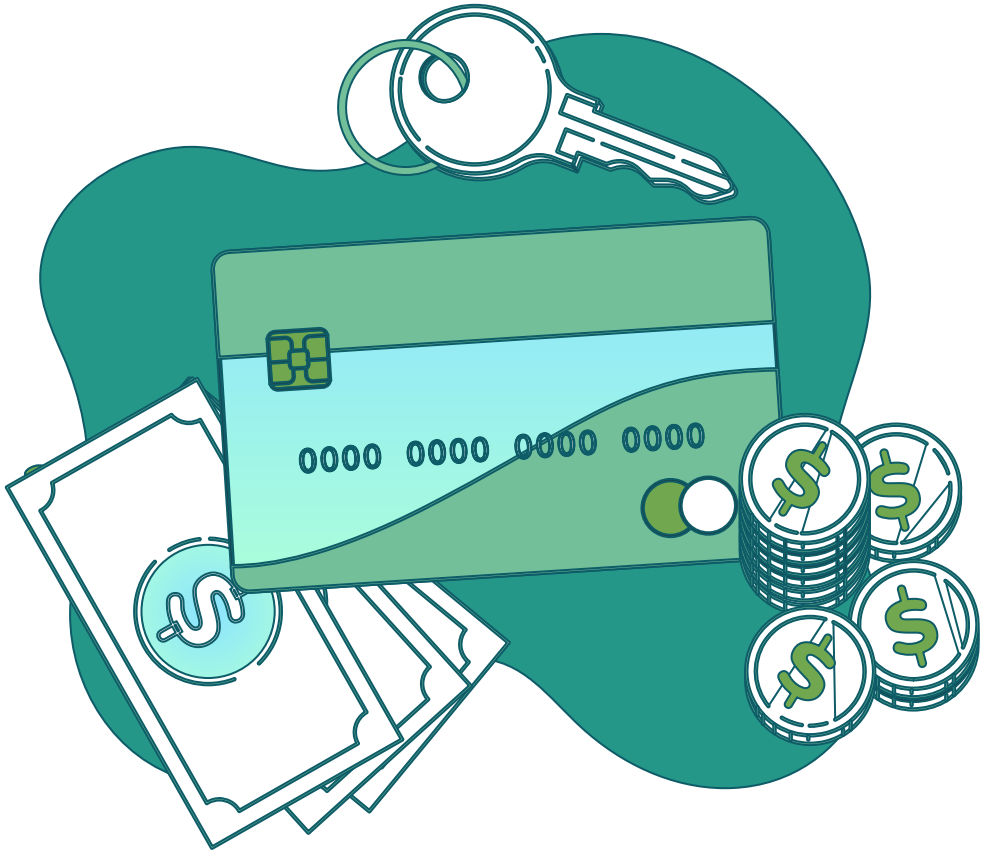
Machine Learning and Pattern Recognition

**Data aggregation,
normalization,
enrichment**

- Identifies behavior pattern baselines;
- Relies on and enriches SIEM events;
- Analysts train the model by evaluating alerts as True or False Positive.

Predictive Analytics

Using historical data to predict future events or trends



- Identifying potential threats before they occur;
- This enables organizations to take proactive measures to prevent security incidents;
- Helps prioritizing threats, enabling organizations to focus their resources on the most critical **threats**.

04

Natural Language Processing

Search

Translates technical queries into regular language

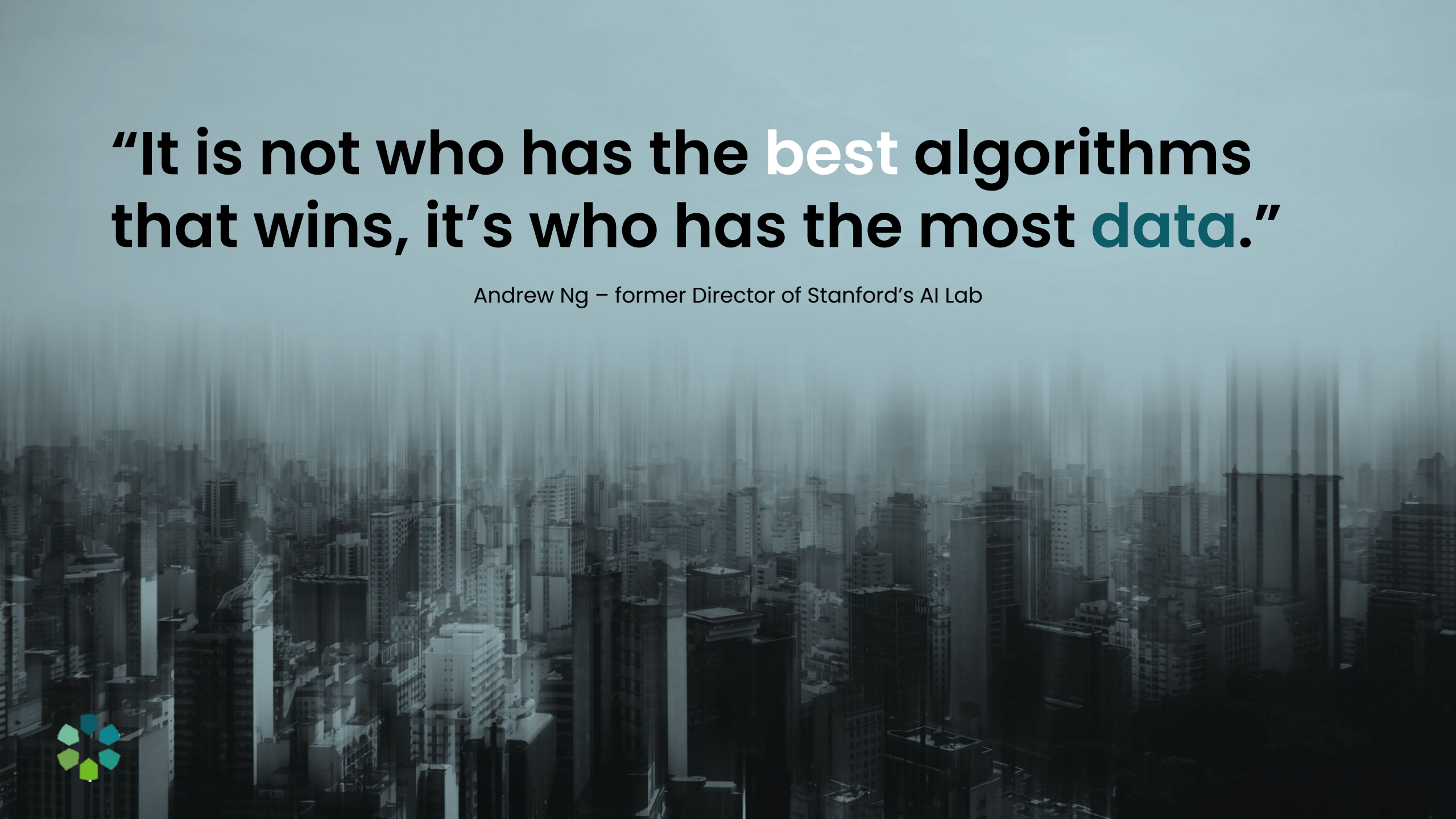
Go from

Msg_type “i-panel-vulnerability-alert-b2b2c” AND alert_severity:”Critical” FROM >30 days

To

“Show me critical event logs from my b2b2c network appliances over the last 30 days”

This can be used in all areas of SOC operations


“It is not who has the best algorithms that wins, it’s who has the most data.”
Andrew Ng – former Director of Stanford’s AI Lab

Data ingestion

- Useful in maintaining changes in the logs being parsed or deviations from standards lead to missing key information;

- Makes it a lot easier to onboard new systems in the monitoring cycle.

"Import critical event logs from my b2b2c network with a frequency of 1 second"

Threat hunting

Go from

```
activity_type = 'process-create' &&
toLower(process_name)='sc.exe' &&
contains(toLower(process_command_line), 'stop', 'windefend')
```

To

"Author a correlation rule which will detect the suspicious activity of disabling the Windows Defender service"

Detections are core to the ability of a SOC to discover and understand threats to their environment

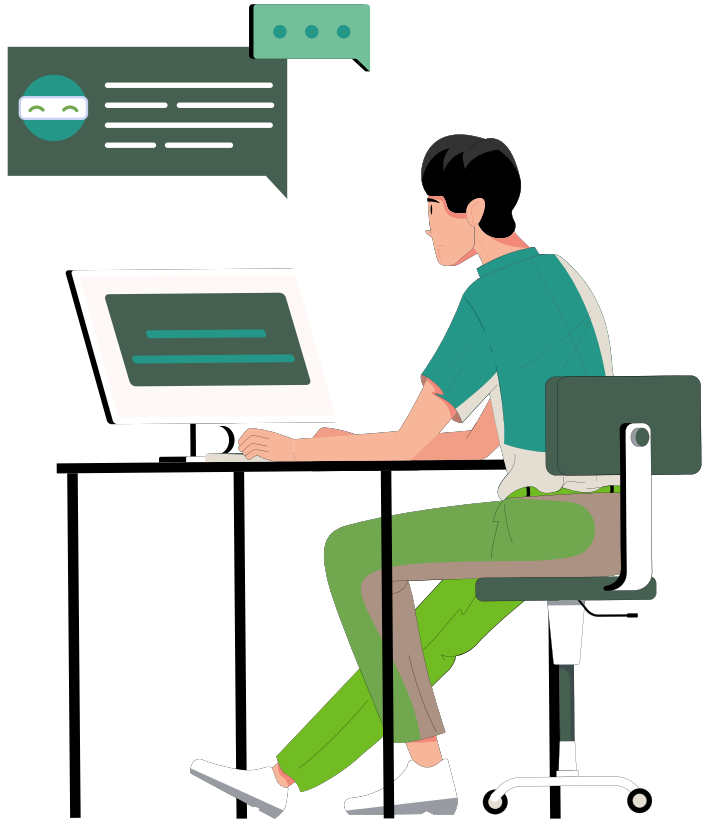
Threat hunting

Expand beyond specific indicator detection by identifying threat actor based on historical patterns

"Examine the last 90 days of logs, listing all events with suspicious activity of disabling the Windows Defender service and display it in a graph"

Documentation

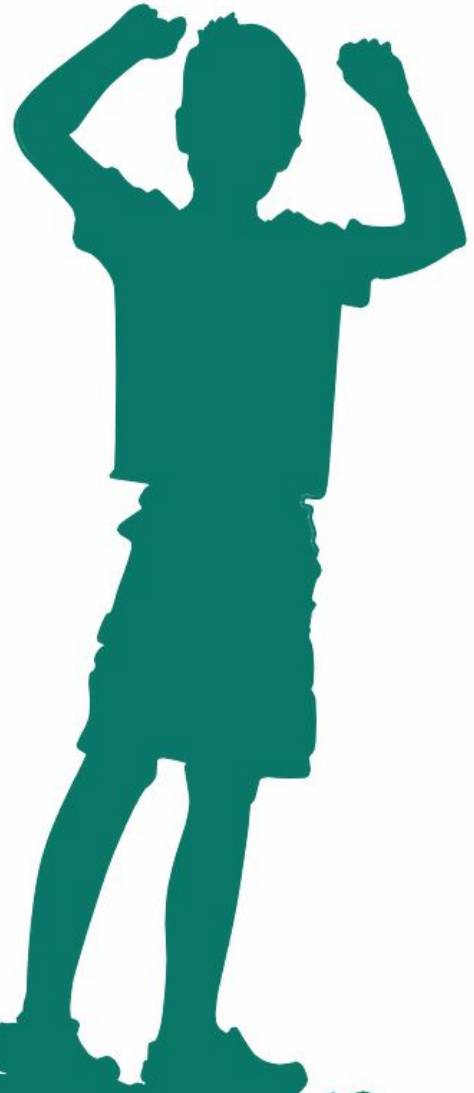
Assume accurate detection and identification of security anomalies, malicious or suspicious behavior, and their tactics, techniques, and procedures (TPPs)



You have 4 initial disparate events that are part of the same “story”:

1. Logging into a laptop from a network belonging to an unapproved VPN;
2. Escalating privileges;
3. Moving laterally;
4. Exfiltrate sensitive data.

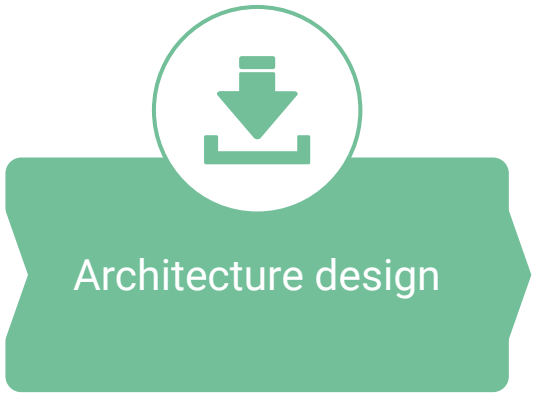
Create the story, have it validated by a SOC analyst, and then add it to a report for a much-increased speed of a post-mortem.



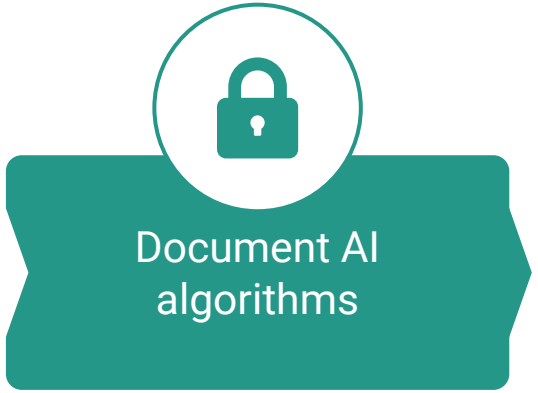
05

Blueprint

Key steps



1. Identify the type of data that needs to be monitored;
2. The type of threats that need to be detected;
3. The level of automation required for incident response



1. How are they trained on data;
2. How are they used to detect and respond to threats;
3. Data sources;
4. Performance metrics.

1. Monitor for performance issues;
2. Updating the AI algorithms;
3. Train analysts.

SOC AS A SERVICE

Powered by FORT

We employ the latest and most advanced technologies, tactics, and strategies to provide unmatched minimal response time and effectiveness

- **Built around a core set of activities** our SOC services are designed to address your requirements in regard to cyber monitoring and defense
- **Incident triage, analysis, and response,** including 24x7 real-time alert monitoring and near-instantaneous notification
- **Leveraging Artificial Intelligence** to enrich events and allow first responders to take informed decisions
- **Dark web monitoring** that provides increased early detection of leaks

Contact

Vladimir Ghiță
CEO
vlad@fort.ro
+40 723 141 186

About FORT

At Fort, we are your firm partner in safeguarding your business, ensuring your operations run smoothly and without interruption, protecting your reputation from the constant tide of cyber threats.This year, FORT has become one of the main competitors in Romanian cybersecurity space, with a team of over 40 experts with a solid background in the local and international markets.

Visit us at fort.ro

06

Q&A