



Enhance Resilience with Future AI Cybersecurity

Zach Lewis





Our mission is to connect people to the technology and tradecraft necessary to make our country, and our world, a better, safer place.

- Mission Focused Full Stack Digital Services Company
- Tactical and Strategic deployment
- Cloud development in Government spaces
- Multiple Department of Defense Primes

<https://www.clarityinnovates.com/>

Clarity's Competencies

- Full stack digital services
- Application development
- DevSecOps engineering
- Human Centered Design
- Design Thinking
- Agile thinking and methodologies
- XP processes to including
- Test Driven Development
- CI/CD pipelines
- Pair programming
- Code refactoring
- Cloud native development
- Cloud native security
- Green/brown fielding
- X as-a-Service
- Platform engineering
- Systems architecture



Presenter



Zach Lewis

Clarity Dev Lead - CISSP/CSSLP

- Tech Enthusiast, Full Stack Developer/30+ year IT Professional
- Solution Oriented Consultant .
- SRE, App Sec Consultant, Strategic Initiatives, Knowledge Management

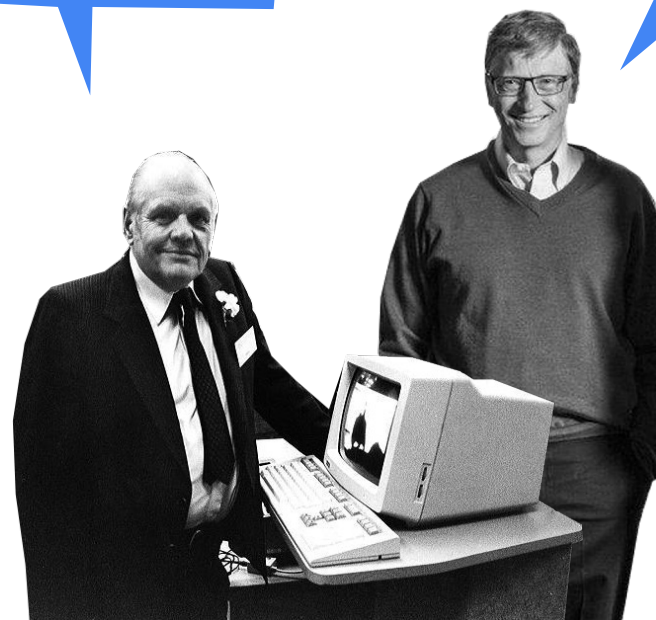
<https://www.linkedin.com/in/zachary-lewis-2aa8032>

How Things Change

There's no reason for any individual to have a computer in their home
- Ken Olsen

A computer on every desk and in every home, running Microsoft software.
- Bill Gates

PDP-11



SPACEX



OpenAI

TESLA



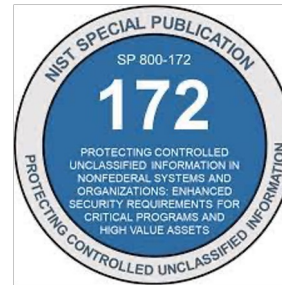
Meta

Apple Vision Pro

Resilience

The ability to **anticipate**, **withstand**, **recover** from, and **adapt** to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Sources: NIST SP 800-172.



When Complex is as simple as it Gets – Resilience vs. Anticipation

Author: Emery Roe

<https://mess-and-reliability.blog/2021/02/15/cant-we-be-best-anticipatory-and-resilient-at-the-same-time/>

Resilience is said to be optimizing the ability to absorb or rebound from shocks, while minimizing the need to anticipate these shocks ahead of time. **Anticipation, in contrast, is to optimize the ability to plan ahead and deal with shocks before they happen**, while minimizing having to cope with shocks when they do occur.



		Strategy With Respect To Resilience	
		<i>Optimizing ability to absorb and rebound</i>	<i>Minimizing need to absorb and rebound</i>
Strategy With Respect to Anticipation	<i>Optimizing ability to plan ahead</i>	“Maximum Readiness”	“Anticipation”
	<i>Minimizing need to plan ahead</i>	“Resilience”	Supposedly ideal, but still impossible

Table 1: Relationship between “resilience” and “anticipation” under complexity

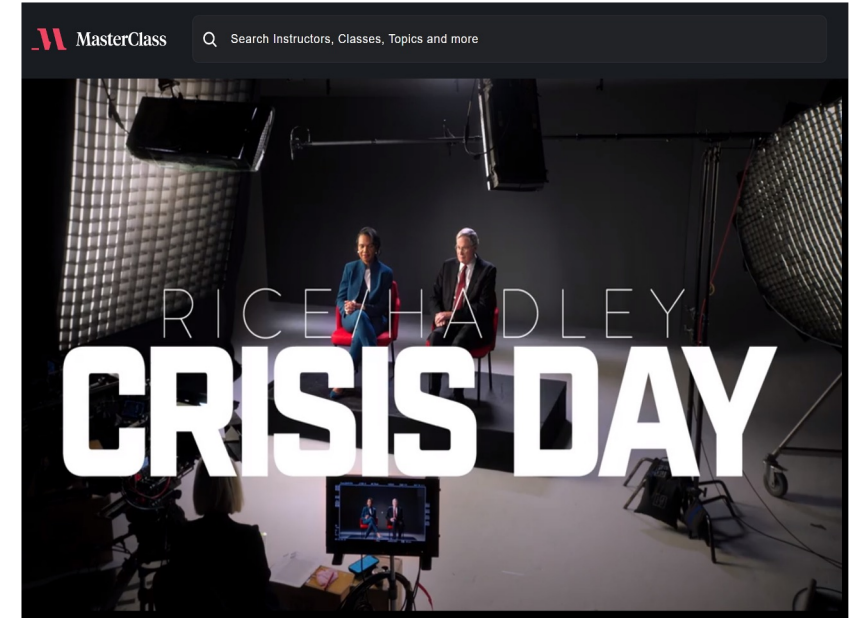
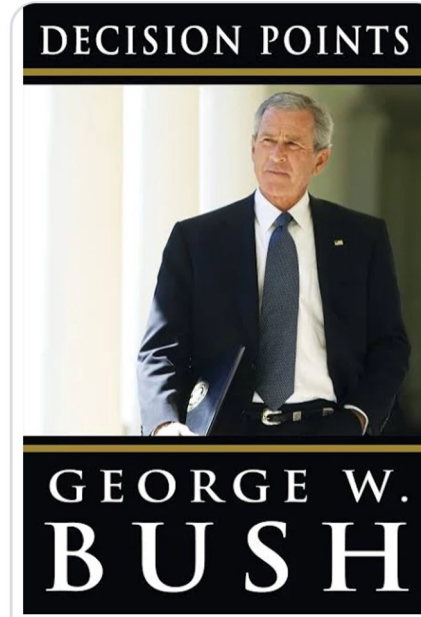
ICE BREAKER



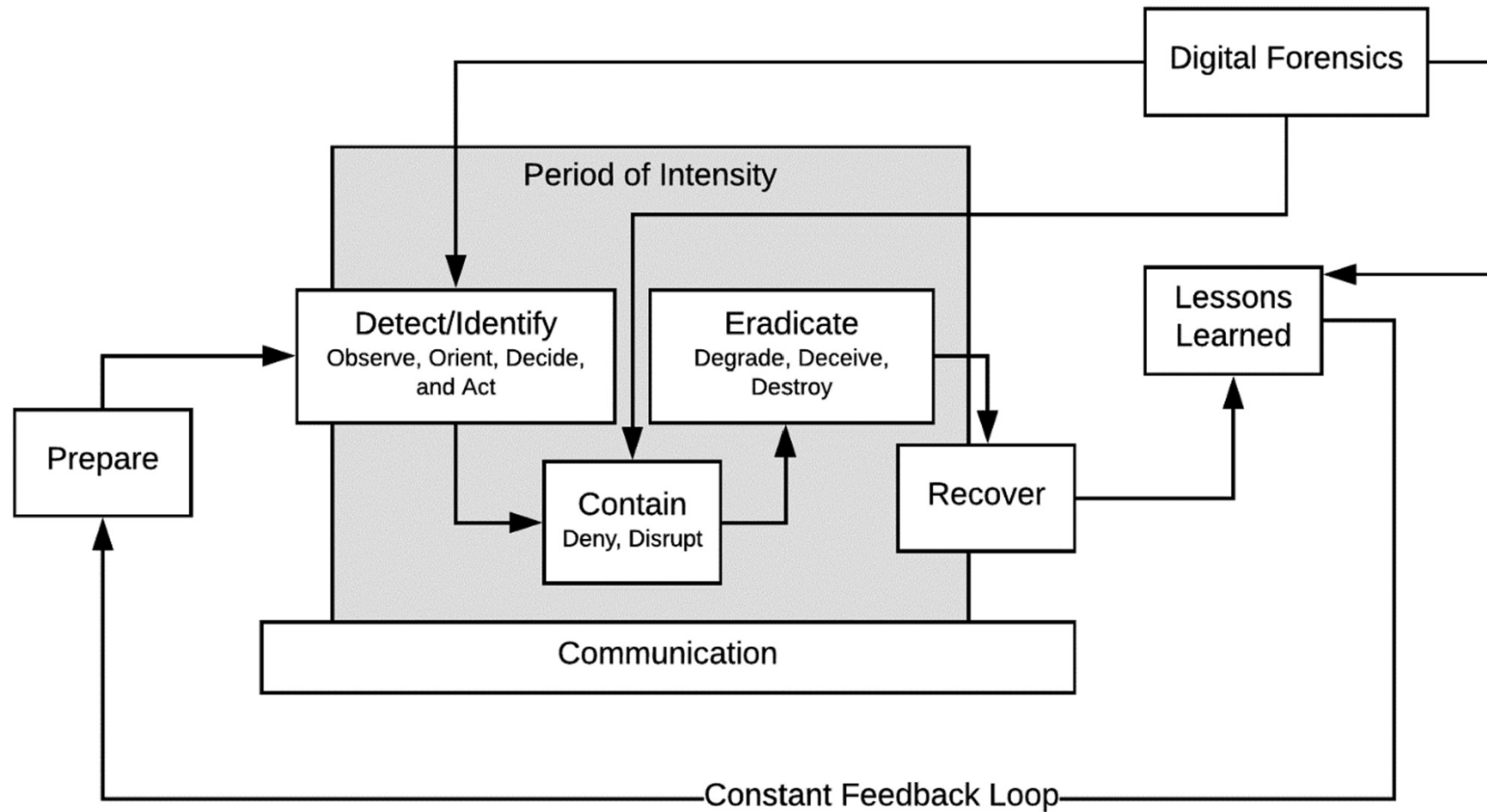
Questions on Resilience – 9/11 Event

Hindsight questions

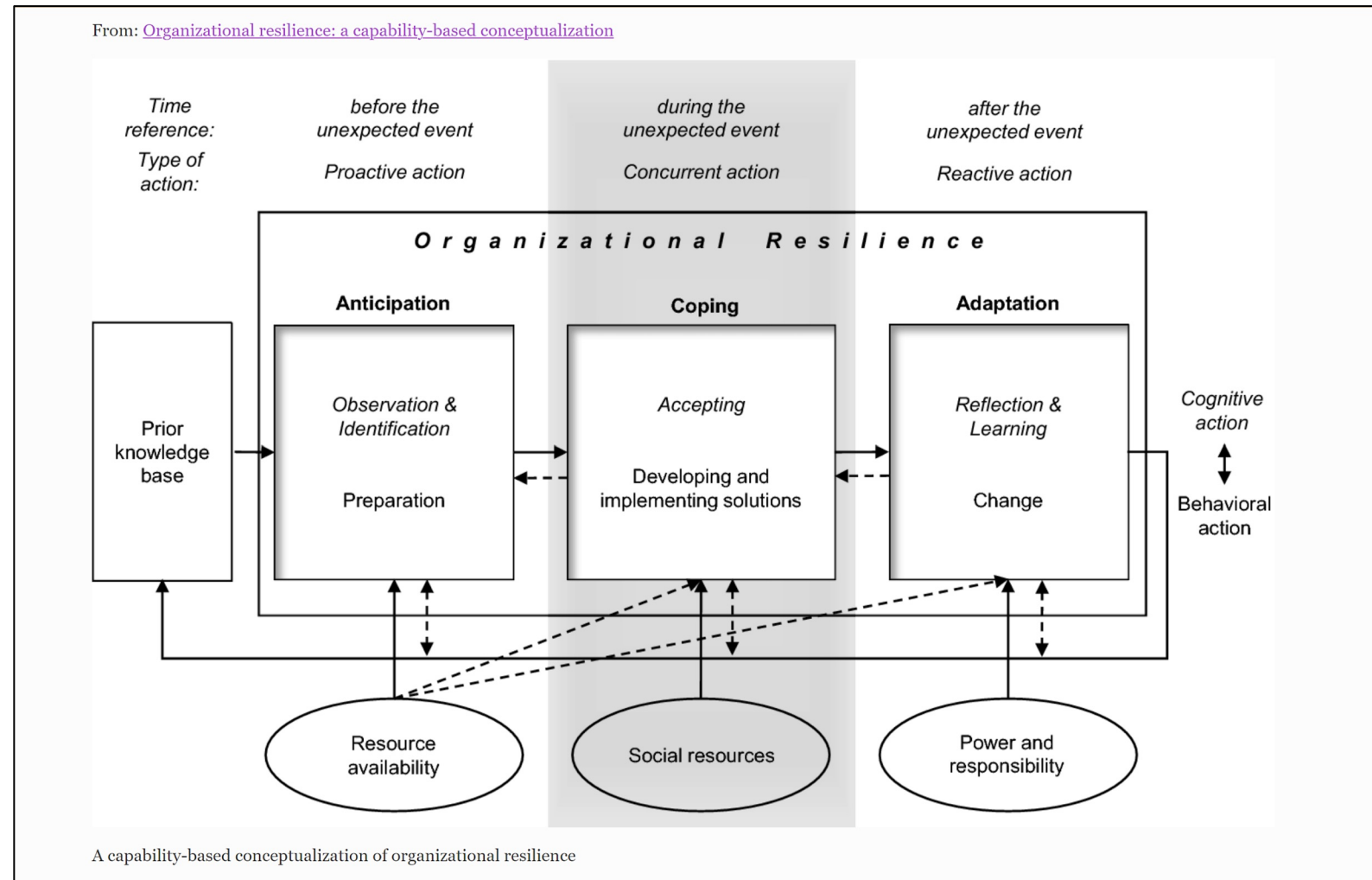
- **Anticipate** – What people, processes, data, workflows, and technology are needed to prepare for this event ?
- **Withstand** – Response Time mattered.
- **Recover** – What should recovery look like ?
- **Adapt** – How should we adapt ?



Modern Incident Response Life Cycle



A capability-based conceptualization of organizational resilience



<https://link.springer.com/article/10.1007/s40685-019-0085-7>

Systems will have failures

<https://downdetector.com/>



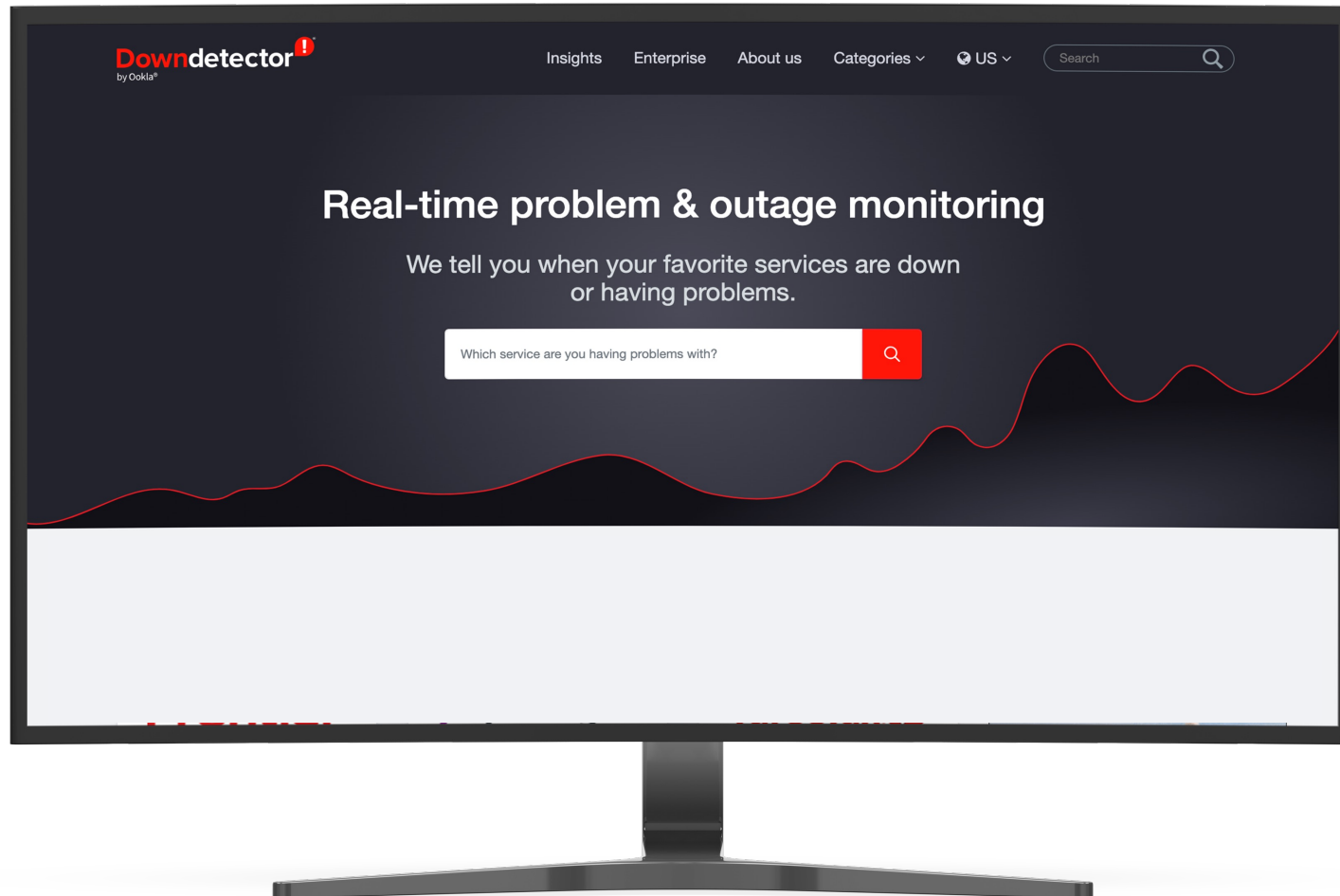
aws



IBM



Systems will have failures



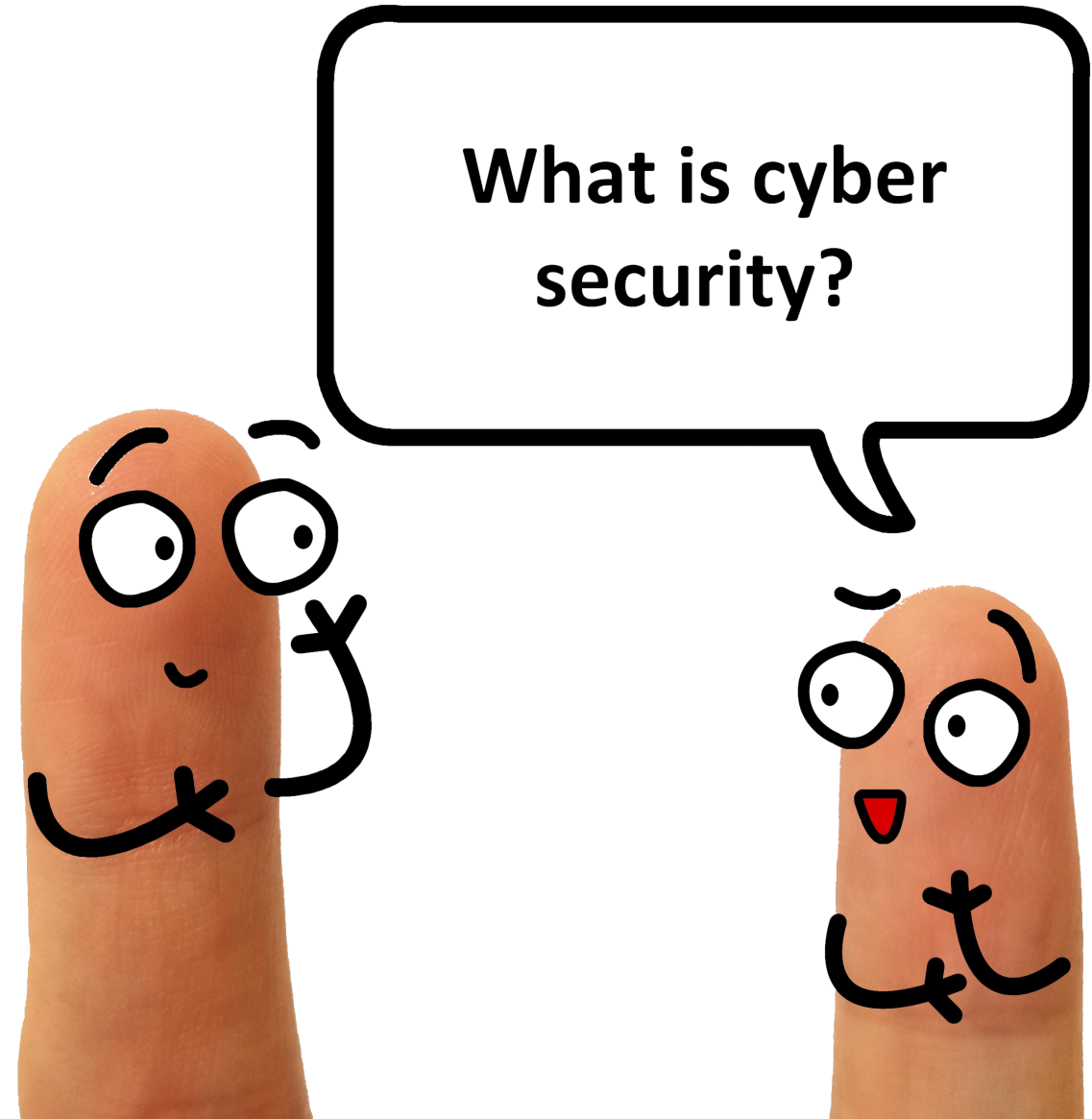
<https://downdetector.com/>

Resilience

Cyber resilience is the ability to anticipate, prevent, respond to, and recover from cyber threats, in a timely and effective manner.

Key Areas of Concerns

- Availability
- Capacity
- Efficiency
- Extensibility
- Manageability
- Maintainability
- Performance
- Portability
- Privacy
- Recoverability
- Reliability
- Scalability
- Security
- Serviceability



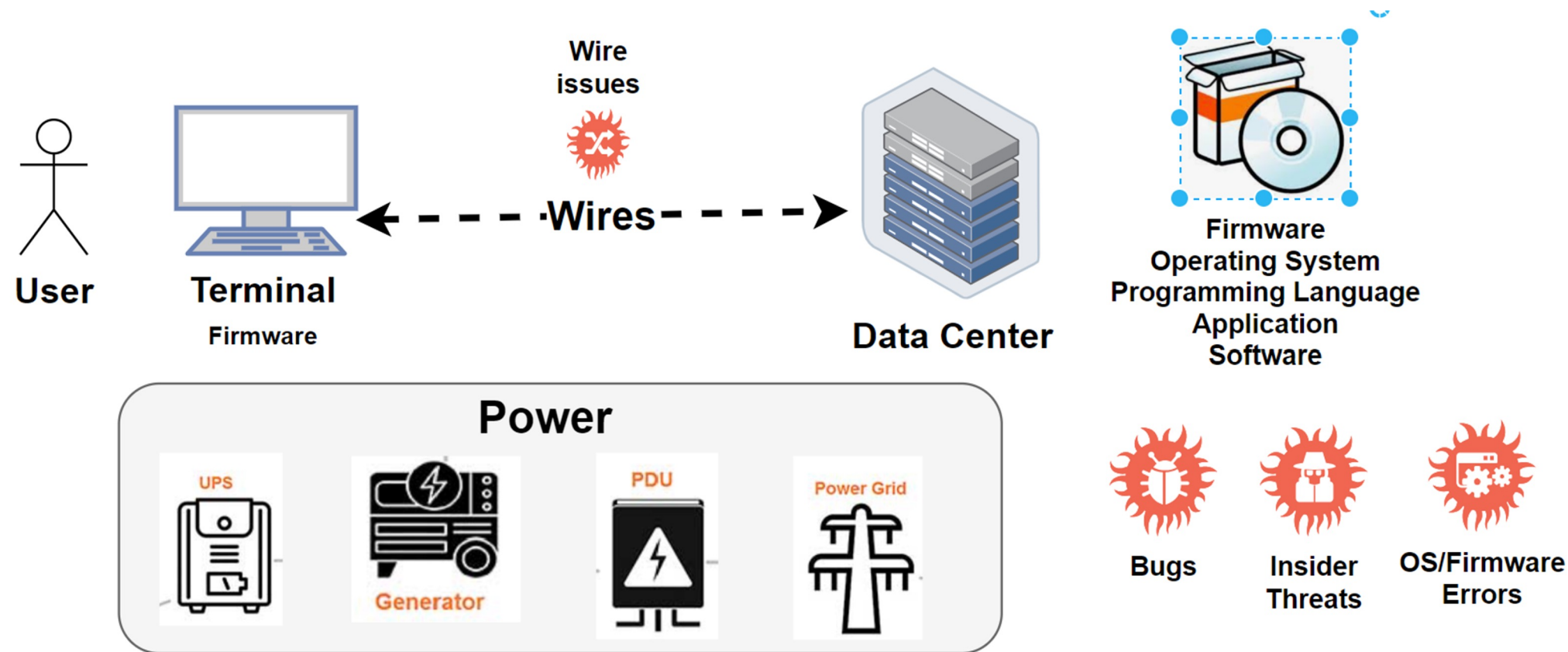
Key Point – AI and Information Overload

Artificial intelligence (AI) can be a powerful tool for managing content overload. AI algorithms can analyze vast amounts of data and quickly filter and prioritize content based on a user's preferences and interests.

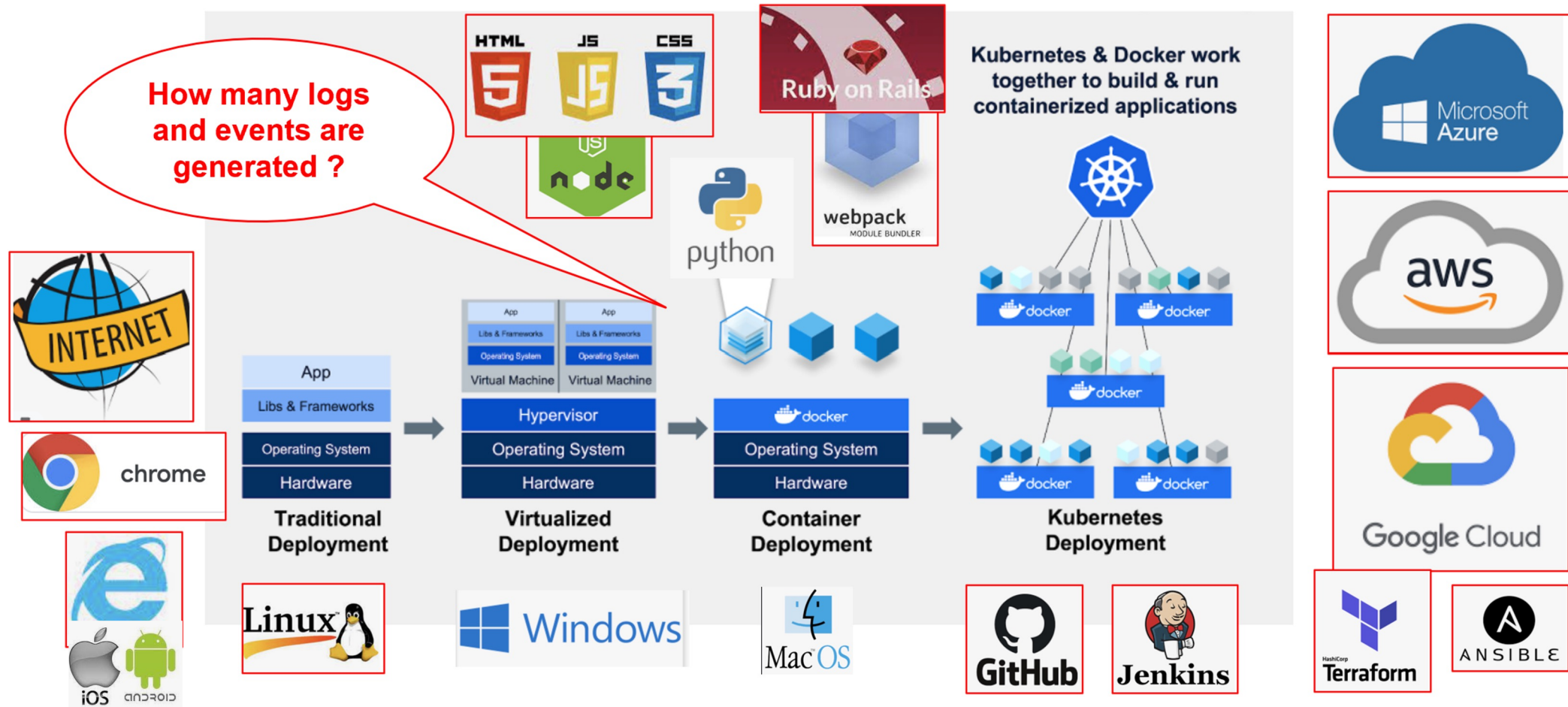
<https://www.linkedin.com/pulse/content-overload-artificial-intelligence-some-responses-from/>



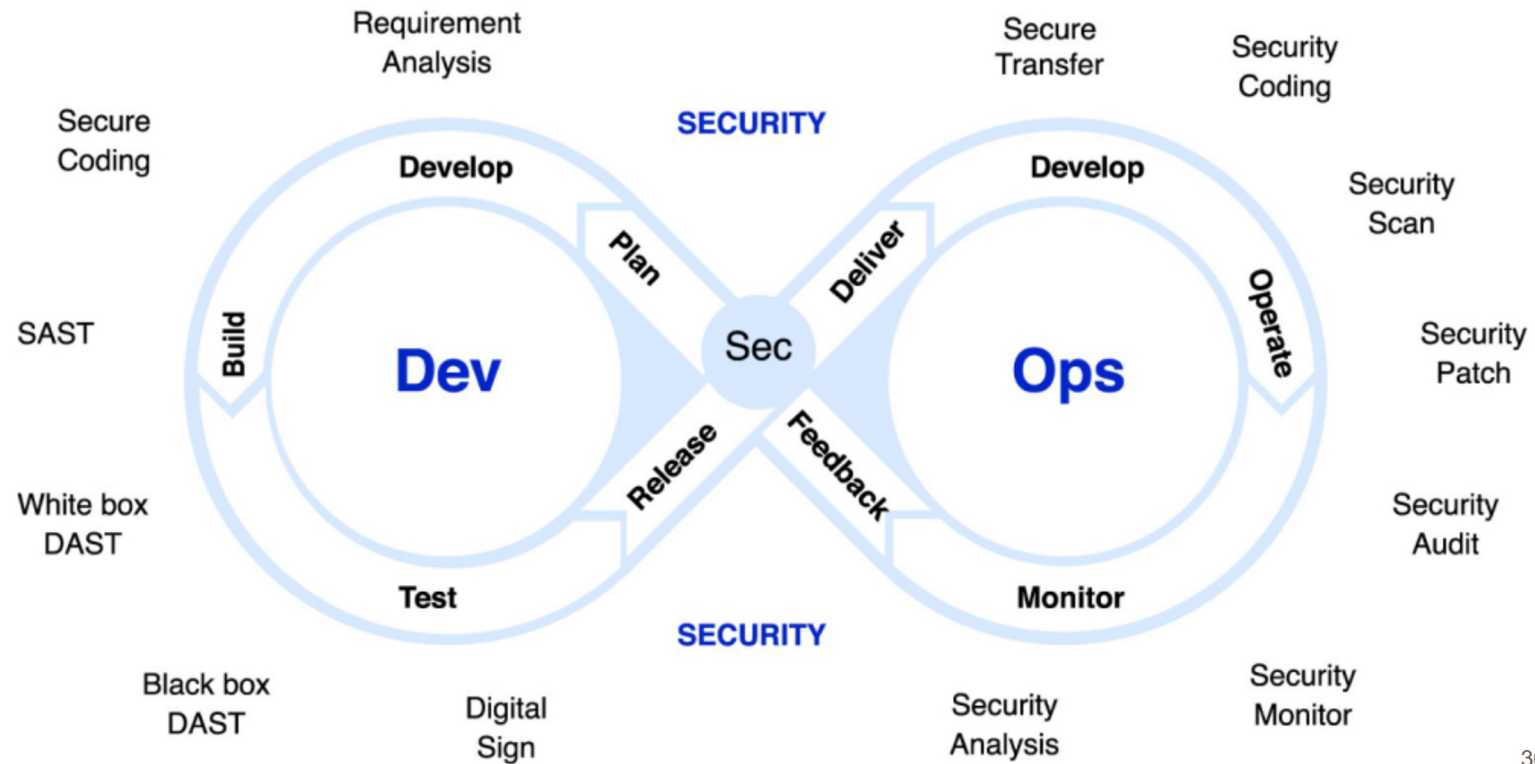
What did Resilience mean 30 years ago ?



What does Resilience mean today and in the Future ?



Today DevSecOps



30

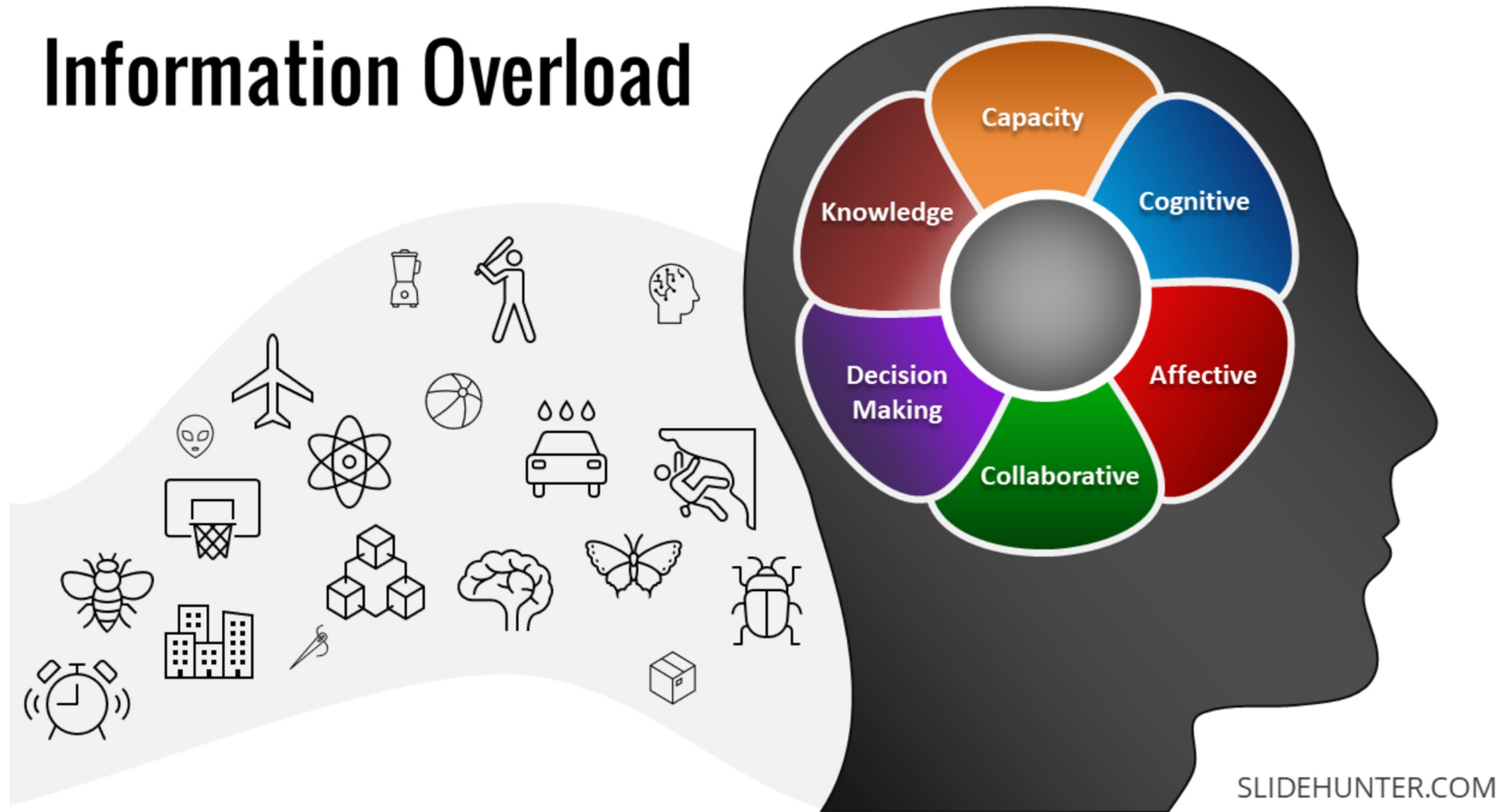
What happens when a few key DevSecOps engineers are away or leave ?

Our expert is out all this week and we do not know what to do ?



SYSTEM ERROR
CHECK

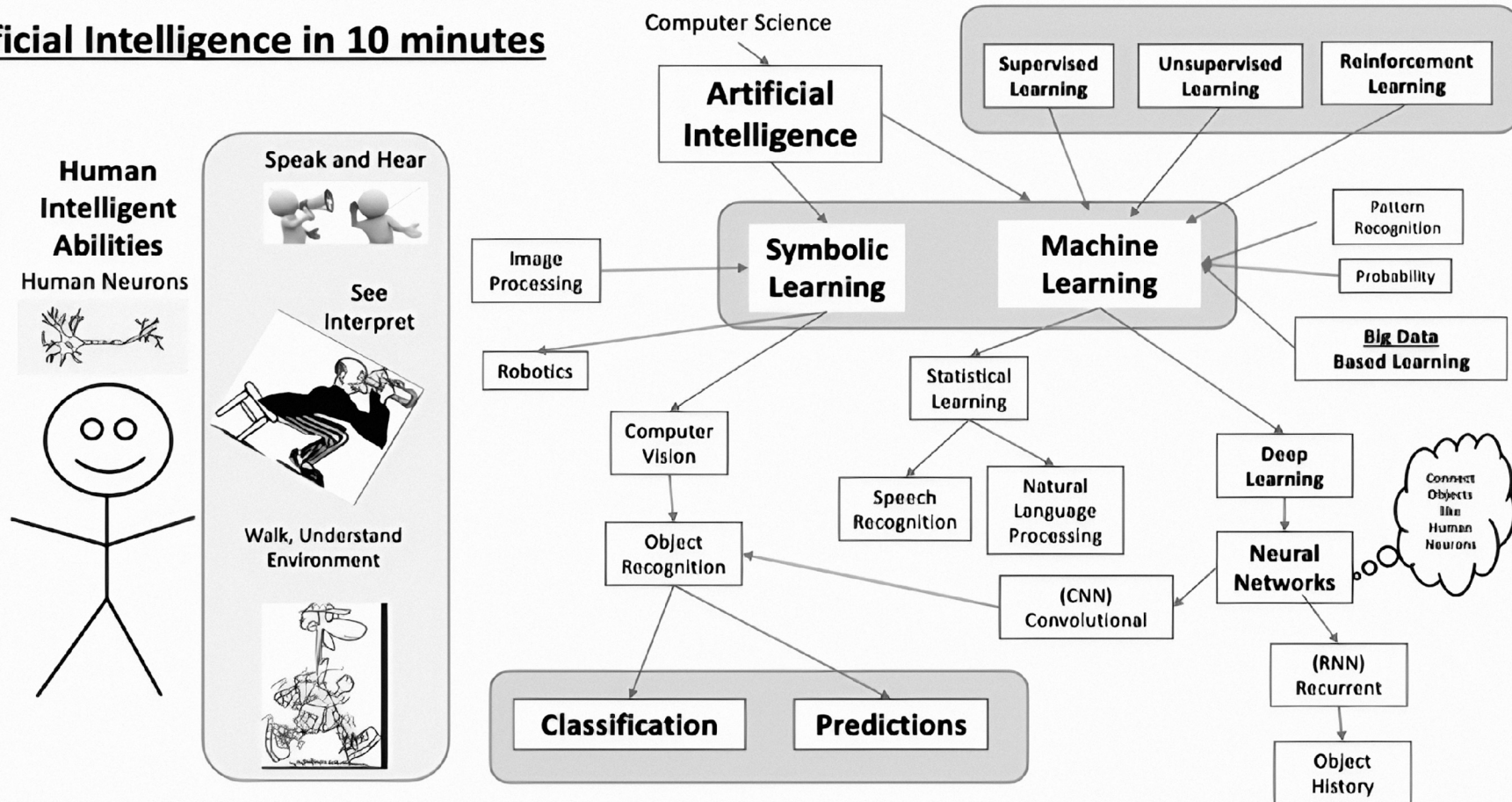
Information Overload



<https://techbuzzireland.com/2021/05/12/6-ways-to-preventing-information-overload-in-your-presentations/>

Quick - AI Overview

Artificial Intelligence in 10 minutes



Example of What is still needed .. AI boundaries

<https://ec.ai/>



[Home](#) [Company](#) [Blog](#) [Book a demo](#)

AI that thinks before it talks

Provably Correct. Fully transparent. Solve your toughest problems.



Google Cloud Next '23

Visit EC at the AI Pavilion during [Google Cloud Next '23](#), August 29-31

[Register here](#)



Runyon



Security Data Management – Things We Know

Attack Points/Threat Surface

MITRE

ATT&CK®

Matrices ▾

Tactics ▾

Techniques ▾

Data Sources

Mitigations ▾

Groups

Software

Campaigns

Resources ▾

Blog ↗

Contribute

Search 🔍

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK®

Getting Started

Take a Tour

Contribute

Blog ↗

FAQ

Random Page ▾

ATT&CK Matrix for Enterprise

layout: flat ▾

show sub-techniques

hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques	17 techniques	31 techniques	9 techniques	17 techniques	16 techniques	9 techniques
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Exploit Public-Facing	Command and	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected	Communication	Data Transfer Size Limits

 CLARITY

Disclaimer for inside pages: Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.+

Security Data Management – Things We Know

Common Vulnerabilities



[CVE List](#) [CNAs](#) [WGs](#) [Board](#) [About](#) [News & Blog](#)



Go to for:
[CVSS Scores](#)
[CPE Info](#)

[Search CVE List](#) [Downloads](#) [Data Feeds](#) [Update a CVE Record](#) [Request CVE IDs](#)

TOTAL CVE Records: **208339**

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.
NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024. New CVE List download format is [available now](#).

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

CVE News

News has moved to the new CVE website.

[Go to new News page >>](#)

CVE Podcast

Podcasts have moved to the new CVE website.

[Go to new Podcast page >>](#)

CVE Blog

Blogs are moving to the new CVE website.

[Go to new Blogs page >>](#)

Become a CNA

[CVE Numbering Authorities](#), or "CNAs," are essential to the CVE Program's success and every [CVE Record](#) is added to the [CVE List](#) by a CNA.

Join today!

- [Business benefits](#)
- [No fee or contract](#)
- [Few requirements](#)
- [Easy to join](#)



[Go to new CVE website](#)

[Learn How to Become a CNA >>>](#)
[Watch CNA Onboarding Videos >>](#)

Newest CVE Records

 **CVE**
@CVEnew · 4h

CVE-2023-37219 Tadiran Telecom Composit
- CWE-1236: Improper Neutralization of
Formula Elements in a CSV File
cve.org/CVERecord?id=C...

[Follow @CVEnew >>](#)

Security Data Management – Things We Know

Common Weaknesses

**Common Weakness Enumeration**
A Community-Developed List of Software & Hardware Weakness Types

**New to CWE?**
[Start here!](#)

ID Lookup:

[Home](#) | [About](#) | [CWE List](#) | [Mapping](#) | [Top-N Lists](#) | [Community](#) | [News](#) | [Search](#)

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.



2023 CWE Top 25 Most Dangerous Software Weaknesses

This list demonstrates the currently most common and impactful software weaknesses. Often easy to find and exploit, these can lead to exploitable vulnerabilities that allow adversaries to completely take over a system, steal data, or prevent applications from working.

[Top 25 List](#) | [Key Insights](#) | [Methodology](#)

CWE List Quick Access

Search CWE

ENHANCED BY Google

View CWE

[by Software Development](#)

[by Hardware Design](#)

[by Research Concepts](#)

[by Other Criteria](#)

Total Weaknesses: 933

Community Engagement

Hardware CWE Special Interest Group
[Join HW CWE SIG](#)

ICS/OT Special Interest Group
[Join ICS/OT SIG](#)

REST API Working Group
[Join REST API WG](#)

User Experience Working Group
[Join UE WG](#)

CWE/CAPEC Board
[Read meeting minutes](#)

Please see our [Guidelines for New Content Suggestions](#)
For other ways to get involved, [contact us](#)

CWE News

News [2023 CWE Top 25 Weaknesses "On the Cusp" List Now Available](#)

News [2023 "CWE Top 25" Now Available!](#)

News [CWE Version 4.12 Now Available](#)

News [Enhancing Automotive Security with CWE](#)

News [Choose How You View CWE Weaknesses Using the New "Custom" Filter](#)

[More >>](#)

System Monitoring Tools

What happens to all this data ?

Prefer Loose Coupling: Business requirements change, and your production system will look different a year from now. similarly, your monitoring system needs to evolve over time as the services it monitors evolve through different patterns of failure.”



What If ?

What if there was an AI Model and System that could digest event logs, emails, text, zoom meetings, scan an existing system and take input about a potential system to provide a detailed resilience report. It could analyze the data to determine **the attack/threat surface, identify all of the weaknesses, dependencies people, tech and environment vulnerabilities, and risk** with a goal to generate a detailed action plan.

What if the AI Model understood Chaos engineering and could simulate all potential threat events and provide a detailed resiliency plan ?

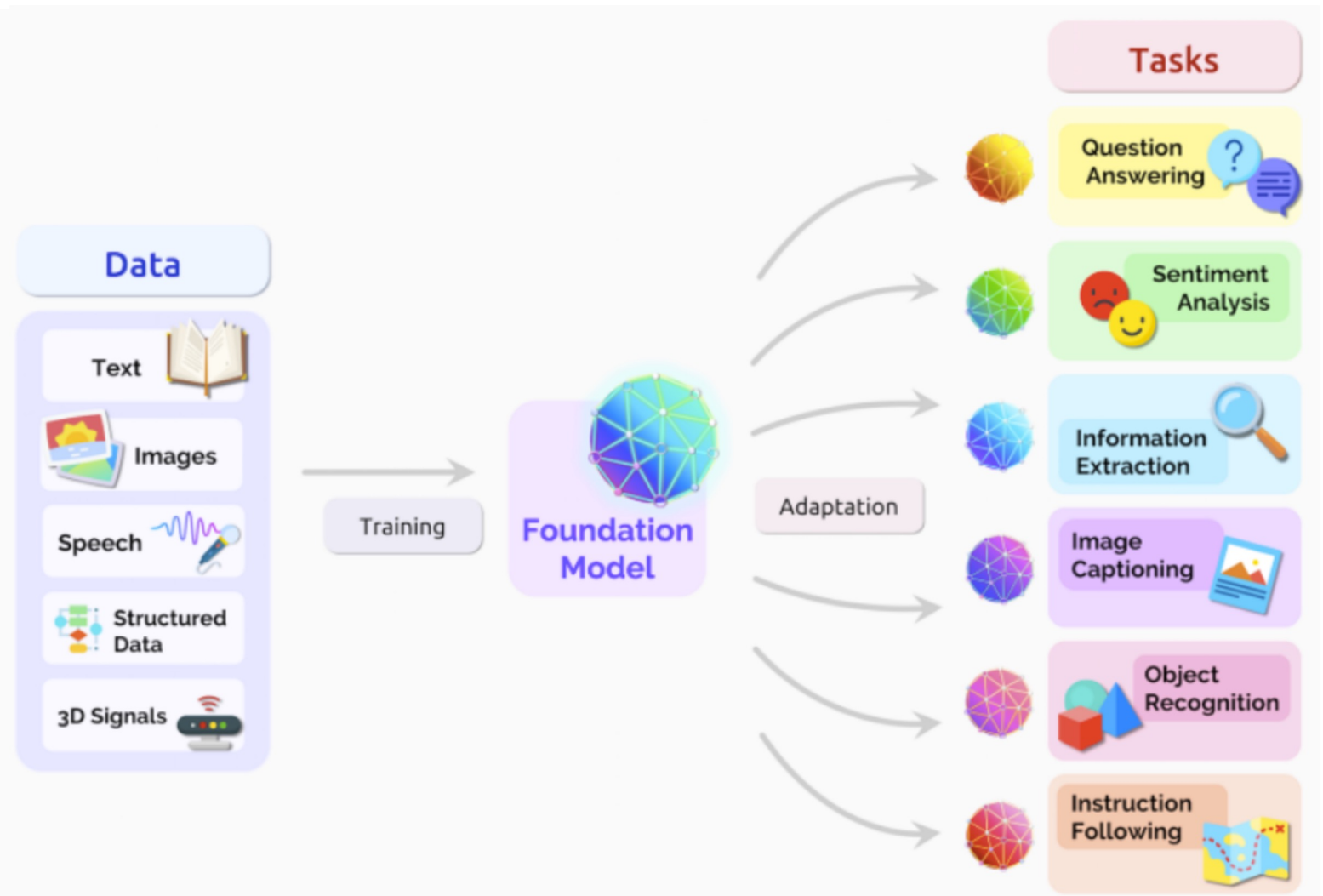
What would be required ?



Quick – Large Language Models (LLM)

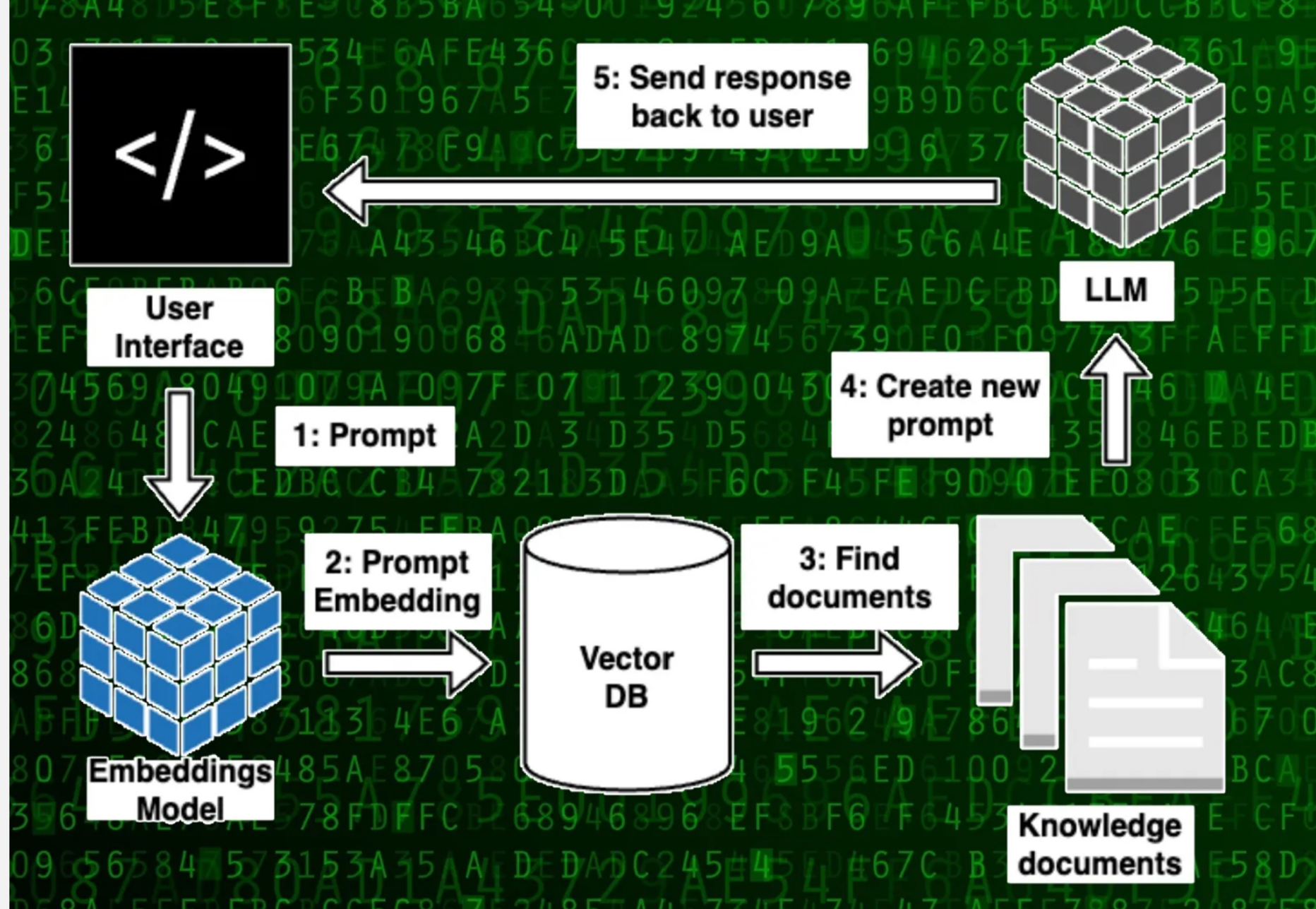
LLM is a type of artificial intelligence (AI) that can generate human-quality text.

LLMs are trained on massive datasets of text and code, and they can be used for a variety of tasks, such as writing, translating, and coding.



It is just this simple.

But most LLM Models require a costly and fast processing system with a GPU



Quick – Large Language Models (LLM)

Three Types of Machine Learning Models

Descriptive to help understand what happened in the past.

- What if a model could help with forensic cybersecurity incidents.

Prescriptive to automate business decisions and processes based on data.

- What if a model could help create a comprehensive threat model for a new or existing system.

Predictive to predict future business scenarios.

- What if a model could help with preventing cybersecurity events by predicting threats based on real time events and logs.

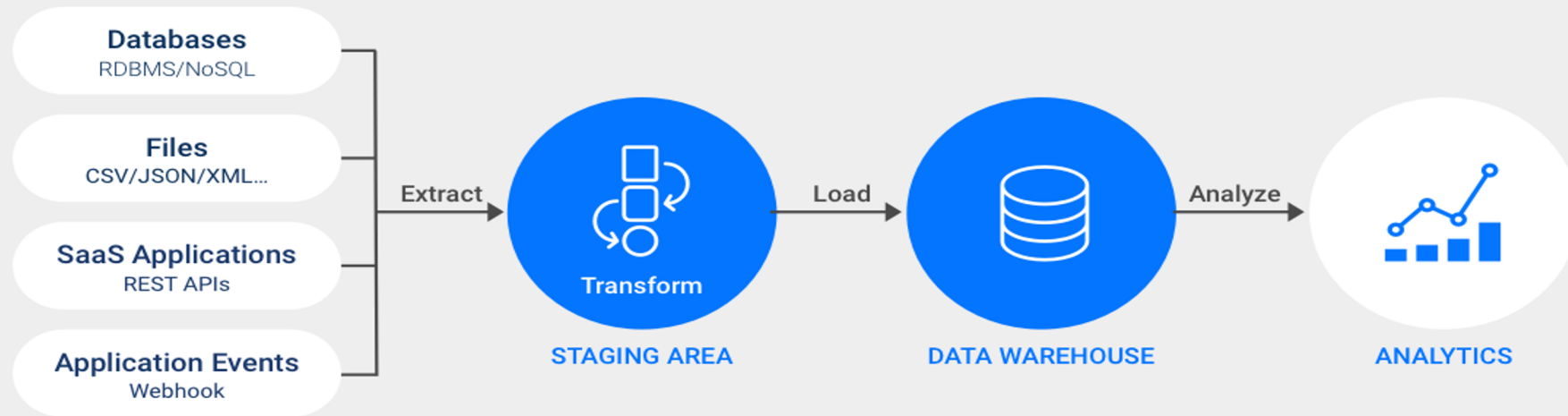
Data Needed for AI Model Building

Do you have a data management system that consolidates and labels all of this data for use in building an AI LLM model ?

- Tabletop Exercises
- Access Control
- Firewalls
- (IDS/IPS) Detection and Protection
- Security Policies and Procedures
- Security Information and Event Management (SIEM)
- Regular Testing and Simulation
- Penetration Testing
- Anomaly Detection
- Threat Intelligence
- Incident Response Plan
- Forensics Tools
- Employee work and vacation schedules
- Help Desk Logs

Extract, transform, and load (ETL)

ETL PROCESS

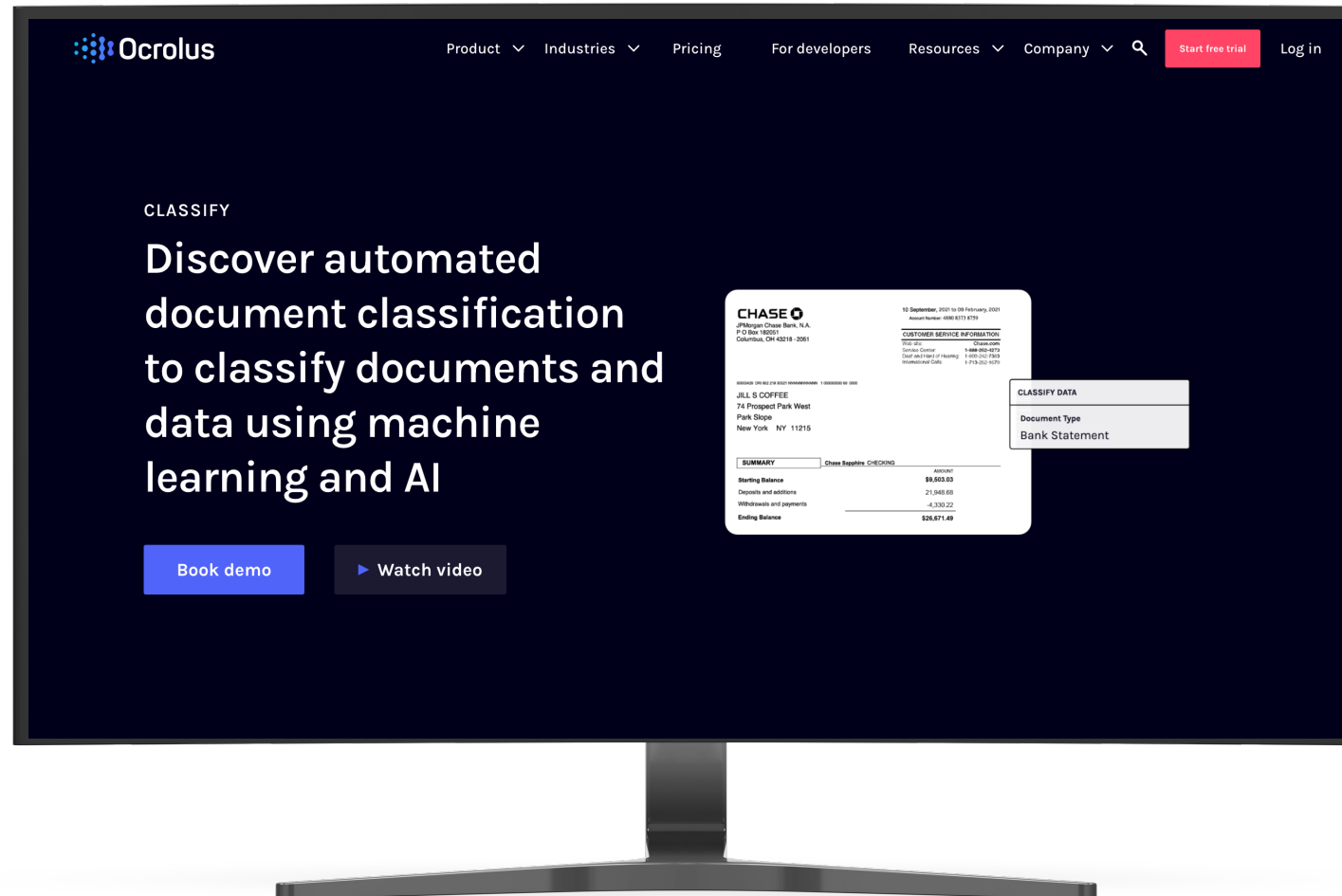


Open Source Products for Data PreProcessing



<https://unstructured-io.github.io/unstructured/index.html>

Example of Commercial Products for Data PreProcessing

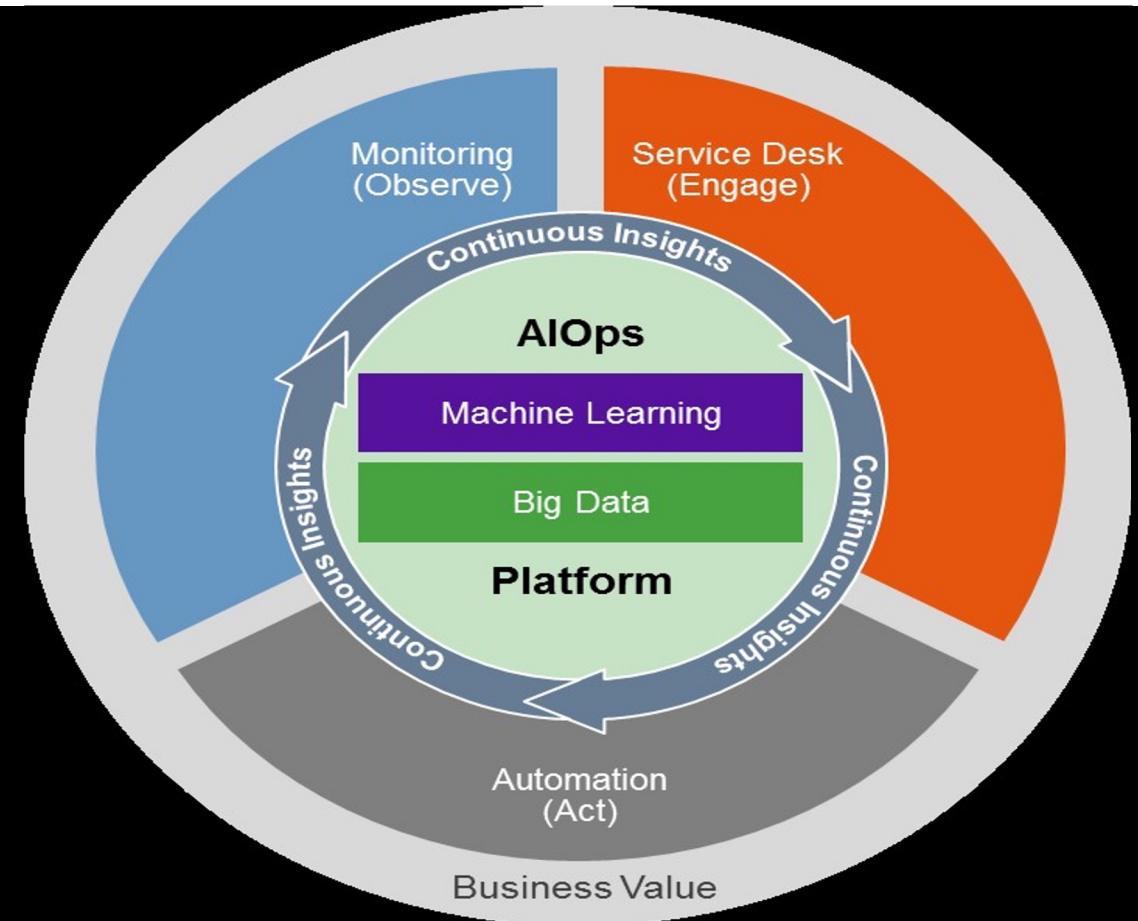


<https://www.ocrolus.com/>

Security Data Management – Things We Know

AIOps is a Few Years Old . What more is needed ?

AIops combines big data and machine learning to automate IT operations processes, including event correlation, anomaly detection and causality determination.



AI Threat Modeling

What kind of data can be used to train AI models for better detection of threats and countermeasure techniques?

The data which can be used to train and deploy the AI models may include the following:

- **Attack technique dataset** - This dataset may include information about past attacks, techniques and known vulnerabilities.
- **Network log dataset** - This dataset may include events about the system itself, as well as normal and abnormal traffic details in the logs.
- **Vulnerability dataset** - This dataset includes information about system and software vulnerabilities, including their severity and risk factors, which are publicly available by credited sources like MITRE and OWASP.
- **Threat intelligence dataset** - This dataset may include recent information about known threats, vulnerabilities, tactics and techniques.

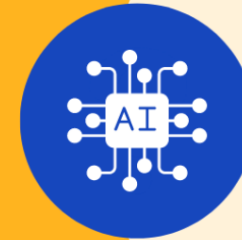
<https://community.threatmodeler.com/threatmodeling-appsec-130/generative-ai-for-threat-modeling-667>

AI Threat Modeling

Generative AI for Threat Modeling

2 months ago • 0 replies • 267 views

Generative AI for Threat Modeling

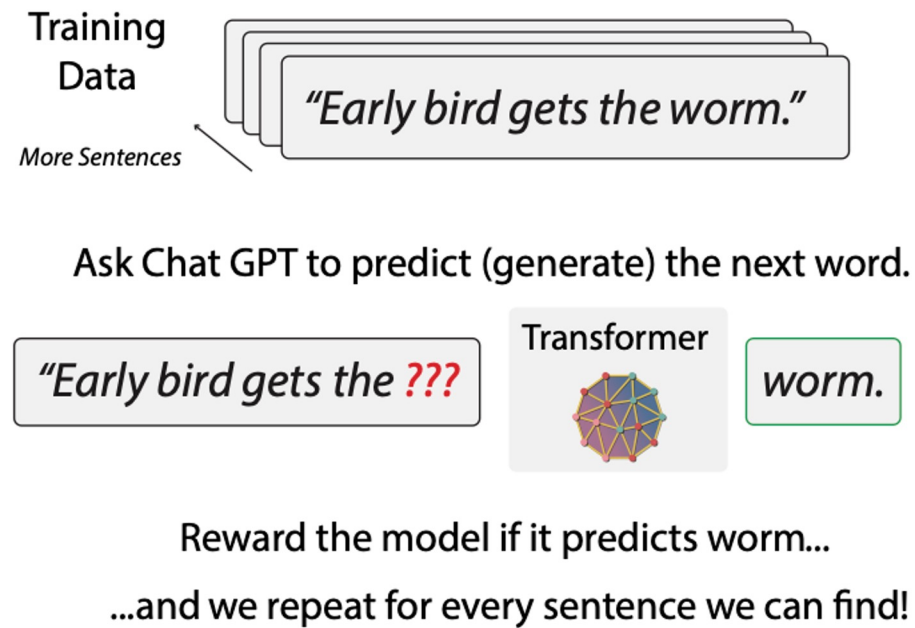


<https://community.threatmodeler.com/threatmodeling-appsec-130/generative-ai-for-threat-modeling-667>

Understanding the Ingredients in ChatGPT is Simpler Than You Think

by Chris Ré.

How does Chat GPT work?



Generative

We are asking Chat GPT to generate the next word!

Pretrained

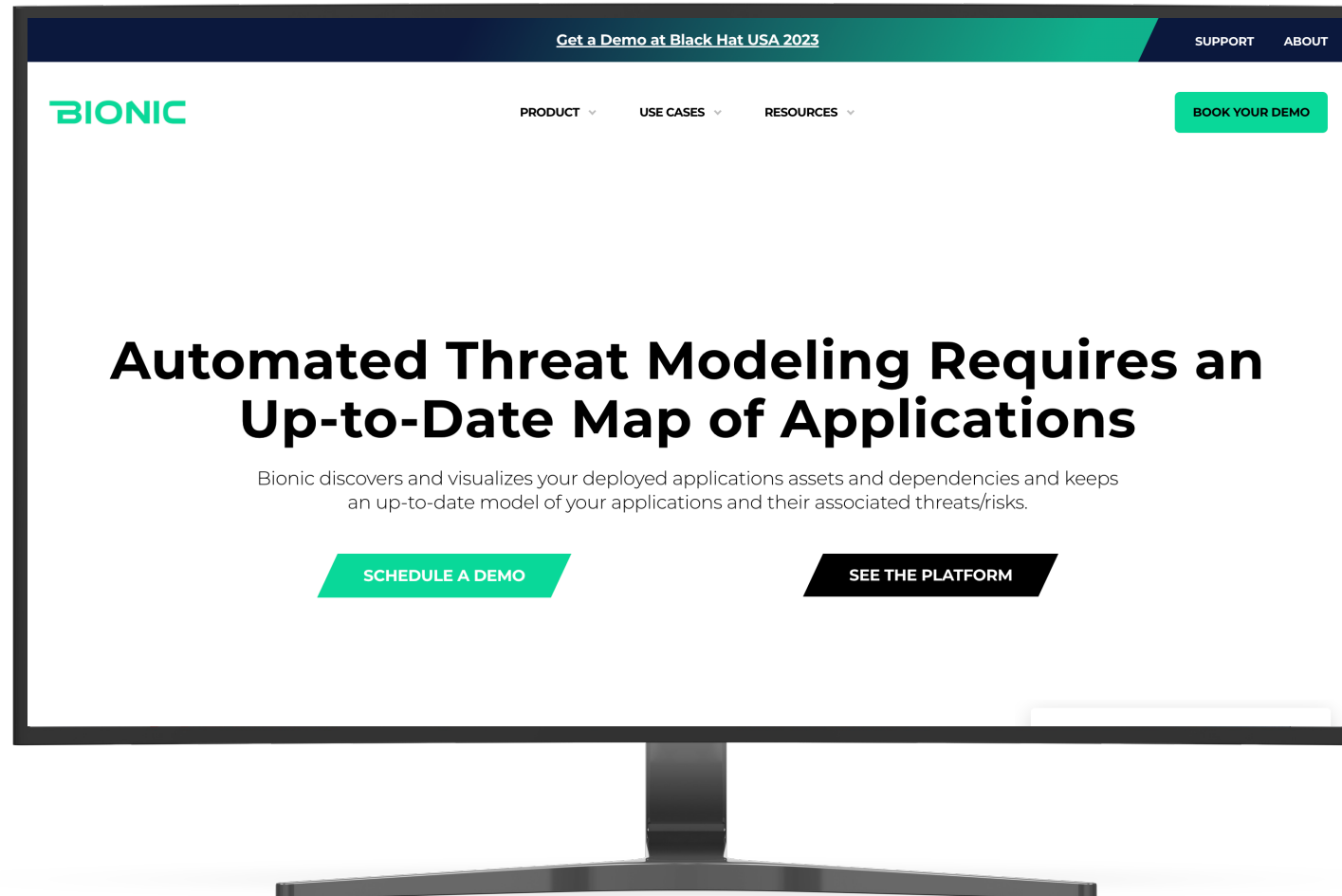
Trained on a simple task, but can be applied to many others!

Transformer

The ML model that guesses the word.

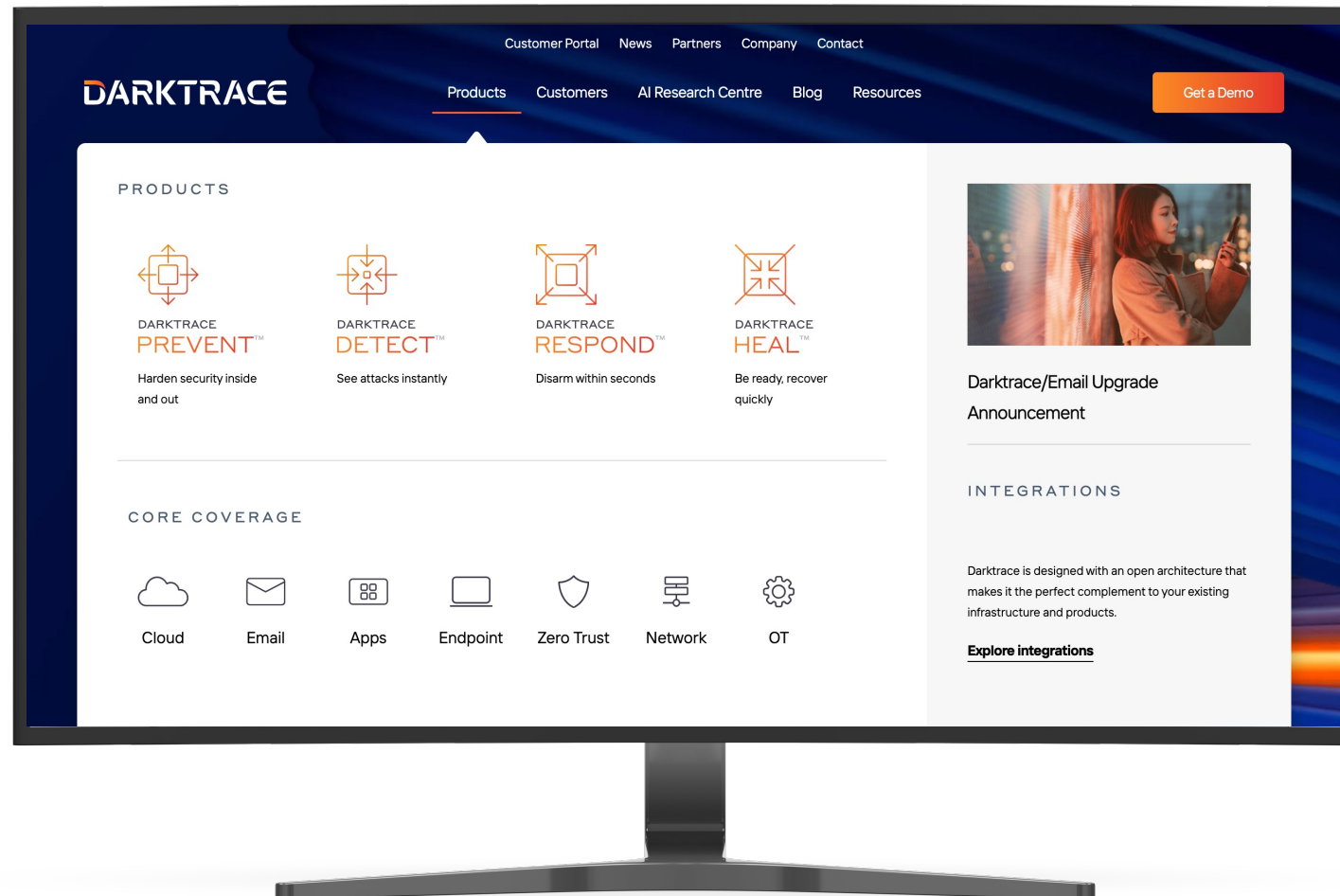
<https://hazyresearch.stanford.edu/blog/2023-04-20-how-chatgpt-works>

Data, Data, Data



<https://bionic.ai/threat-modeling/>

What more is need ? Most solutions are limited in coverage.



<https://darktrace.com/>

|.NET Why .NET ▾ Features ▾ Learn ▾ Docs ▾ Downloads Community

LIVE TV

All Microsoft ▾ Search 🔍

Home / Machine learning / ML.NET / Model Builder

 **Build intelligent apps** Infuse the power of OpenAI into your .NET applications.

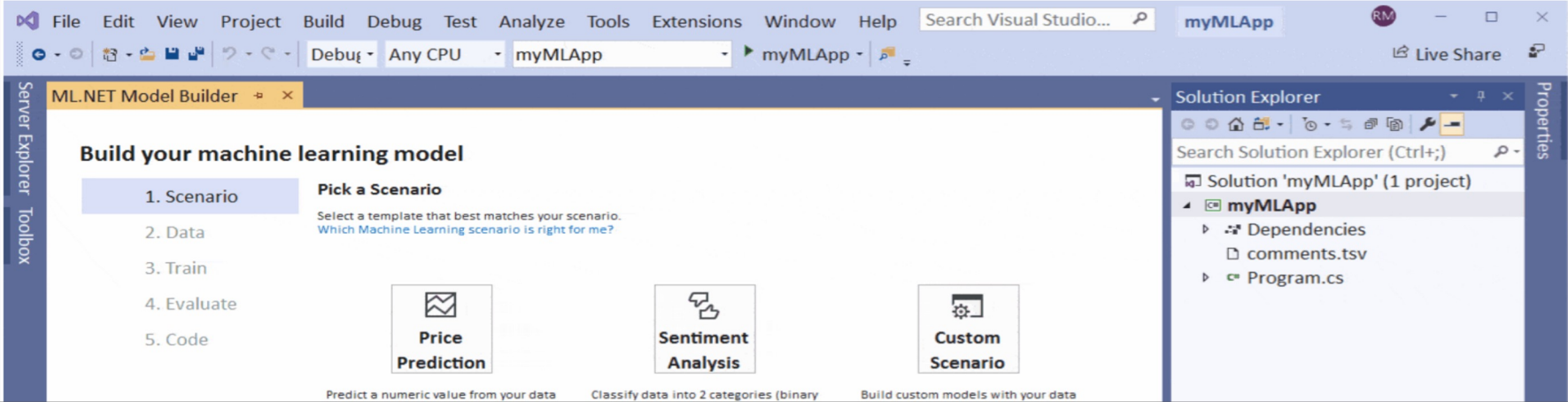
Get started today ✕

ML.NET Model Builder

Approachable machine learning in Visual Studio

Get started

Download



ML.NET Tutorial - Get started in 10 minutes

Windows

Linux

macOS

Intro

Download and install

Create your app

Pick a scenario

Download and add data

Train your model

Evaluate your model

Generate code

Consume your model

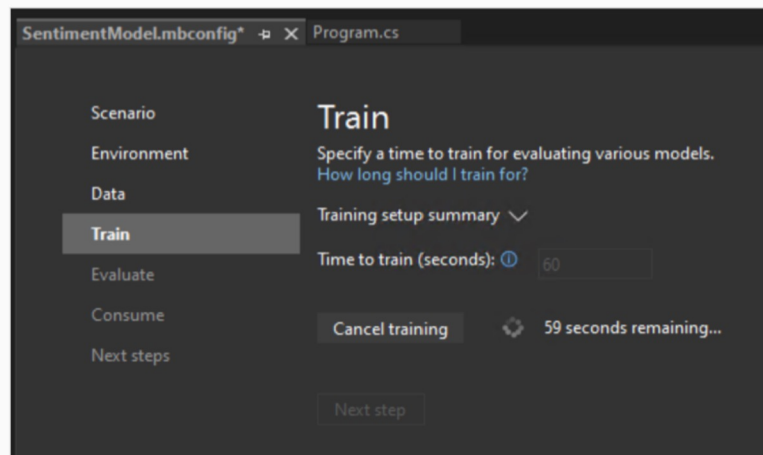
Next steps

Train your model

Now, you'll train your model with the `yelp_labelled.txt` dataset.

Model Builder evaluates many models with varying algorithms and settings based on the amount of training time given to build the best performing model.

1. Change the **Time to train**, which is the amount of time you'd like Model Builder to explore various models, to **60** seconds (you can try increasing this number if no models are found after training) . Note that for larger datasets, the training time will be longer. Model Builder automatically adjusts the training time based on the dataset size.
2. Select **Start training** to start the training process. Once training starts, you can see the time remaining.





<https://towardsdatascience.com/fasttext-bag-of-tricks-for-efficient-text-classification-513ba9e302e7>

FastText is an open-source, free, lightweight library that allows users to learn text representations and text classifiers. It works on standard, generic hardware. Models can later be reduced in size to even fit on mobile devices.

Artificial Intelligence With Python



Q&A

THANK YOU

