

Is Your SOC Overwhelmed? Artificial Intelligence and MITRE ATT&CK Can Help Lighten the Load



Adam Frank
CTO Security Intelligence – IBM Security

You **NEED** to build
your security
practice around
**Artificial
Intelligence!**



The deck is
STACKED against
you!



Your Goals As A Security Operations Team Are Fundamental To Your Business



The Challenges

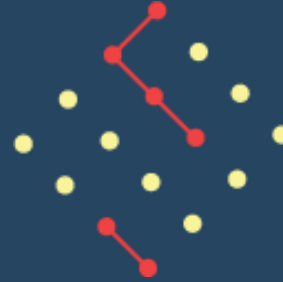
Insight Overload



93%

of organizations are unable to triage all relevant threats

Disconnected Dots



Information is often overlooked simply because analysts do not know how it is connected

Tools can't act



191 Days

Average dwell time of advanced persistent threats

Threats Are Evolving And Organizations Are Struggling

46%

Increase in insider attacks since
2014¹

82%

Insider & privilege misuse breaches
that took months, or even years,
to be discovered²

62%

Security experts who
expect hackers will use
AI within the year³

1.8 million

Unfulfilled cybersecurity
jobs by 2022⁴

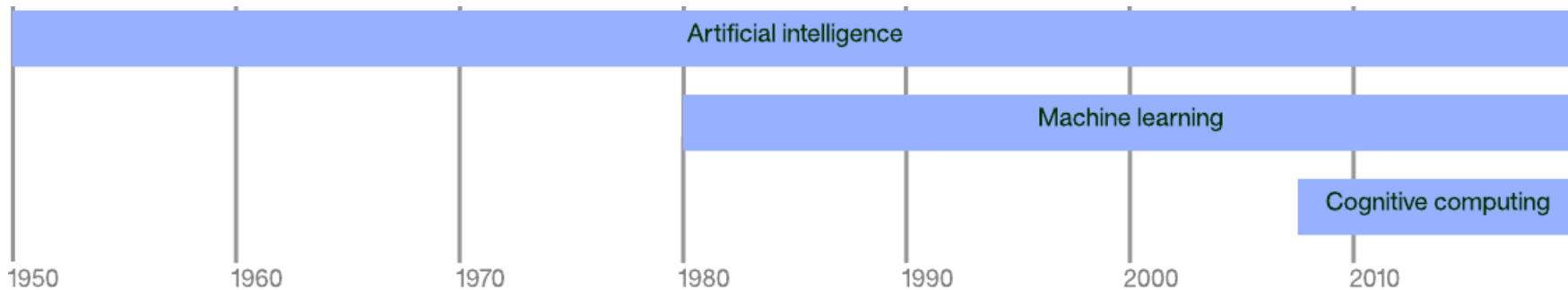
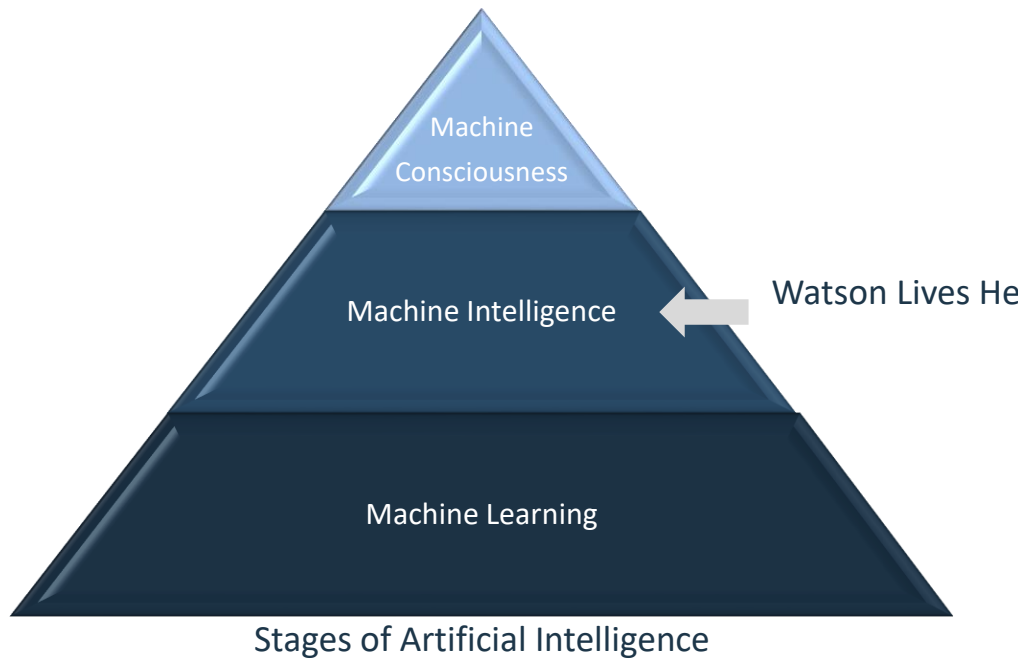
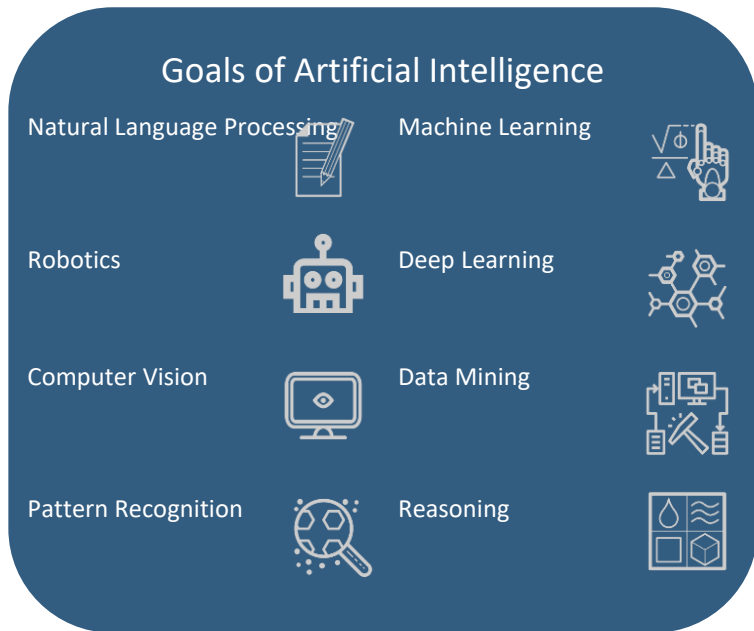
The Stakes Are At An All Time HIGH!



AI, your ACE in the hole?

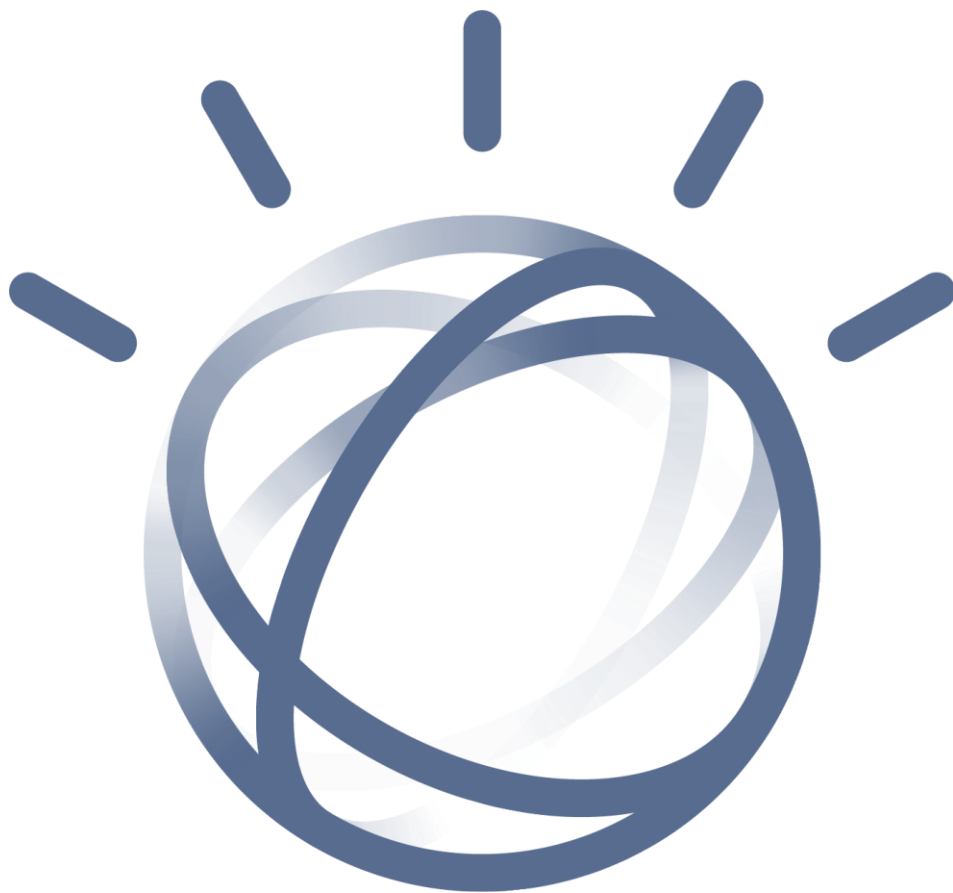


What Is Artificial Intelligence?

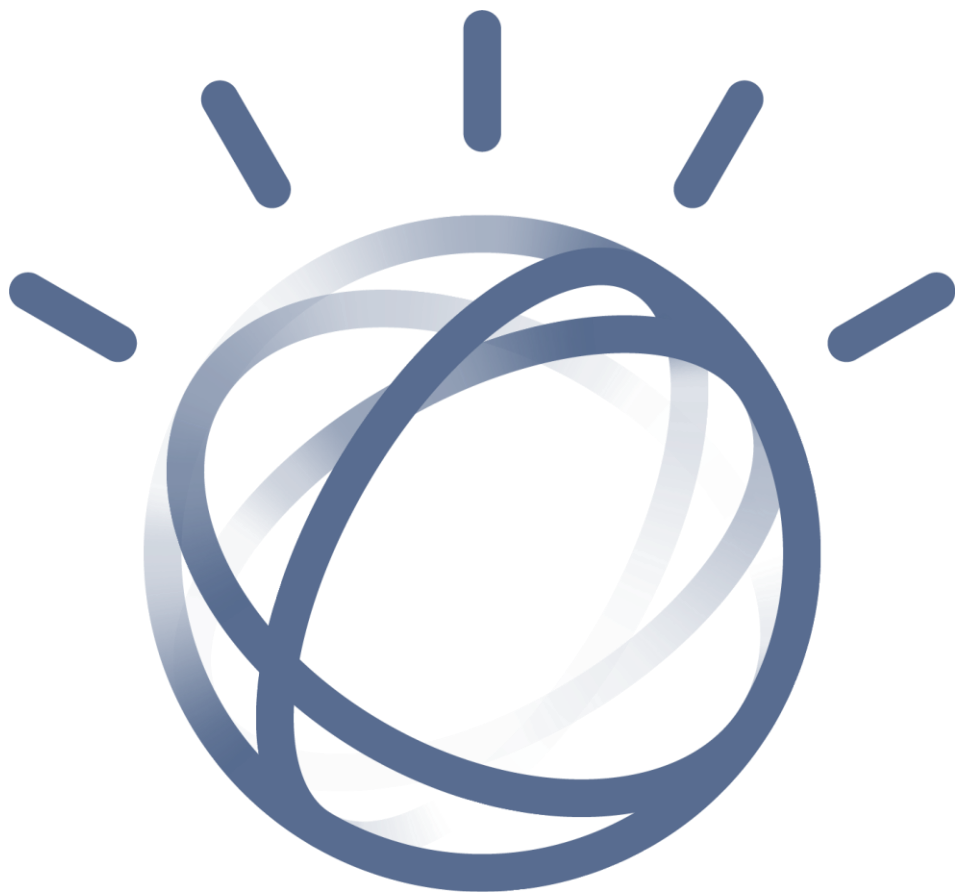


In 2011, the
Watson
computer
system
competed and
won
on *Jeopardy*





Watson is being used
for Healthcare,
Weather, Teaching,
Cooking and **Cyber
Security!**



Watson can process 500 gigabytes, the equivalent of 1 million books, per second!

Investigating An Incident Without AI



Tackle Where The Bulk of Your Team's Time Is Spent:

Incident Analysis

Continuously monitor the alert queue, collect investigative data and context including root cause diagnosis necessary to escalate security alerts

Response

Respond to security incidents and provide remediation

Threat Hunting

Perform deep-dive analysis, look for new analytic methods for detecting and preventing threats



**Simplify these
tasks**

Unlock A New Partnership Between Analysts And Their Technology



Three Key Benefits of adopting AI

Force Multiply Your Team's Efforts

Automate your repetitive SOC tasks



Drive Consistent and Deeper Investigations

Gain actionable insights into critical incidents



Reduce Dwell Times

Adopt a quicker and more decisive escalation process




How to speak **AI**

Using the MITRE
ATT&CK
framework



The **ATT&CK** Framework is more than a fun way to write Attack, it stands for

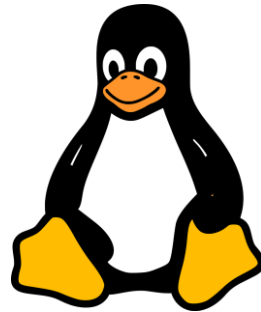
Adversarial Tactics,
Techniques &
Common **K**nowledge.



It is a framework started by **MITRE** Corporation in 2013 and has been growing ever since.

ATT&CK is community driven and updated quarterly by **MITRE**, it represents the **Tactics** and **Techniques** in a manner not specific to specific products or signature.

There are currently 3 **Matrices** for: **PRE-ATT&CK**, **ATT&CK** Enterprise and Mobile



macOS

How ATT&CK Is Laid Out

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 Items	27 Items	42 Items	21 Items	53 Items	15 Items	20 Items	15 Items	13 Items	9 Items	19 Items
Drive-by Compromise	Command-Line Interface	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Brute Force	Account Discovery	Remote Desktop Protocol	Clipboard Data	Data Compressed	Commonly Used Port
Exploit Public-Facing Application	Execution through API	Create Account	Bypass User Account Control	Bypass User Account Control	Credential Dumping	Application Window Discovery	Remote File Copy	Data from Network Shared Drive	Data Encrypted	Data Encoding
Hardware Additions	Graphical User Interface	New Service	New Service	File Deletion	Credentials in Files	File and Directory Discovery	Windows Admin Shares	Data Staged	Exfiltration Over Alternative Protocol	Multiband Communication
Replication Through Removable Media	PowerShell	Registry Run Keys / Startup Folder	Process Injection	Masquerading	Input Capture	Network Share Discovery	Application Deployment Software	Input Capture	Exfiltration Over Command and Control Channel	Remote File Copy
Scripting	Rundll32	Scheduled Task	Valid Accounts	Network Share Connection Removal	Account Manipulation	Password Policy Discovery	Software Model	Screen Capture	Automated Exfiltration	Standard Application Layer Protocol
Spearphishing Attachment	Scripting	Scheduled Task	Accessibility Features	Obfuscated Files or Information	Credentials in Registry	Permission Groups Discovery	Distributed Component Object Model	Audio Capture	Data Transfer Size Limits	Standard Cryptographic Protocol
Spearphishing Link	Service Execution	Account Manipulation	AppCert DLLs	Process Injection	Exploitation for Credential Access	Process Discovery	Exploitation of Remote Services	Automated Collection	Exfiltration Over Other Network Medium	Communication Through Removable Media
Spearphishing via Service	User Execution	AppCert DLLs	AppInit DLLs	Rundll32	Access	Query Registry	Logon Scripts	Data from Information Repositories	Exfiltration Over Physical Medium	Custom Command and Control Protocol
Supply Chain Compromise	CMSTP	AppInit DLLs	Application Shimming	Scripting	Forced Authentication	Remote System Discovery	Logon Scripts	Replication Through Removable Media	Exfiltration Over Physical Medium	Custom Cryptographic Protocol
Trusted Relationship	Compiled HTML File	Application Shimming	DLL Search Order Hijacking	Valid Accounts	Hooking	Security Software Discovery	Pass the Hash	Data from Local System	Scheduled Transfer	Custom Cryptographic Protocol
Valid Accounts	Control Panel Items	Authentication Package	Exploitation for Privilege Escalation	Binary Padding	Kerberoasting	System Information Discovery	Pass the Ticket	Data from Removable Media	Scheduled Transfer	Custom Cryptographic Protocol
	Dynamic Data Exchange	BITS Jobs	Exploitation for Privilege Escalation	Binary Padding	LLMNR/NBT-NS Poisoning	System Network Configuration Discovery	Replication Through Removable Media	Email Collection	Domain Fronting	Fallback Channels
	Execution through Module Load	bootkit	Extra Window Memory Injection	Code Signing	Network Sniffing	System Network Connections Discovery	Shared Webroot	Man in the Browser	Multi-hop Proxy	Multi-Stage Channels
	Exploitation for Client Execution	Change Default File Association	File System Permissions Weakness	Compiled HTML File	Private Keys	System Owner/User Discovery	Taint Shared Content	Video Capture	Multilayer Encryption	Remote Access Tools
	InstallUtil	Component Firmware	Hooking	Component Firmware	Two-Factor Authentication Interception	System Service Discovery	Third-party Software		Standard Non-Application Layer Protocol	Uncommonly Used Port
	LSASS Driver	Component Object Model Hijacking	Image File Execution Options Injection	Component Object Model Hijacking		System Time Discovery	Windows Remote Management		Web Service	
	Mahta	DLL Search Order Hijacking	Path Interception	Control Panel Items						
	Regsvcs/Regasm	External Remote Services	Port Monitors	Deobfuscate/Decode Files or Information						
	Regsvr32	File System Permissions Weakness	Scheduled Task	Scheduled Task						
	Scheduled Task	Hidden Files and Directories	Service Registry Permissions Weakness	Disabling Security Tools						
	Signed Binary Proxy Execution	Hooking	SID-History Injection	DLL Search Order Hijacking						
	Signed Script Proxy Execution	Hypervisor	Web Shell	DLL Side-Loading						
	Third-party Software	Image File Execution Options Injection		Exploitation for Defense Evasion						
	Trusted Developer Utilities	Injection		Extra Window Memory injection						
	Windows Management Instrumentation	Logon Scripts		File Permissions Modification						
	Windows Remote Management	LSASS Driver		File System Logical Offsets						
	XSL Script Processing	Modify Existing Service		Hidden Files and Directories						
		Netsh Helper DLL		Image File Execution Options Injection						
		Office Application Startup		Indicator Blocking						
		Path Interception		Indicator Removal from Tools						
		Port Monitors		Indicator Removal on Host						
		Redundant Access		Indirect Command Execution						
		Screensaver		Install Root Certificate						
		Security Support Provider		InstallUtil						
		Service Registry Permissions Weakness		Modify Registry						
		Shortcut Modification		Mshta						
		SIP and Trust Provider Hijacking		NTFS File Attributes						
		System Firmware		Process Doppelgänger						
		Time Providers		Process Hollowing						
		Valid Accounts		Redundant Access						
		Web Shell		Regsvcs/Regasm						
		Windows Management Instrumentation Event Subscription		Regsvr32						
		Winlogon Helper DLL		Rootkit						
				Signed Binary Proxy Execution						
				Signed Script Proxy Execution						
				SIP and Trust Provider Hijacking						
				Software Packing						
				Template Injection						
				Timstomp						
				Trusted Developer Utilities						
				Web Service						
				XSL Script Processing						

How ATT&CK Is Laid Out

Initial Access 10 Items	Execution 27 Items	Persistence 42 Items	Privilege Escalation 21 Items	Defense Evasion 53 Items	Credential Access 15 Items	Discovery 20 Items	Lateral Movement 15 Items	Collection 13 Items	Exfiltration 9 Items	Command And Control 19 Items
Drive-by Compromise	Command-Line Interface	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Brute Force	Account Discovery	Remote Desktop Protocol	Clipboard Data	Data Compressed	Commonly Used Port
Exploit Public-Facing Application	Execution through API	Create Account	Bypass User Account Control	Bypass User Account Control	Credential Dumping	Application Window Discovery	Remote File Copy	Data from Network Shared Drive	Data Encrypted	Data Encoding
Hardware Additions	Graphical User Interface	New Service	New Service	File Deletion	Credentials in Files	File and Directory Discovery	Windows Admin Shares	Drive	Exfiltration Over Alternative Protocol	Multiband Communication
Replication Through Removable Media	PowerShell	Registry Run Keys / Startup Folder	Process Injection	Masquerading	Input Capture	Network Share Discovery	Application Deployment Software	Data Staged	Input Capture	Remote File Copy
Spearpishing Attachment	Rundll32	Scheduled Task	Valid Accounts	Network Share Connection Removal	Account Manipulation	Password Policy Discovery	Distributed Component Object Model	Screen Capture	Exfiltration Over Command and Control Channel	Standard Application Layer Protocol
Spearpishing Link	Scripting	Accessibility Features	Obfuscated Files or Information	Process Injection	Credentials in Registry	Permission Groups Discovery	Exploitation of Remote Services	Automated Exfiltration	Automated Exfiltration	Standard Cryptographic Protocol
Spearpishing via Service	Service Execution	Account Manipulation	AppCert DLLs	Process Injection	Exploitation for Credential Access	Process Discovery	Exploitation of Remote Services	Audio Capture	Data Transfer Size Limits	Communication Through Removable Media
Supply Chain Compromise	User Execution	AppInit DLLs	AppInit DLLs	Rundll32	Forced Authentication	Query Registry	Automated Collection	Automated Collection	Exfiltration Over Other Network Medium	Custom Command and Control Protocol
	CMSTP	AppInit DLLs	Application Shimming	Scripting	Hooking	Remote System Discovery	Login Scripts	Data from Information Repositories	Exfiltration Over Physical	Custom Cryptographic Protocol
	Compiled HTML File	Application Shimming	DLL Search Order Hijacking	Valid Accounts		Remote Software Discovery	Pass the Hash			Data Obfuscation

Execution

27 items

Command-Line Interface

Execution through API

Graphical User Interface

PowerShell

Rundll32

Scripting

Service Execution

User Execution

CMSTP

Compiled HTML File

Control Panel Items

Dynamic Data Exchange

Persistence

42 items

Accessibility Features

Create Account

New Service

Registry Run Keys / Startup Folder

Scheduled Task

Account Manipulation

AppCert DLLs

AppInit DLLs

Application Shimming

Authentication Package

BITS Jobs

Privilege Escalation

21 items

Access Token Manipulation

Bypass User Account Control

New Service

Process Injection

Valid Accounts

Accessibility Features

AppCert DLLs

AppInit DLLs

Application Shimming

DLL Search Order Hijacking

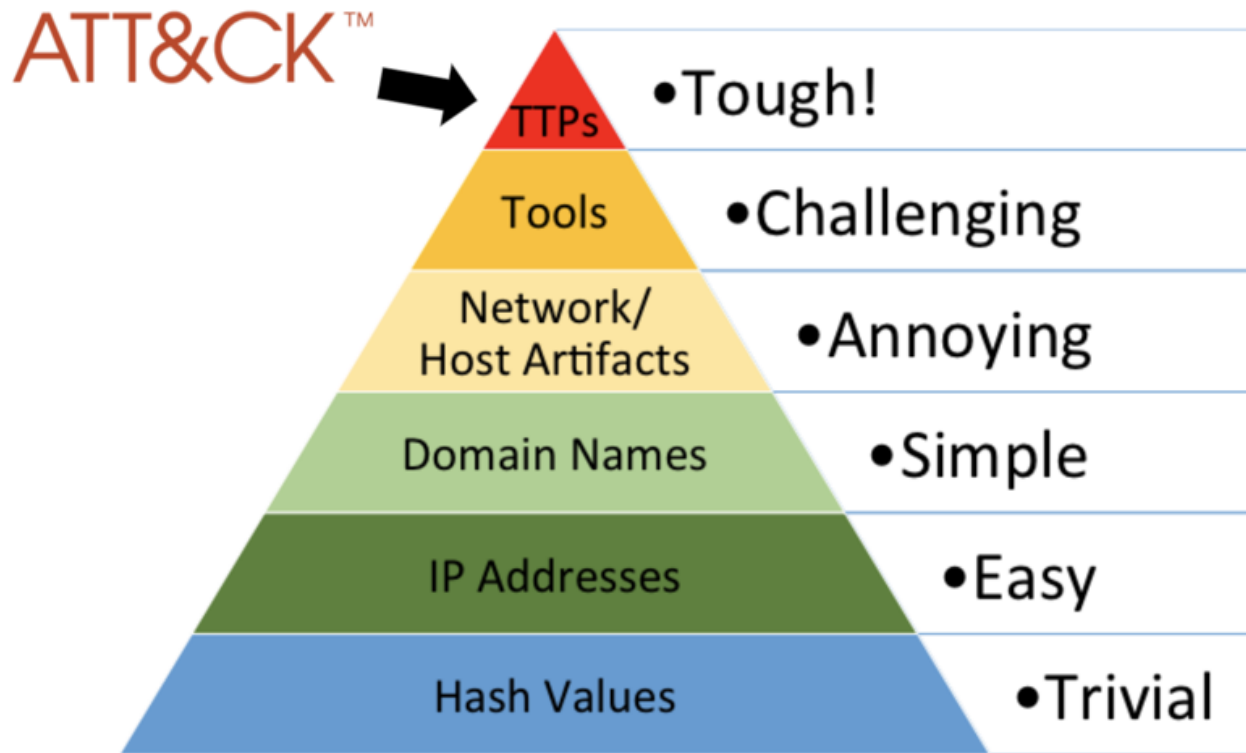
Exploitation for Privilege Escalation

Custom Cryptographic Protocol
Data Obfuscation
Domain Fronting
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multilayer Encryption
Remote Access Tools
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service

What Is A TECHNIQUE in ATT&CK?

Technique	New Service
Description	When operating systems boot up, they can start programs or applications called services that perform background system functions. [...] Adversaries may install a new service which will be executed at startup by directly modifying the registry or by using tools.
Platform	Windows
Permissions Required	Administrator, SYSTEM
Effective Permissions	SYSTEM
Detection	Monitor service creation through changes in the Registry and common utilities using command-line invocation ...
Mitigation	Limit privileges of user accounts and remediate Privilege Escalation vectors...
Data Sources	Windows registry, process monitoring, command-line parameters
Examples	Carbanak, Lazarus Group, TinyZBot, Duqu, CozyCar, CosmicDuke, hcdLoader, ...
References	1. Microsoft. (n.d.). Services. Retrieved June 7, 2016.

Where Does ATT&CK Fit

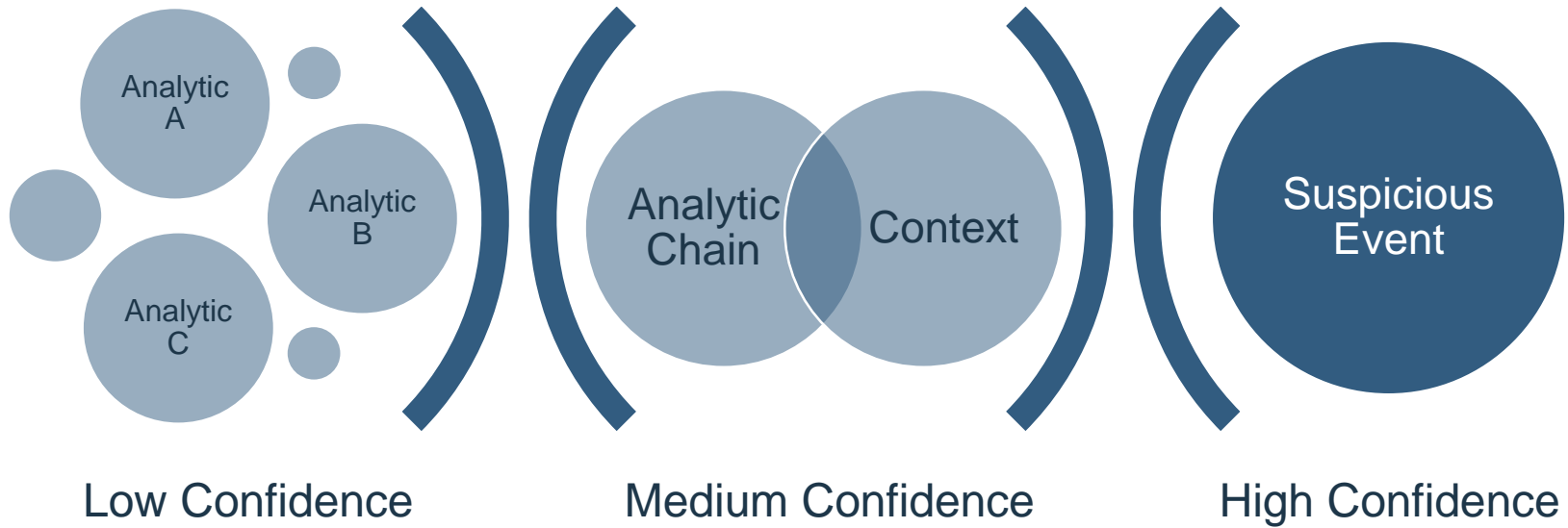


Source: David Bianco, <https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

David Bianco's Pyramid of Pain

Your Threat Intelligence, Detection Tools
and Remediation Tools are being
mapped to **ATT&CK** by vendors and
users

Techniques Alone Do Not Equal A Breach



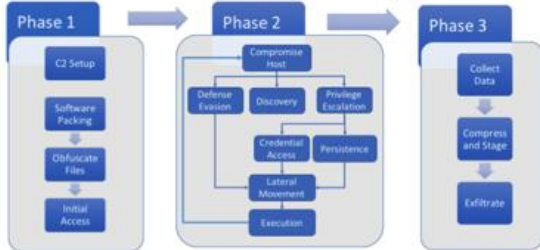
Measuring Your Defenses Using ATT&CK

Structured Threat Intel

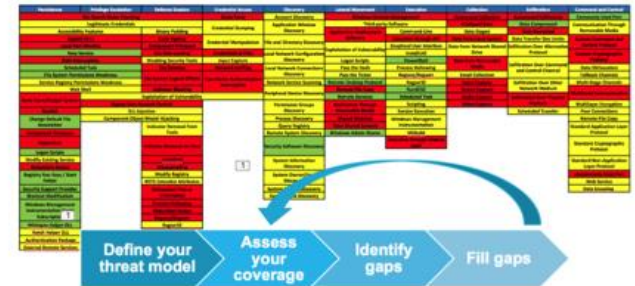
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
...

ATT&CK™

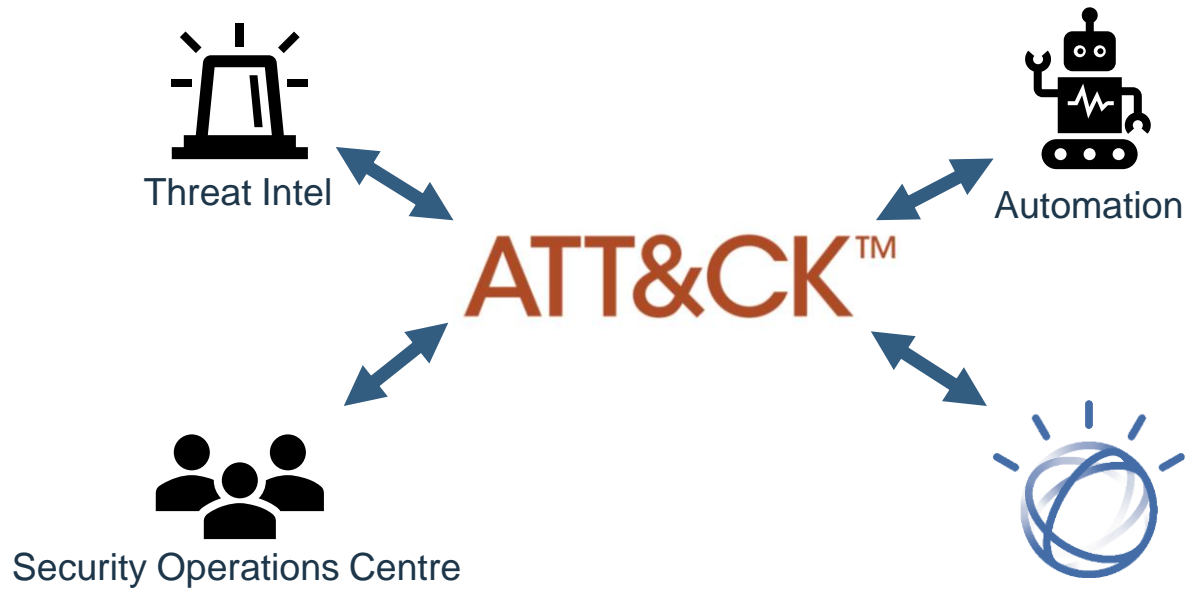
Intel-Driven Adversary Emulation



An ever-improving & validated defense



It All Fits Together Into your Operations





Brace yourselves...

~~Winter is coming~~

Here

How To Defeat Our Threats

- You need Tools with AI embedded in your SOC now
- Mature your automation and detection methods to leverage the AI by adopting the ATT&CK Framework.
 - Map your detection use cases to the ATT&CK Framework
 - Fit your tools into the Framework based on their capabilities

Helpful Links

- MITRE ATT&CK Framework

<https://attack.mitre.org>

- IBM Watson for Cyber Security



<https://www.ibm.com/security/artificial-intelligence>

- Follow us on Social Media:



<https://twitter.com/IBMSecurity>



<https://www.linkedin.com/showcase/ibm-security/>






<https://www.youtube.com/ibmsecurity>



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.