Cybersecurity and AI / Machine Learning in Healthcare

Shaun Kane, CISSP, CASP, C|EH
Director of Cybersecurity

Dr. Jonathan Mullin, PhD
Chief Scientist

What is Cybersecurity?

Cybersecurity is the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. (Wikipedia)

> "All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."
> — **Sun Tzu, The Art of War**

Adversaries

Hacktivists

"We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us."

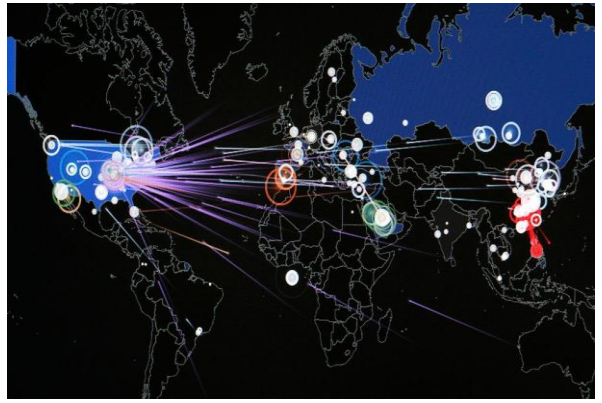
Cybercriminals

Cybercrime is a crime that involves a computer and a network.

Cyberterrorists

Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.

Cyberwarfare



Cyberwarfare is the use of digital attacks against an enemy state, causing comparable harm to actual warfighting apparatus, personnel, and/or disruption of vital computer systems.

M.I.C.E.

Healthcare Data Breaches

2021 – 10 Largest Healthcare Data Breaches (SC Magazine)

~22.6 million patients

2021 – largest cybersecurity impacts in the history of Healthcare

Use of legacy technologies

Failing to patch known security gaps

Failure to prioritize identity and access management

Failure to prioritize High Value Assets

Failure to visualize and inventory assets

Do you see Cybersecurity as a Cost Center or a Business Enabler?

Average Costs Per Breach

IBM - *Cost of a Data Breach Report 2021:*

- 2021 had the highest average cost in 17 years
  - Data breach costs rose from USD 3.86 million to USD 4.24 million, the highest average total cost in the 17-year history of this report.
- Remote work due to COVID-19 increased cost
  - The average cost was USD 1.07 million higher in breaches where remote work was a factor in causing the breach, compared to those where remote work was not a factor.
- Compromised credentials caused the most breaches
  - The most common initial attack vector, compromised credentials, was responsible for 20% of breaches at an average breach cost of USD 4.37 million.

Average Costs Per Breach

- Security AI had the biggest cost-mitigating effect
  - Automation and security artificial intelligence (AI), when fully deployed, provided the biggest cost mitigation, up to USD 3.81 million less than organizations without it.
- A Zero Trust approach helped reduce cost
  - The average cost of a breach was USD 1.76 million less at organizations with a mature zero trust approach, compared to organizations without zero trust.

Zero Trust Architecture

Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to “never trust, always verify.” Every access request is fully authenticated, authorized, and encrypted before granting access. Microsegmentation and least privileged access principles are applied to minimize lateral movement. Rich intelligence and analytics are utilized to detect and respond to anomalies in real time. (Microsoft)

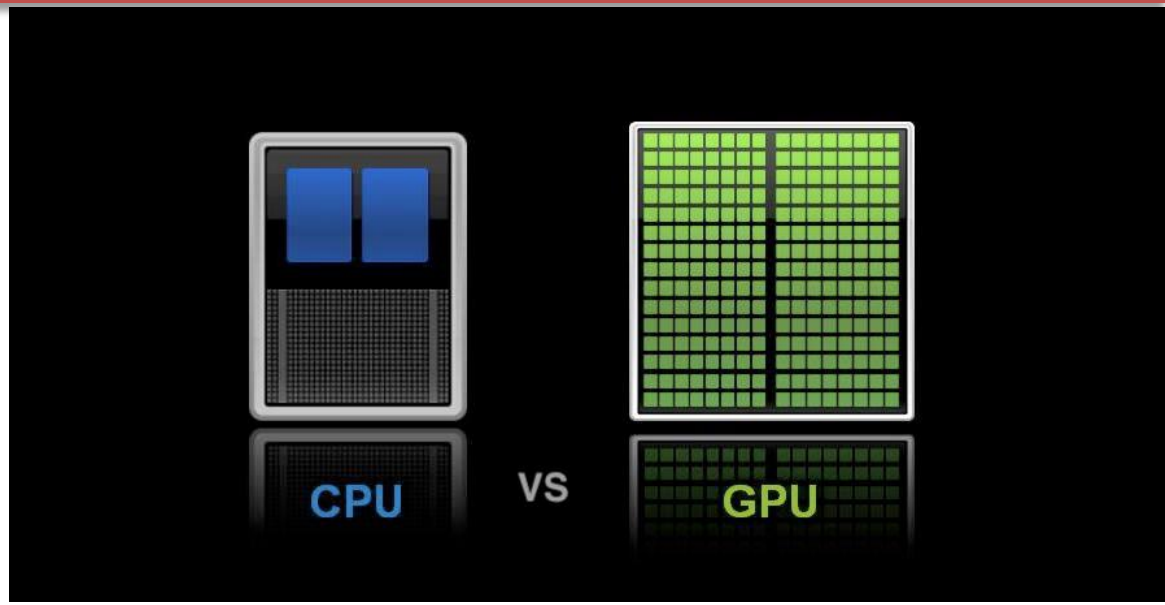
Infinite Cycle

Cybersecurity never ends, never rests, never quits.

- Multiple Cybersecurity Frameworks (NIST CSF, RMF, CMMC, FedRAMP, HIPAA HITECH, PCI-DSS) [Process]
- Multiple Cybersecurity Disciplines (C-Suite, EVP, Architect, Engineering, Analyst, Network, Software, DevSecOps, Policy Analyst, Incident Responder, et al.) [People]
- Multiple Cybersecurity Technologies (Firewalls, Intrusion Prevention, Intrusion Detection, Anti-Virus, Anti-Malware, etc.) [Technology]

All are factors that either positively or negatively impact your revenue

Traditional Cybersecurity



- Signature base methods
  - Only detects previously seen threats
  - Easily evaded by modern ML techniques
- Moves at the speed of CPU
  - Fight ML w/ ML, requires GPU
- Oriented to traditional network/host
  - Modern Networks moving to cloud/VMs
- We approach our security not by trusting labels.
  - We use the ZeroTrust concepts to let models develop labels
  - We use patterns-of-Life within CyberData to apply controls based on behavioral analysis.
  - We don't trust the users, We model them and alert for unusual actions.

TriNNity is NLP for cyber

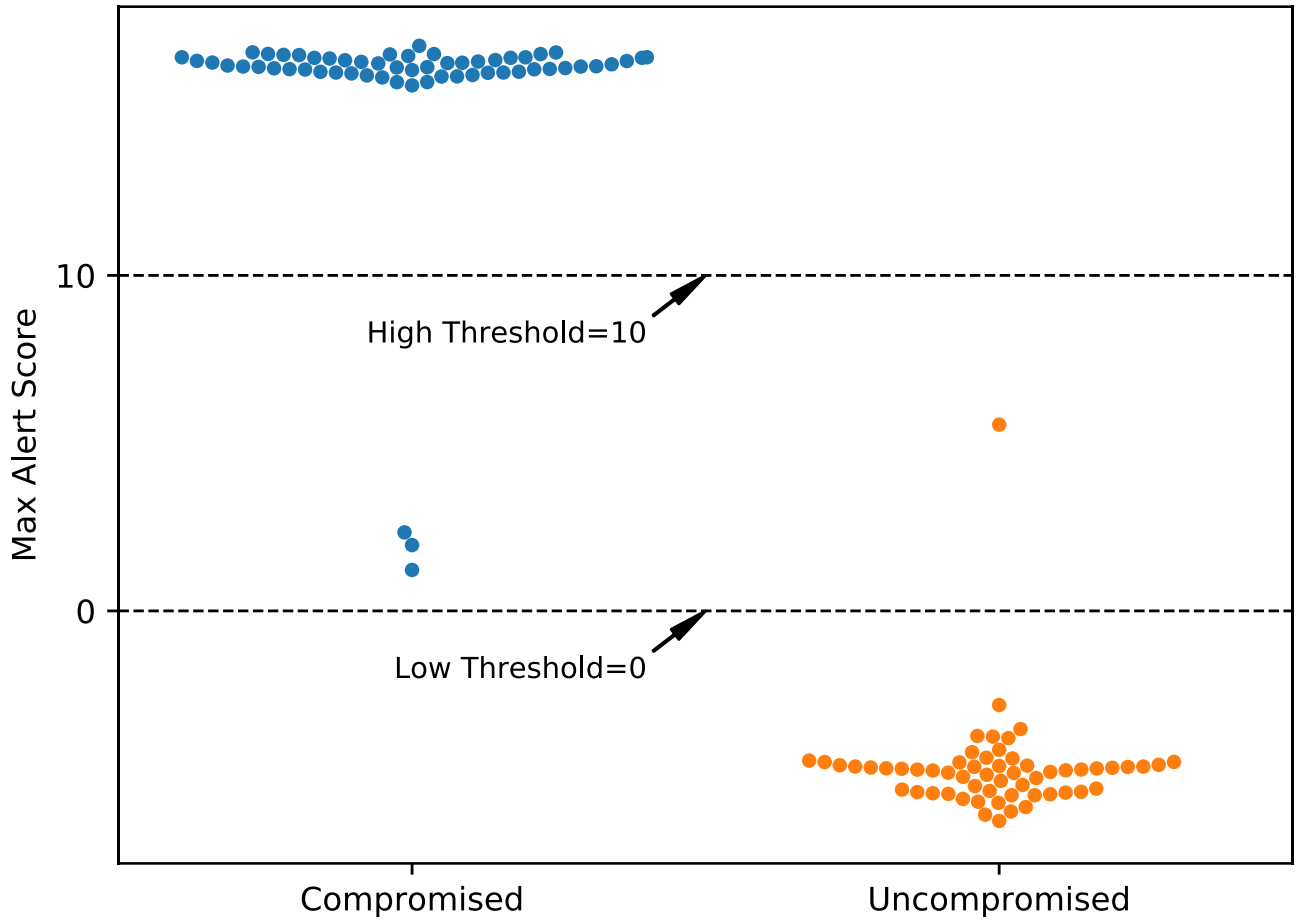
- Cyber data can be expressed as text: Windows Event Logs, Network Packets, etc.
- Apply NLP to learn the “language” of a cyber data
- No data labeling necessary (Zero Trust focused)
- Detects never-before-seen threats (Bring your 0 days)

We've Got you Covered

- We detect from initial access to C2 and Exfiltration.
- We monitor your network, the endpoints, and processes holistically
- One approach, specialized models, timely alerts

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain		SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking		DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning		Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking		DLL Side-Loading	Network Sniffing					Remote Access Tools
	Regsvcs/Regasm	External Remote Services		Exploitation for Defense Evasion	Password Filter DLL					Remote File Copy

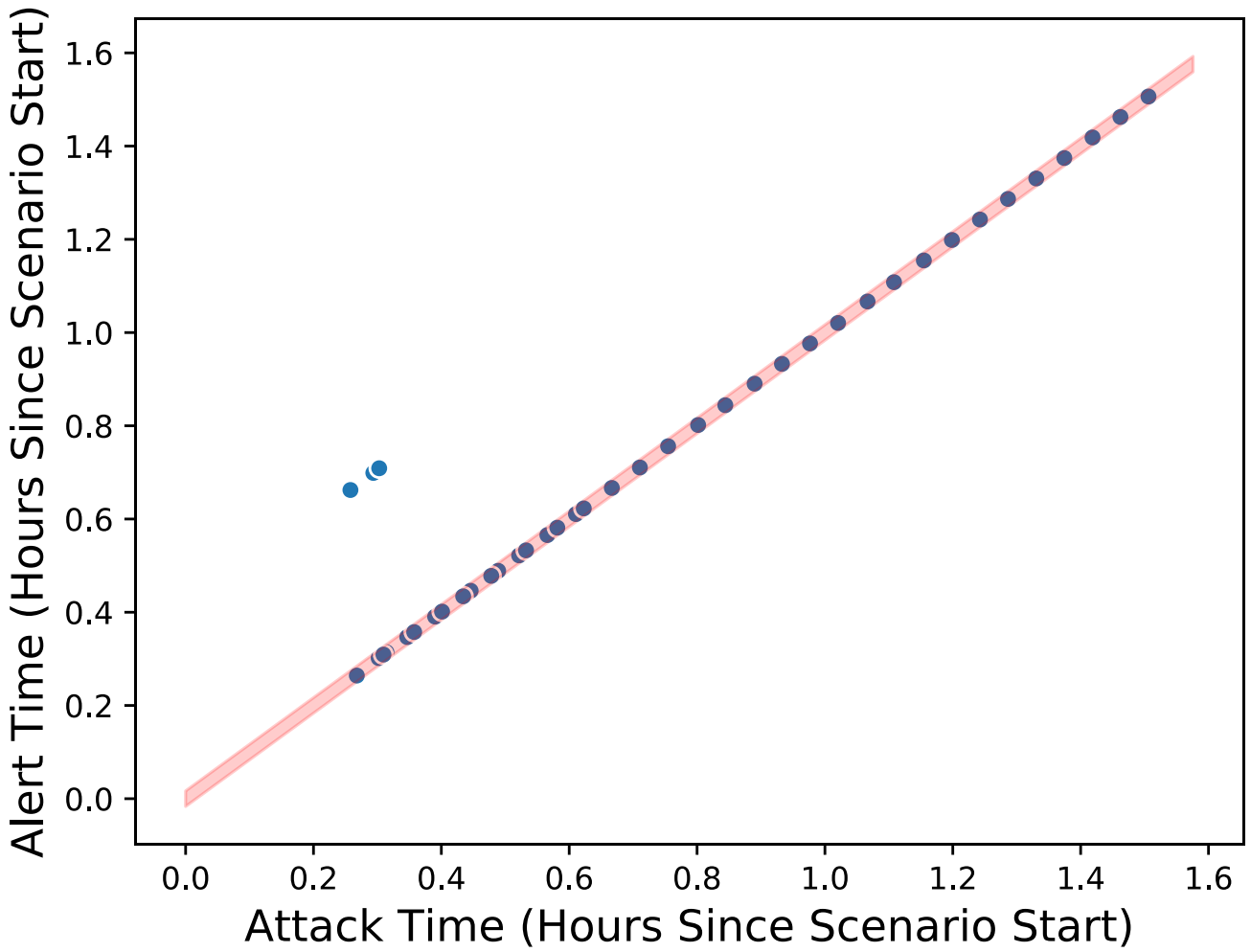
Detects threats with high accuracy



- 0 is highest benign alert score
- Nothing special about thresholds
- 1 “false positive” with low threshold: kernel panic.

Single scope knob for adjustable sensitivity

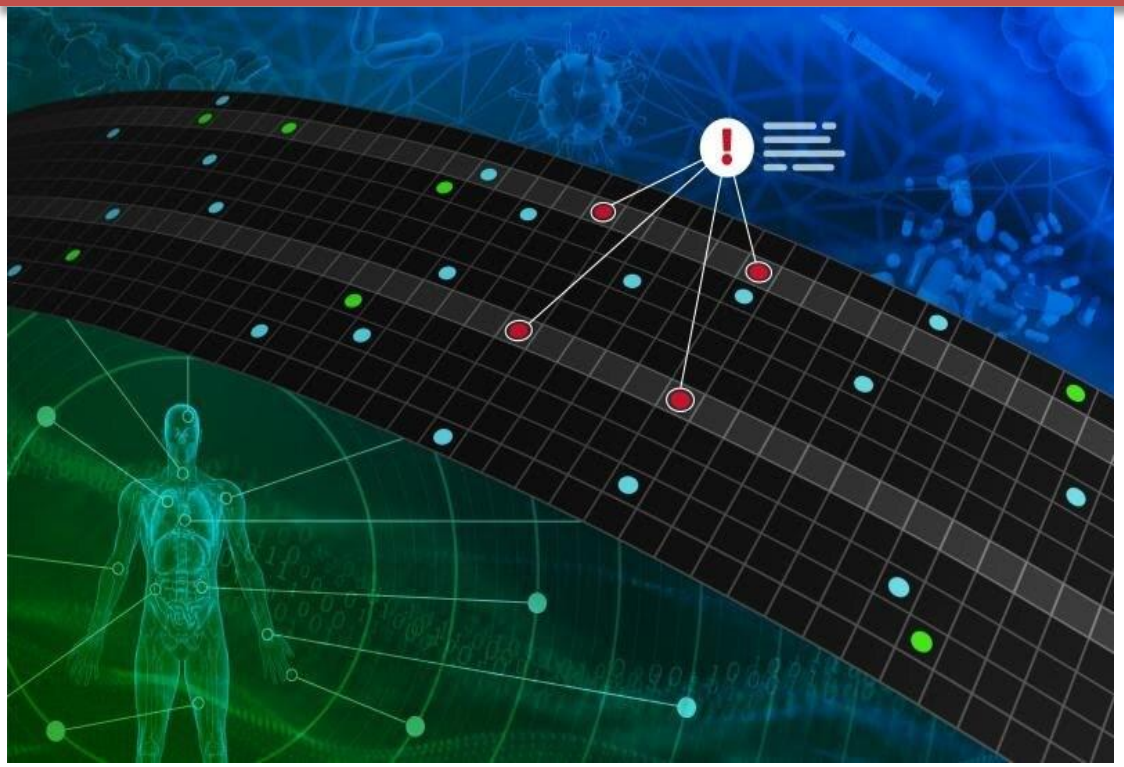
<1 min detection



Points within red band alerted within one minute of the attack occurring

High Precision in time and alerts

AI is here for Healthcare



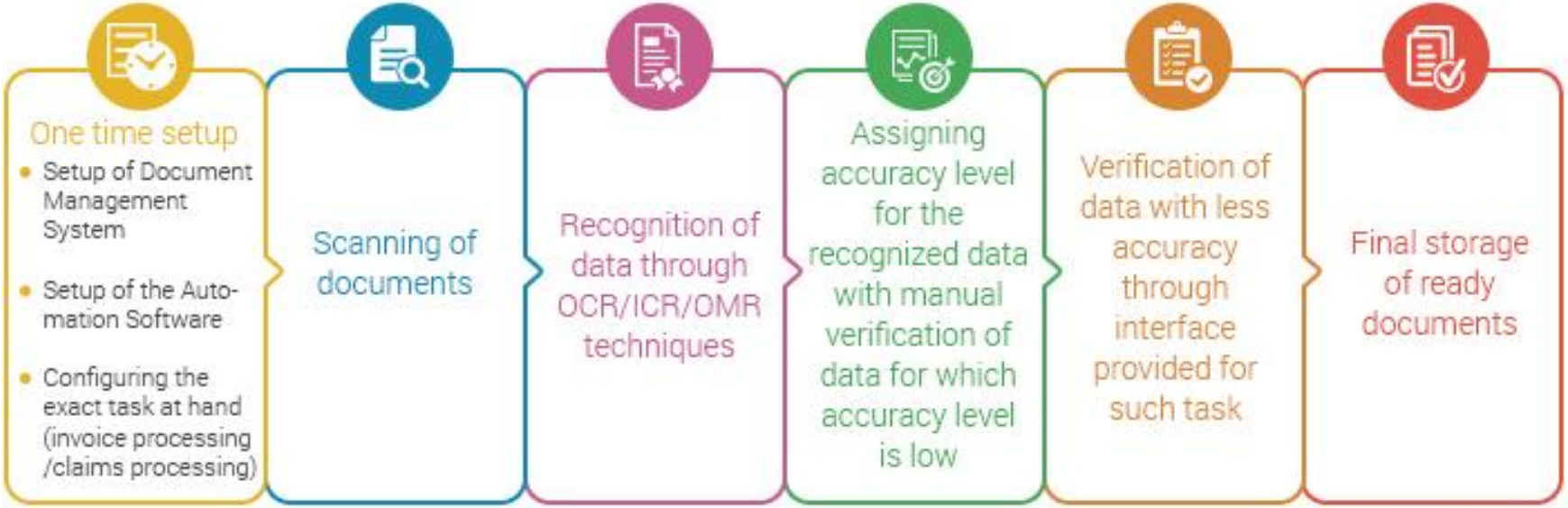
Initial work has been on retuning Visual AI for assisting diagnoses

We at DCI have work on expressing Health indicators (phenotypic) and Expressing that as a vector (set of numbers)

These approaches allow us to directly translate the advances in Cyber to the health field as well

Medical Records

- Bring in the past
- Deal with paper



Digital Document	Semantic Annotations	Named Entity Recognition	Graph Analytic	Anomaly detection
• OCR • Digital records	• Word models • Text cleaning	• Transformer models • Entity statistic	• Knowledge graphs • Geo-Locate	• Find errors • Catch correlations missed in person

Billing, same structure

- Again, the power of NLP allows for building relationships within your existing data resources
- Re-use the power of custom fit AI/ML to specialize in Billing
- Still can bring in the old and the paper, modify the AI/ML and retune

- OCR
- Digital records

- Word models
- Text cleaning

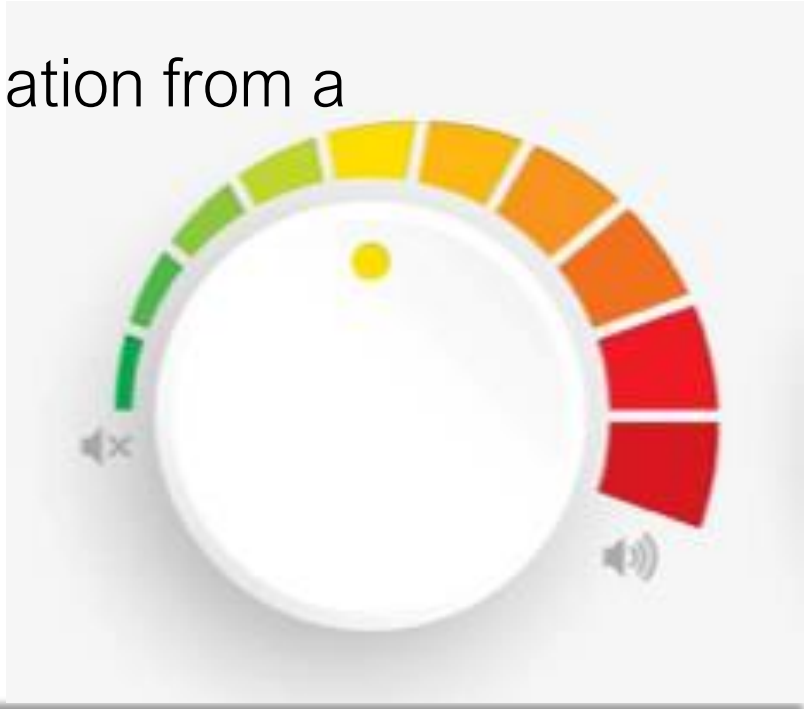
- Transformer models
- Entity statistic

- Knowledge graphs
- Geo-Locate

- Find errors
- Catch correlations missed in person

Scalable Automation

- We have designed our approaches to assist and empower
- Our models don't just tell you an answer, they explain WHY
- That WHY builds trust and allows users to scale automation from a recommendation to full automation



Enabling the Revenue Cycle

Every bit of patient data is valuable to someone else as well as to your organization. A common axiom of Cybersecurity Professionals is “Assume Breach.” Your organizations’ cybersecurity teams are working quite hard in a resource-constrained environment. Alas, there are always issues to remediate.

The magic of DCI Solutions is that we crave difficult problems to solve, and that is an enormous part of our corporate culture. Consequentially, it is also our approach to solving difficult problems - using persistence, drive, and creativity.

We’d love to talk with you about how to better enable your revenue cycle while protecting your data and keeping your environment secure and your patients safe.