



Stop the Heist: How to D3FEND Against ATT&CKS and Save the Day

Owen Garrett

Deepfence, Inc

owen@deepfence.io



The task of securing Modern Infrastructure



The legacy view – “my application is a castle”

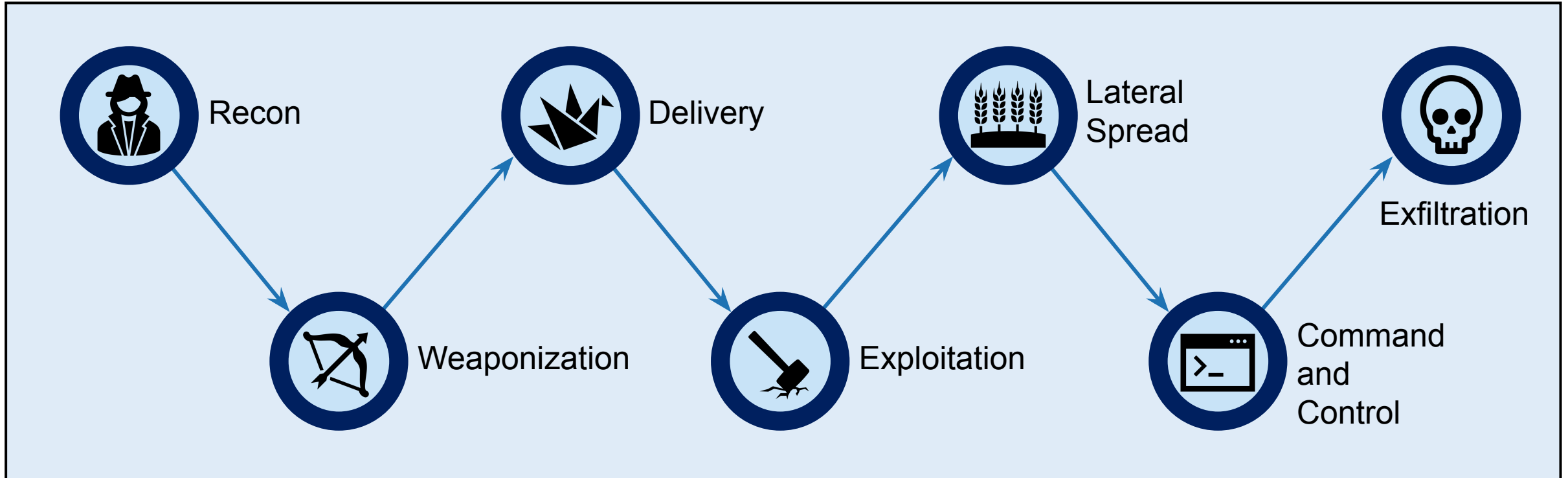


Production Platforms are a vibrant, growing city

- Complex, fluid, open, with many valuable assets
- Sophisticated attackers know to infiltrate and spread



Anatomy of a Heist: Cyber Kill Chain



The Casino Fish Tank Attack



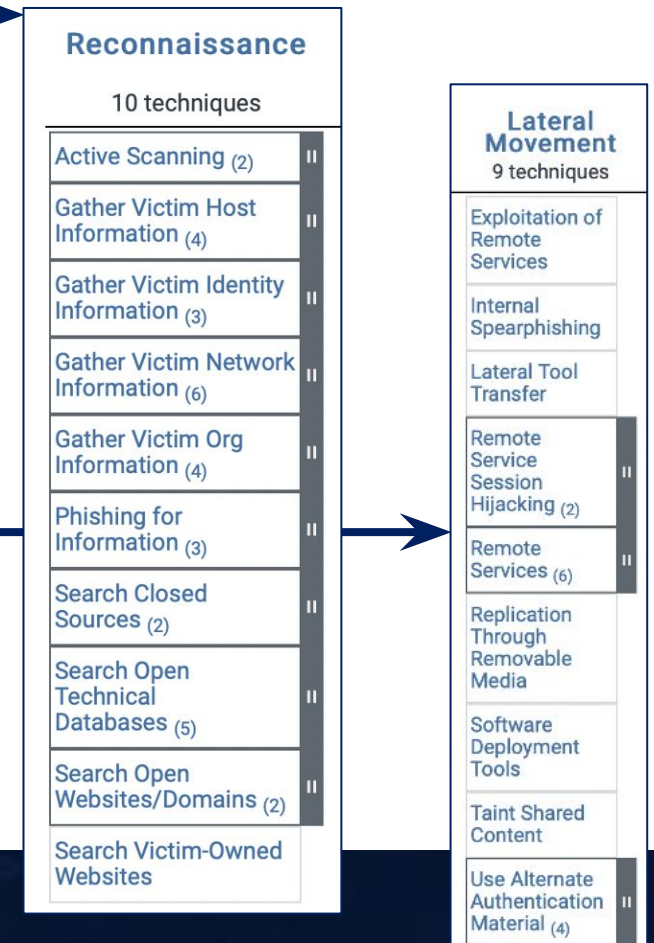
Next Generation – MITRE ATT&CK framework



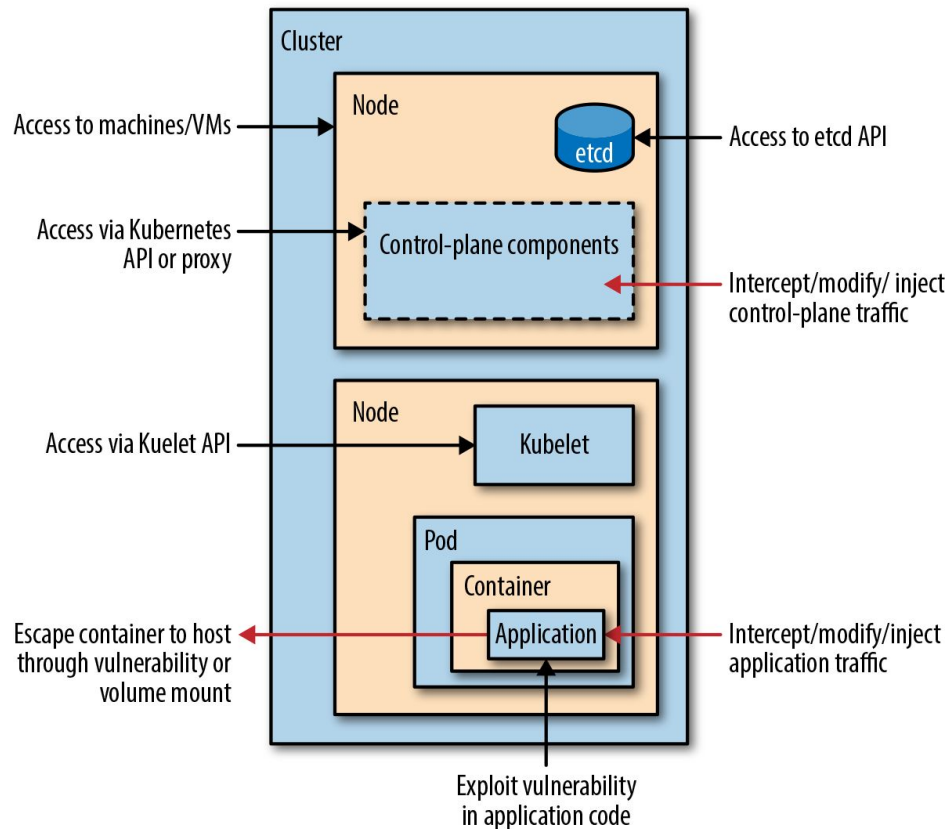
Adversary's Goals and Methods

Tactics, decomposed into **techniques** and **procedures**

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defensive Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact



Kubernetes Attack Surface



- Enormous Attack Surface
- Multiple potential beachheads and opportunities for lateral spread
 - CI compromise
 - Rogue Controller Services
 - Exposed Services
 - Compromised third-party images
 - Overly-permissive RBAC, Network or Service Account Policies

Source: O'Reilly: Kubernetes Security
by Liz Rice, Michael Hausenblas

Microsoft's Kubernetes Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Using Cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Data Destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal networking	Denial of service
Application vulnerability	Application exploit (RCE)		Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access Kubernetes dashboard	Applications credentials in configuration files	
Exposed Dashboard	SSH server running inside container					Instance Metadata API	Writable volume mounts on the host	
							Access Kubernetes dashboard	
							Access tiller endpoint	

Application-level threats and risks

Distributed, ephemeral moving parts with varying risk and threat profiles; made from first- and third-party components and tools.

Kubernetes cluster operations threats and risks

Software supply chain, build, and continuous integration (CI)-related risks and the delivery automation and continuous delivery.

Kubernetes infrastructure automation tooling, such as application and infrastructure monitoring and microservices life-cycle autonomous controllers.

Human operators (DevOps/site reliability engineering staff) who have privileges to perform actions within the cluster.

Source: <https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/>
<https://www.darkreading.com/threat-intelligence/microsoft-s-kubernetes-threat-matrix-here-s-what-s-missing>

Shopify

SUMMARY BY SHOPIFY



Shopify infrastructure is isolated into subsets of infrastructure. [@0xacb](#) reported it was possible to gain root access to any container in one particular subset by exploiting a server side request forgery bug in the screenshotting functionality of Shopify Exchange. Within an hour of receiving the report, we disabled the vulnerable service, began auditing applications in all subsets and remediating across all our infrastructure. The vulnerable subset did not include Shopify core.

After auditing all services, we fixed the bug by deploying a metadata concealment proxy to disable access to metadata information. We also disabled access to internal IPs on all infrastructure subsets. We awarded this \$25,000 as a Shopify Core RCE since some applications in this subset do have access to some Shopify core data and systems.



You are the star of your own movie



You are the star of your own movie



Discover and maintain your city map



Annotate it with potential security vulnerabilities



Observe activity and alert to suspicious behavior

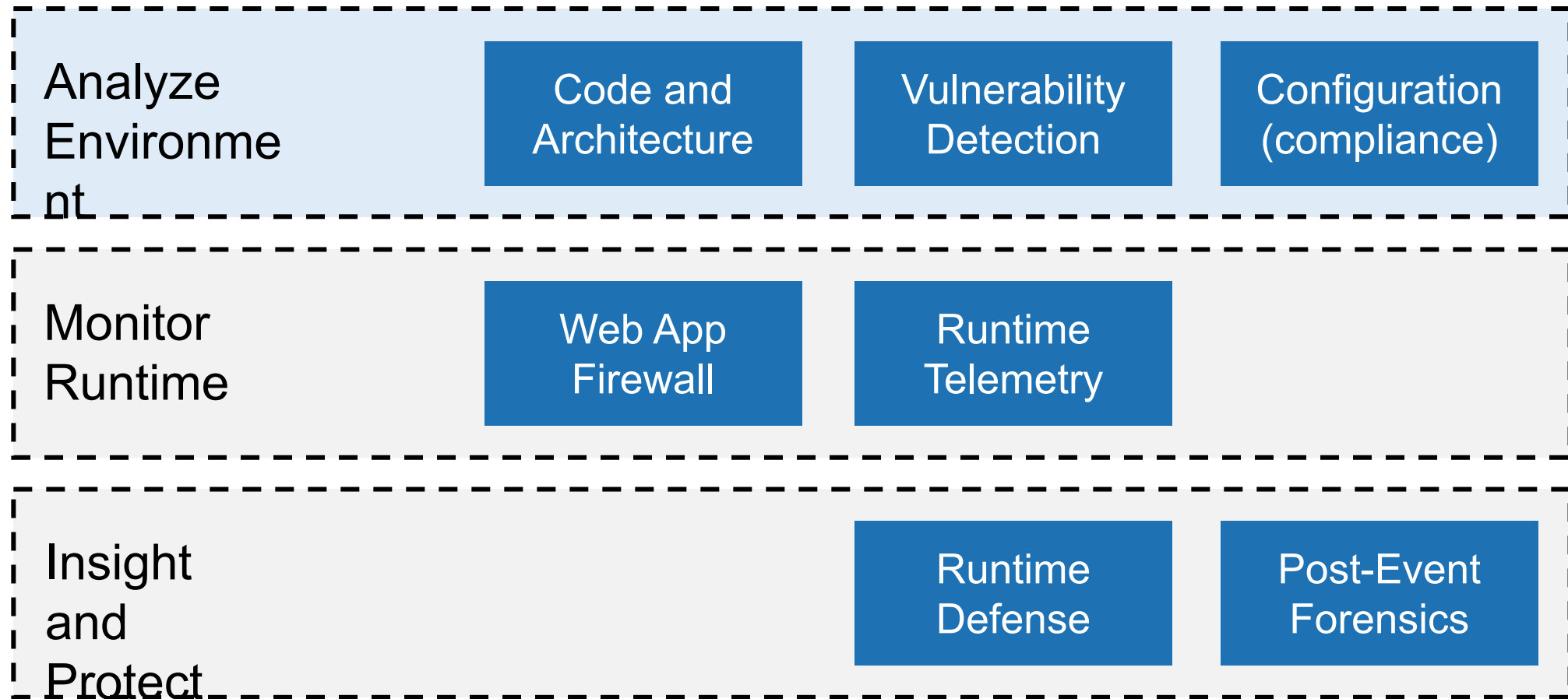


Deploy targeted defense when needed



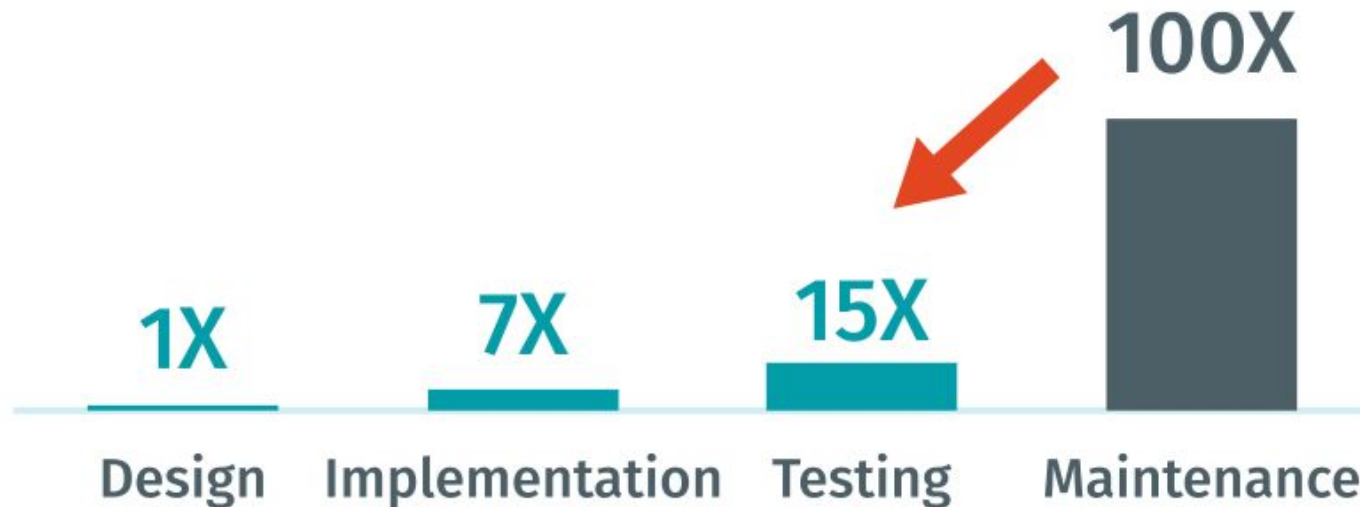
Tools and Processes for Application Security

A process-centric approach to security



A process-centric approach to security

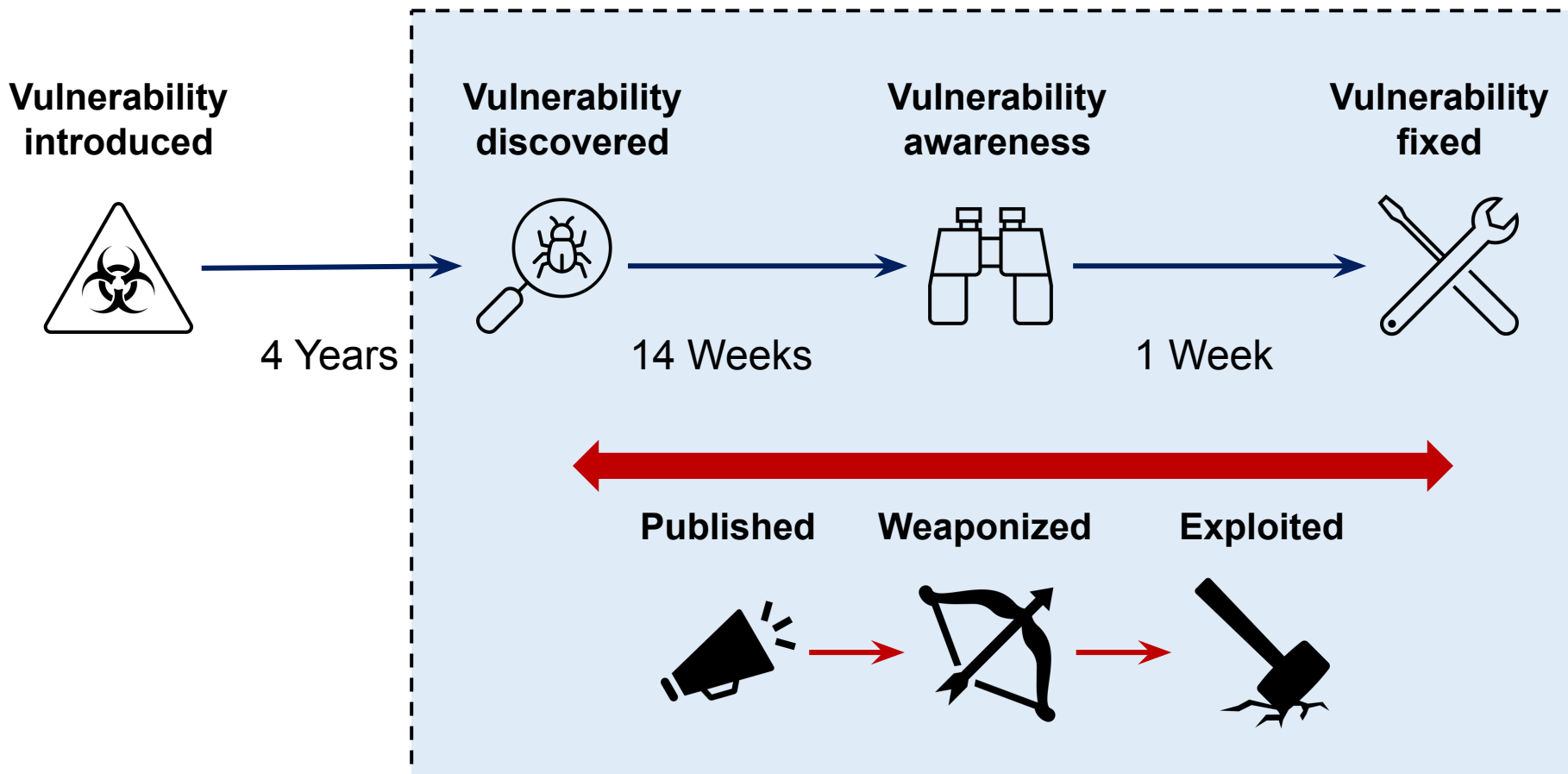
Vulnerability
Detection



Source: IBM Systems Sciences Institute

Fixing Defects Early in the SDLC Reduces
Costs

A process-centric approach to security



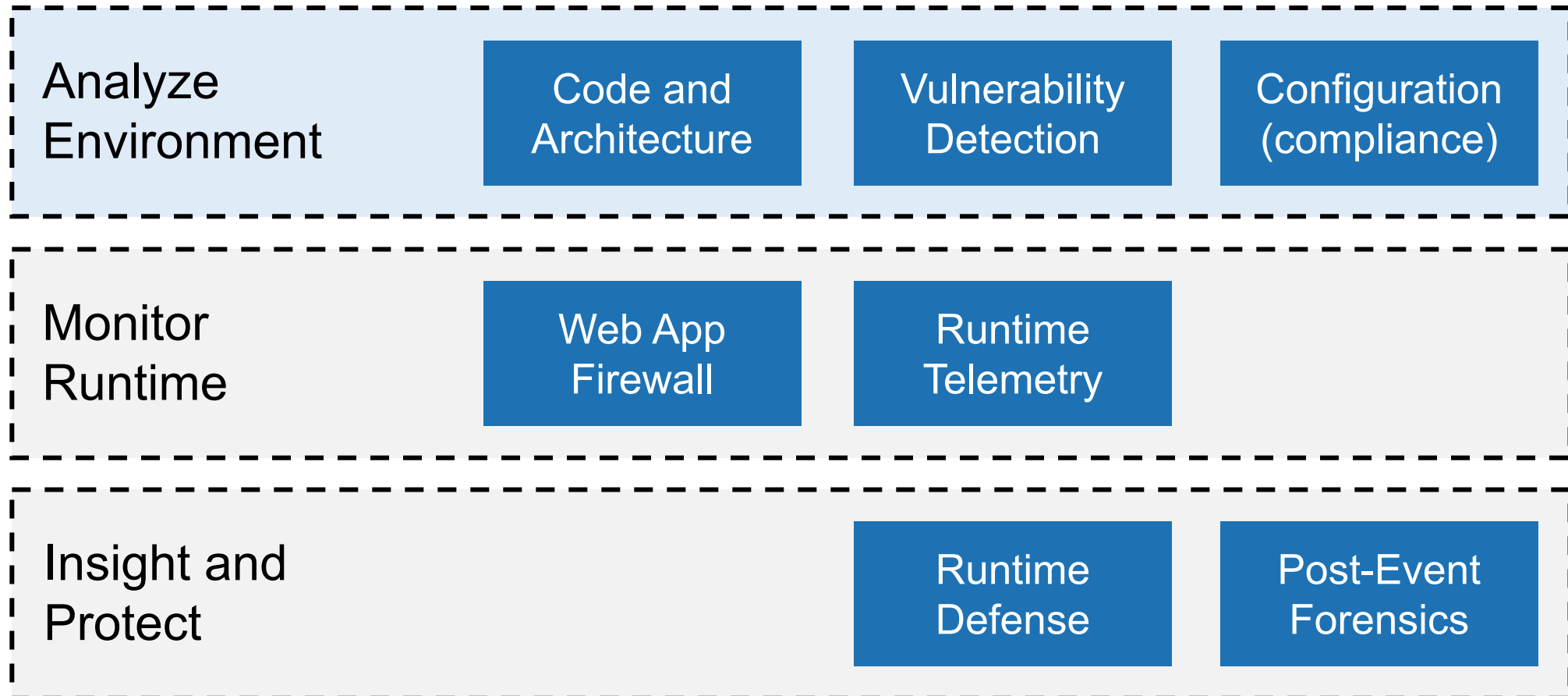
Vulnerability Detection

Sources:

GitHub 2020 Octoverse Report
On average, vulnerabilities in open-source software lie undetected for over 4 years. Once alerted, it takes 4.4 weeks to find a fix and 10 weeks to publish.

Sonatype 2020 State of the Software Supply Chain
51% of organizations take more than 1 week to remediate an OSS dependency vulnerability.

A process-centric approach to security



Spotlight on Misconfiguration

Configuration
(compliance)

- Identify weaknesses in attack surface
- Reduce potential for lateral spread

Collection of categories: CSPA, CSPM, CASB, Platform-specific, for example:

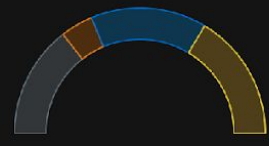
- OpenSCAP profiles
- KubeAudit

The screenshot shows a ZDNet article from October 10, 2019. The headline is "Imperva blames data breach on stolen AWS API key". The sub-headline reads: "Imperva said it accidentally exposed an internal server from where a hacker stole an AWS API key." The article is by Catalin Cimpanu for Zero Day. A "SPECIAL FEATURE" section is visible, titled "Special report: A winning strategy for cybersecurity (free PDF)". The article text includes: "Cyber-security firm Imperva published today a detailed post-mortem report of a security breach the company disclosed two months ago, in August." and "The company blamed the security breach on an Amazon Web Services (AWS) API key a hacker stole from an internal system that was left accessible from the internet." The article also mentions a "detailed bit convoluted, but we summarized the..." and "led to the Imperva breach in the list below:..." and "experienced a period of business growth in..." and "company began adopting cloud technologies to..." and "and infrastructure." and "to evaluate AWS' Relational Database Service..." and "user database." and "loaded a snapshot of its customer database to a test AWS RDS instance." and "ed incident, the company left an internal system accessible from the internet."

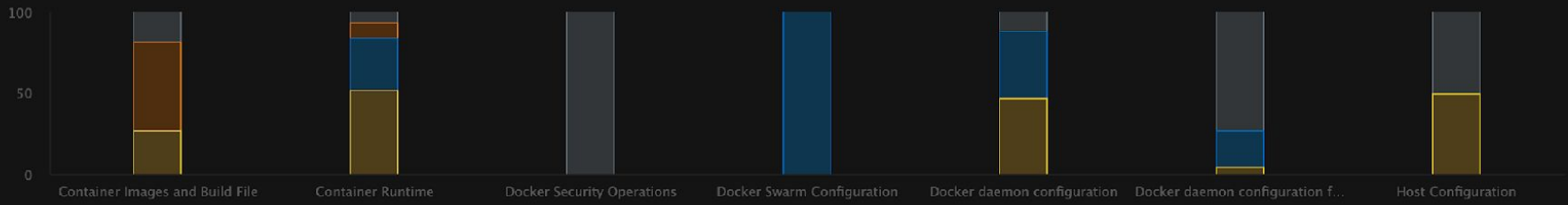
The screenshot shows a tweet from Linus Groh (@linusgroh) dated Jul 5. The tweet text is: ".@GitHubCopilot gave me a [staging.airbnb.com/api](\"https://staging.airbnb.com/api\") link with a key that *still works* (and stops working when changing it), so...". Below the text, it says "Airbnb haven't noticed they leaked that somewhere OR GitHub is feeding private code to Copilot OR somehow it's intentionally public." and "Either way: 🤔". The tweet has 9 replies, 69 retweets, and 221 likes.



gke-deepfence-demo-default-pool-75db9556-c8g9 (30% Compliant) - 5 days ago



info note pass warn



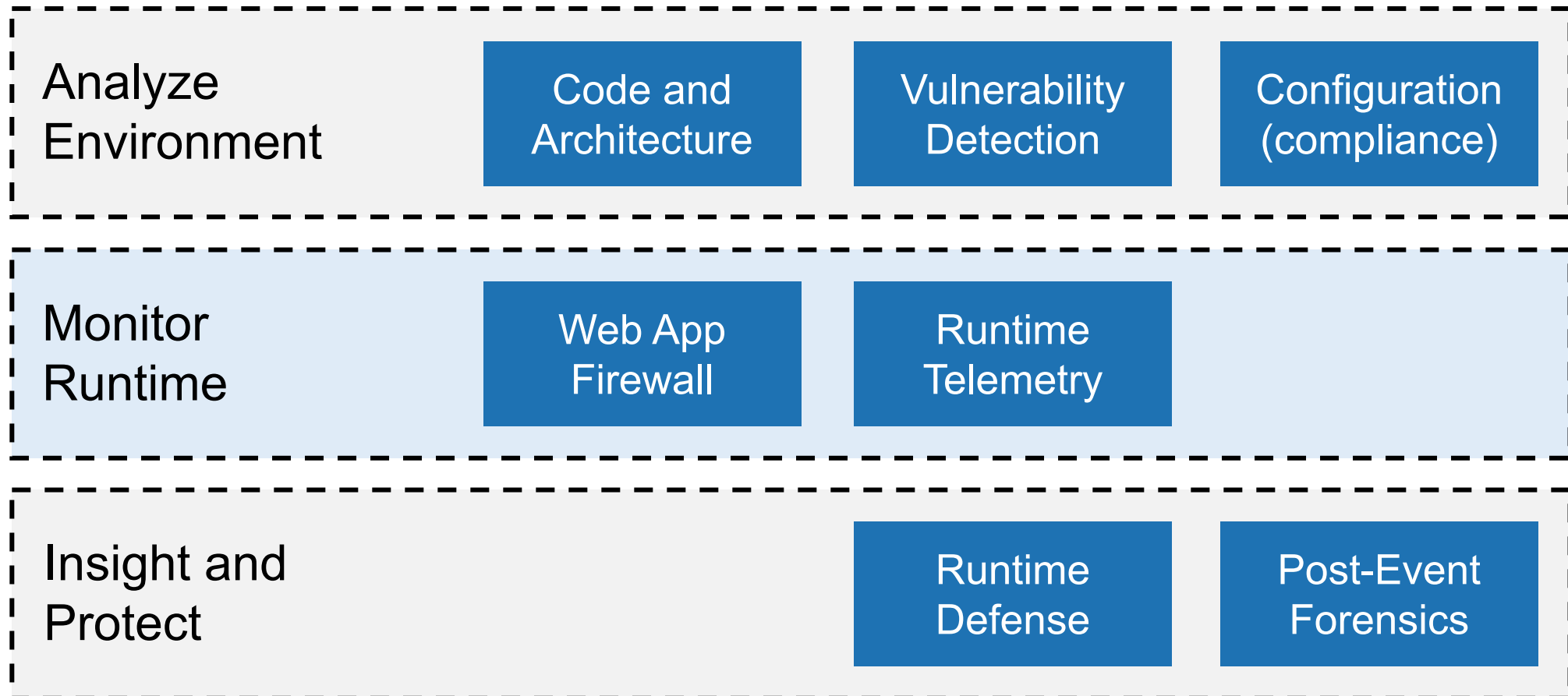
info note pass warn

Compliance Tests

Hide Masked

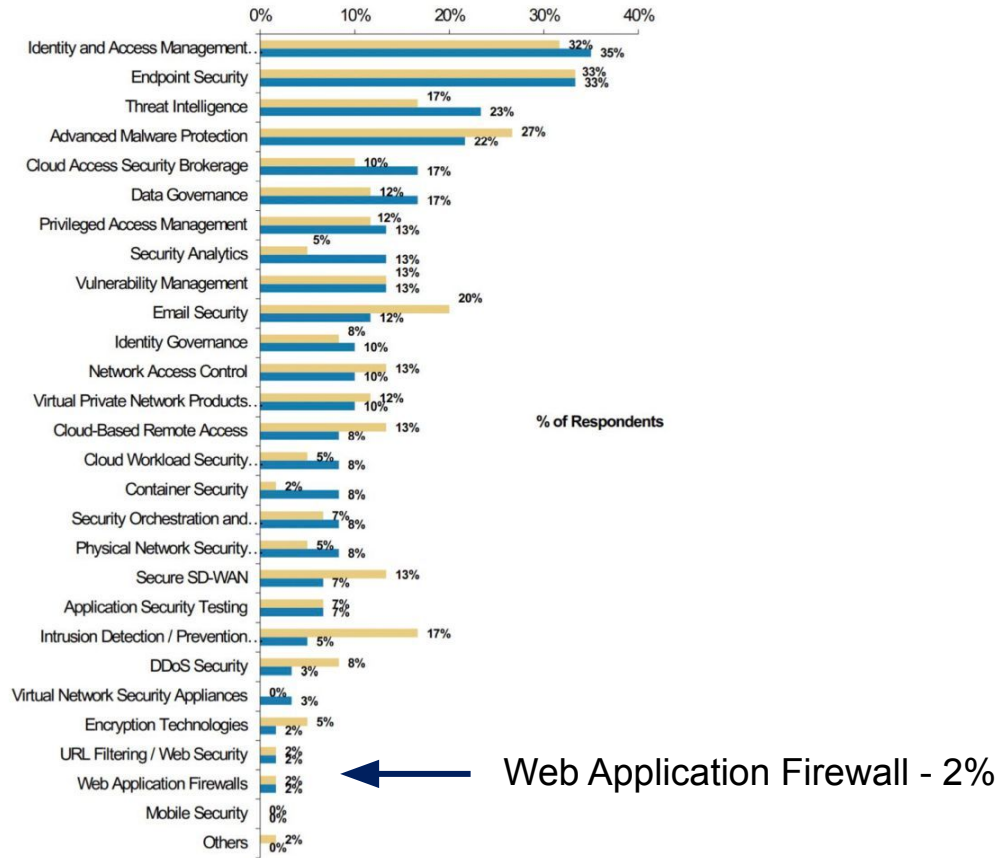
TIMESTAMP	STATUS	CATEGORY	DESCRIPTION	ACTION
Aug 26 2021 23:53:17	Pass	Docker Swarm Configuration	7.9 - Ensure that CA certificates are rotated as appropriate	<input type="checkbox"/>
Aug 26 2021 23:53:17	Pass	Docker Swarm Configuration	7.8 - Ensure that node certificates are rotated as appropriate	<input type="checkbox"/>
Aug 26 2021 23:53:17	Pass	Docker Swarm Configuration	7.7 - Ensure that the swarm manager auto-lock key is rotated periodically	<input type="checkbox"/>
Aug 26 2021 23:53:17	Pass	Docker Swarm Configuration	7.6 - Ensure that swarm manager is run in auto-lock mode	<input type="checkbox"/>
Aug 26 2021 23:53:17	Pass	Docker Swarm Configuration	7.5 - Ensure that Docker's secret management commands are used for managing secrets in a swarm cluster	<input type="checkbox"/>
Aug 26 2021 23:53:17	Pass	Docker Swarm Configuration	7.4 - Ensure that all Docker swarm overlay networks are encrypted	<input type="checkbox"/>
Aug 26 2021 23:53:17	Pass	Docker Swarm Configuration	7.3 - Ensure that swarm services are bound to a specific host interface	<input type="checkbox"/>
Aug 26 2021 23:53:17	Pass	Docker Swarm Configuration	7.2 - Ensure that the minimum number of manager nodes have been created in a swarm	<input type="checkbox"/>
Aug 26 2021 23:53:17	Pass	Docker Swarm Configuration	7.10 - Ensure that management plane traffic is separated from data plane traffic	<input type="checkbox"/>
Aug 26 2021 23:53:17	Pass	Docker Swarm Configuration	7.1 - Ensure swarm mode is not Enabled, if not needed	<input type="checkbox"/>
Aug 26 2021 23:53:17	Info	Docker Security Operations	6.2 - Ensure that container sprawl is avoided	<input type="checkbox"/>
Aug 26 2021 23:53:17	Info	Docker Security Operations	6.1 - Ensure that image sprawl is avoided	<input type="checkbox"/>
Aug 26 2021 23:53:17	Warn	Container Runtime	5.9 - Ensure the host's network namespace is not shared	<input type="checkbox"/>
Aug 26 2021 23:53:17	Note	Container Runtime	5.8 - Ensure that only needed ports are open on the container	<input type="checkbox"/>

A process-centric approach to security



WAF spotlight

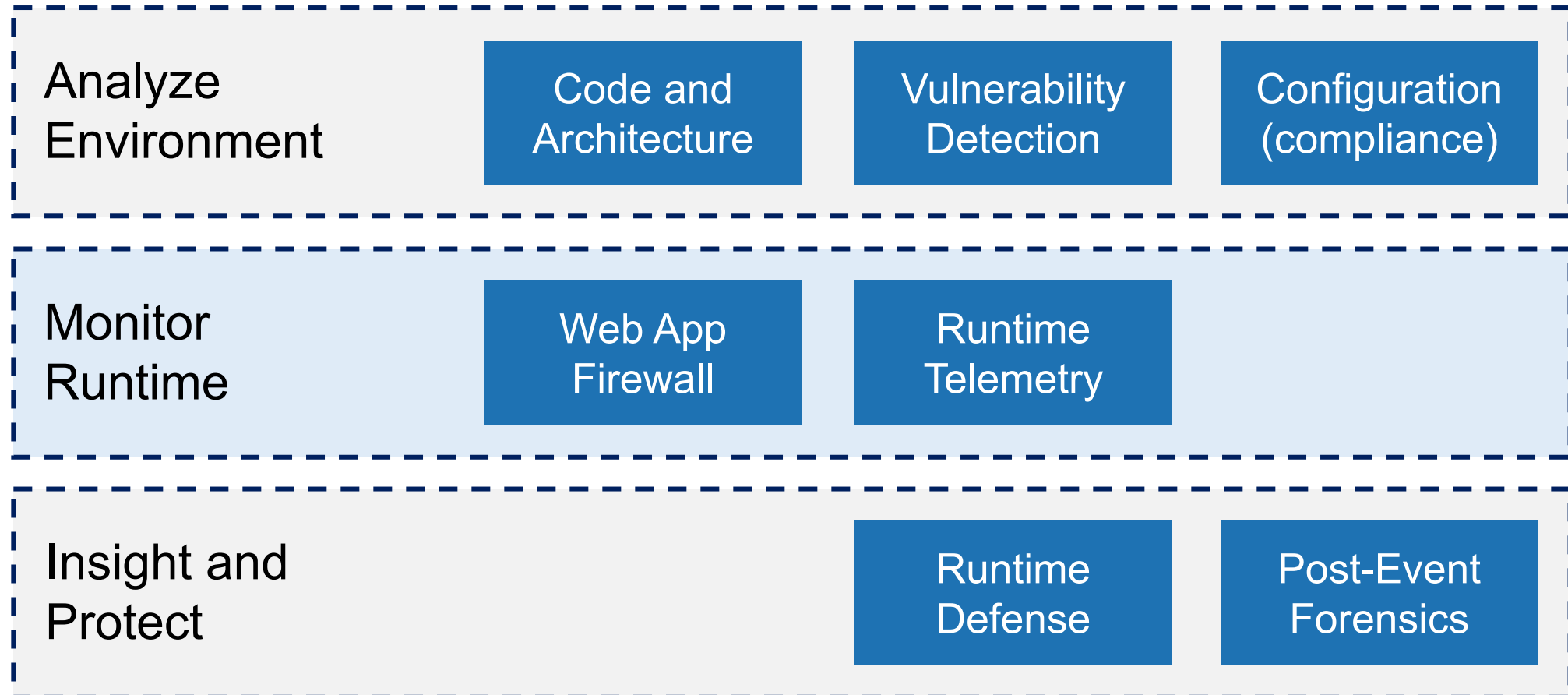
Web App Firewall



WAF mentality == Castle mentality

Top 3 Priorities for Security Spending (survey of 60 Chief Security Officers)

A process-centric approach to security



Runtime Telemetry spotlight

Runtime
Telemetry

Not a traditional WAF

- Broader reach and Lower Performance Impact
- Out-of-band rather than In-band

Two key telemetry types:

- On-Host: File and Process Telemetry
- Off-Host: Network Telemetry

On-Host sensors

File permissions changed
Process started
Tracing Event
Process exited

Off-Host (Network) sensors

Known attack attempts e.g. Apache Struts
Exfiltration
Command-and-Control
Lateral Spread

Alerts

4 Hosts 1 Clusters 4 Pods

CPU: 18.92% Memory: 56.29%

Vulnerability database updated 7.6 hours ago

Integrations are okay

SUMMARY THREAT MAP DISTRIBUTIONS **ATTACK GEO MAP**



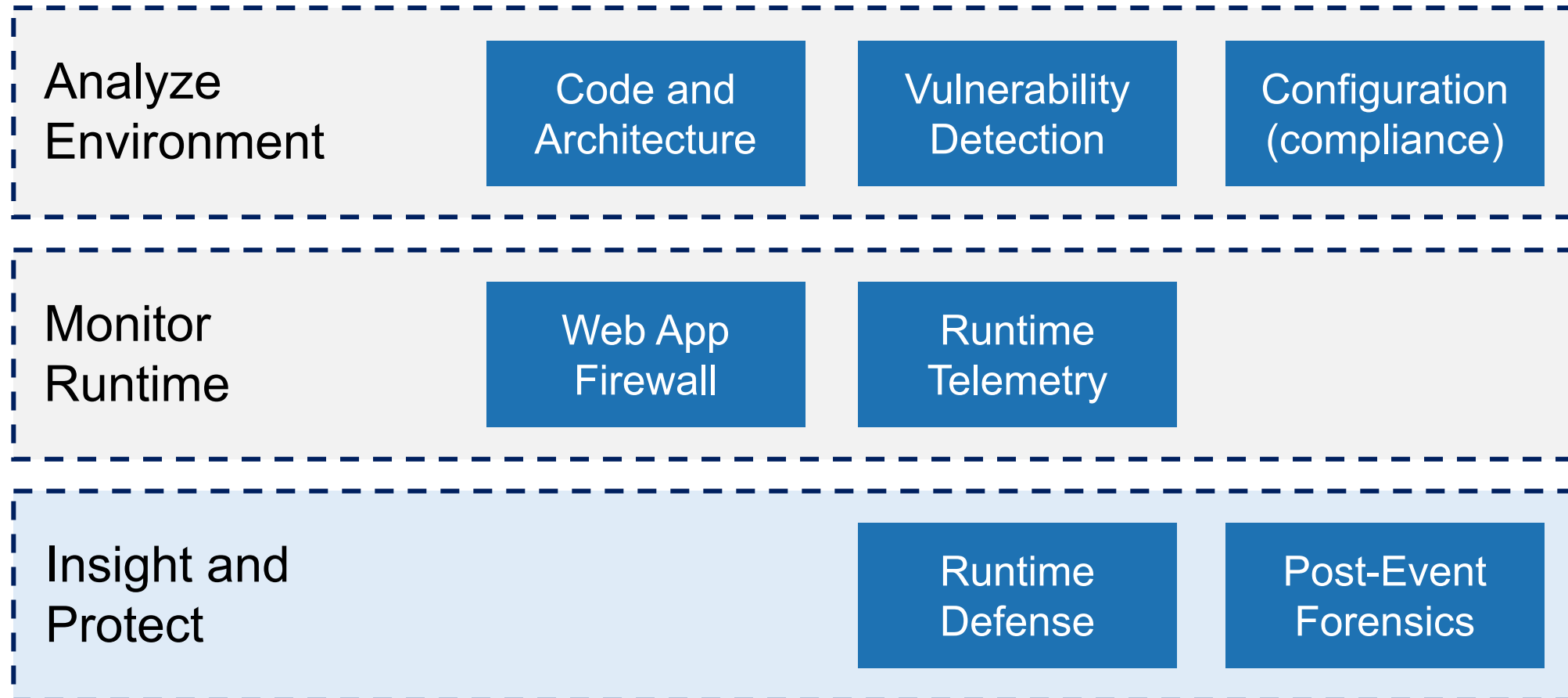
Show 10 Entries

Hostname Kubernetes Cluster Name Masked (1)

TIME	SEVERITY	INTENT	CLASSTYPE	HOST	SUMMARY	ACTION	
Aug 27 2021 0:20:51	Medium	Exploitation	Application policies	gke-deepfence-demo-default-po...	POLICY curl User-Agent Outbound -- Attempted Information Leak	<input type="checkbox"/>	
Aug 27 2021 0:20:51	Medium	Exploitation	Application policies	gke-deepfence-demo-default-po...	POLICY curl User-Agent Outbound -- Attempted Information Leak	<input type="checkbox"/>	
Aug 27 2021 0:20:28	High	Exploitation	Process Anomaly	gke-deepfence-demo-default-po...	Core dumped for pid=bash -i:35589 owned by root	<input type="checkbox"/>	
Aug 27 2021 0:20:13	High	Exploitation	Process Anomaly	gke-deepfence-demo-default-po...	Suspicious tracing event process strace ls -lah:35520 trying to ptrace s...	<input type="checkbox"/>	
Aug 27 2021 0:20:13	High	Exploitation	Process Anomaly	gke-deepfence-demo-default-po...	Suspicious tracing event process strace ls -lah:35520 trying to ptrace s...	<input type="checkbox"/>	
Aug 27 2021 0:19:58	Low	Exploitation	File Anomaly	gke-deepfence-demo-default-po...	File modify operation on file /tmp/shell.bin which has executable code	<input type="checkbox"/>	
Aug 27 2021 0:19:57	High	Weaponization, Payload Delivery...	Web specific apps	35.247.28.157	WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injecti...	<input type="checkbox"/>	
Aug 27 2021 0:19:57	High	Weaponization, Payload Delivery...	Web specific apps	35.247.28.157	WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injecti...	<input type="checkbox"/>	
Aug 27 2021 0:19:57	High	Weaponization, Payload Delivery...	Web specific apps	35.247.28.157	WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injecti...	<input type="checkbox"/>	

- Topology
- Alerts
- Vulnerabilities
- Registries
- Compliance
- Protection Policies
- Workload Firewall
- Correlation
- Integrations
- Settings

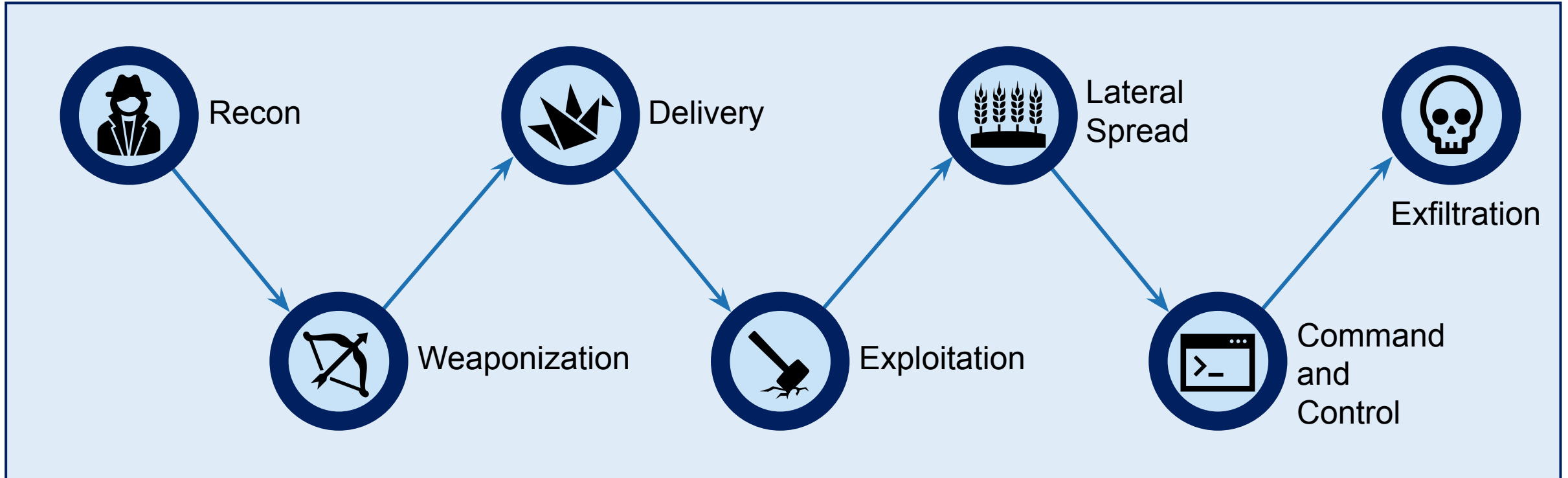
A process-centric approach to security



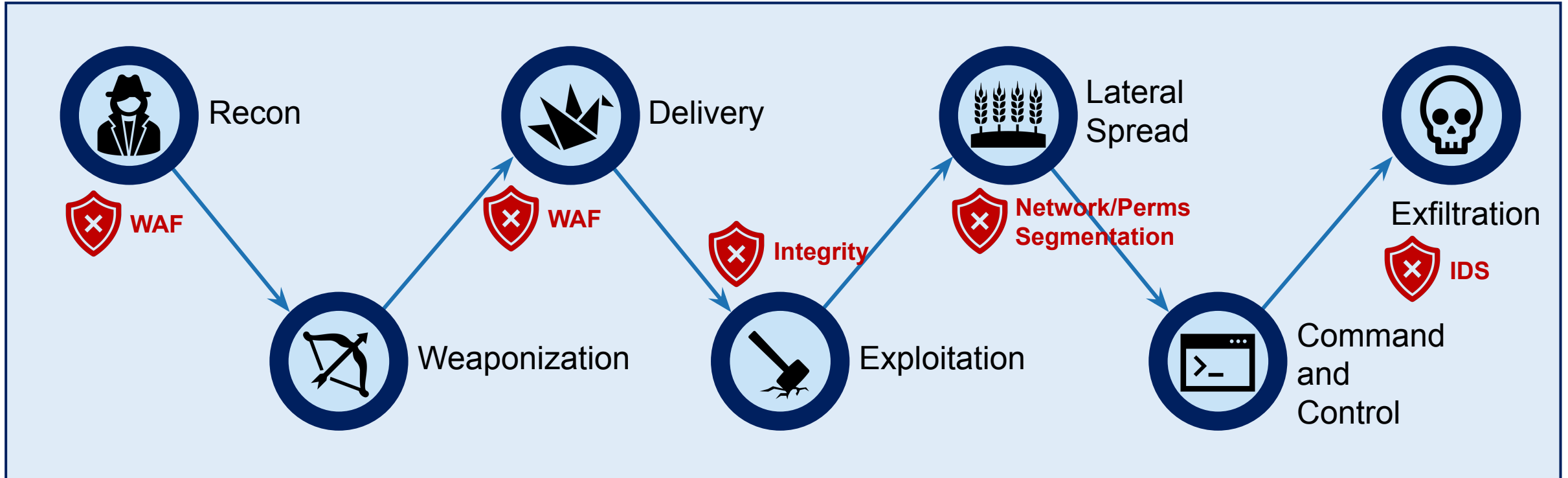


Movie Script for an Attack

Anatomy of a Heist: Cyber Kill Chain



Anatomy of a Heist: Cyber Kill Chain



Next Generation – MITRE ATT&CK framework

MITRE | ATT&CK[®]

Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute Search Q

layout: side 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	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Data from Information Repositories (2)	Data from Local System	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Trusted Relationship	User Execution (3)	Software Deployment Tools	Create or Modify System Process (4)	Event Triggered Execution (15)	Execution Guardrails (1)	Modify Authentication Process (4)	Domain Trust Discovery	Data from Network Shared Drive	Ingress Tool Transfer	Multi-Stage Channels	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)	Valid Accounts (4)	Windows Management Instrumentation	System Services (2)	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Network Sniffing	File and Directory Permissions Modification (2)	Data from Removable Media	Data from Network Shared Drive	Non-Application Layer Protocol	Transfer Data to Cloud Account	Network Denial of Service (2)
Search Victim-Owned Websites			User Execution (3)	External Remote Services	Hijack Execution Flow (11)	Hide Artifacts (7)	OS Credential Dumping (8)	Hide Artifacts (7)	Data from Removable Media	Network Service Scanning	Non-Standard Port	Resource Hijacking	Service Stop
			Windows Management Instrumentation	Hijack Execution Flow (11)	Process Injection (11)	Hijack Execution Flow (11)	Steal Application Access Token	Impair Defenses (7)	Data Staged (2)	Network Sniffing	Protocol Tunneling	System Shutdown/Reboot	System Shutdown/Reboot
				Implant Internal Image	Scheduled Task/Job (7)	Indicator Removal on Host (6)	Steal or Forge Kerberos Tickets (4)	Impair Defenses (7)	Email Collection (3)	Password Policy Discovery	Proxy (4)		
				Modify Authentication Process (4)	Valid Accounts (4)	Indirect Command Execution	Steal Web Session Cookie	Impair Defenses (7)	Input Capture (4)	Peripheral Device Discovery	Remote Access Software		
				Office Application Startup (6)		Masquerading (6)	Two-Factor Authentication Interception	Indicator Removal on Host (6)	Man in the Browser	Permission Groups Discovery (3)	Traffic Signaling (1)		
				Pre-OS Boot (5)		Modify Authentication Process (4)	Unsecured Credentials (7)	Indirect Command Execution	Man-in-the-Middle (2)	Process Discovery	Web Service (3)		
				Scheduled Task/Job (7)		Modify Cloud Compute Infrastructure (4)		Masquerading (6)	Screen Capture	Query Registry			
				Server Software Component (3)		Modify Registry		Modify Authentication Process (4)	Video Capture	Remote System Discovery			
				Traffic Signaling (1)		Modify System Image (2)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)			
				Valid Accounts (4)		Network Boundary Bridging (1)		Modify Registry		System Information Discovery			
						Obfuscated Files or Information (5)		Network Boundary Bridging (1)		System Location Discovery			
						Pre-OS Boot (5)		Obfuscated Files or Information (5)		System Network Configuration Discovery (1)			
								Pre-OS Boot (5)		System Network Connections Discovery			



Recon



Weaponization



Delivery



Exploitation



Lateral Spread



Command and Control



Exfiltration

GROUPS

[Overview](#)[admin@338](#)[Ajax Security Team](#)[APT-C-36](#)[APT1](#)[APT12](#)[APT16](#)[APT17](#)[APT18](#)[APT19](#)[APT28](#)[APT29](#)[APT3](#)[APT30](#)[APT32](#)[APT33](#)[APT37](#)[APT38](#)[APT39](#)[APT41](#)[Axiom](#)[BlackOasis](#)[BlackTech](#)[Blue Mockingbird](#)[Bouncing Golf](#)[Home](#) > [Groups](#) > [APT29](#)

APT29

APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).^{[1][2]} They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. **APT29** reportedly compromised the Democratic National Committee starting in the summer of 2015.^{[3][4][5][6]}

In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR; public statements included citations to **APT29**, Cozy Bear, and The Dukes.^{[7][8]} Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, and Dark Halo.^{[9][10][11][12]}

ID: G0016

① **Associated Groups:** Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke

Contributors: Matt Brenton, Zurich Insurance Group; Katie Nickels, Red Canary

Version: 2.0

Created: 31 May 2017

Last Modified: 30 April 2021

[Version Permalink](#)

Associated Group Descriptions

Name	Description
Dark Halo	[12]
StellarParticle	[11]
NOBELIUM	[10]
UNC2452	[9]
YTTRIUM	[13]
The Dukes	[3][14][15]
Cozy Bear	[5][14][15]
CozyDuke	[5]

Techniques Used

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
---------------------------------	--------------------------------------	--------------------------------	----------------------------	------------------------------	---------------------------------------	----------------------------------	------------------------------------	----------------------------	----------------------------------	-----------------------------	--------------------------------------	------------------------------	-------------------------

Active Scanning (1/2)	Acquire Infrastructure (2/6)	Drive-by Compromise	Command and Scripting Interpreter (5/3)	Account Manipulation (2/4)	Abuse Elevation Control Mechanism (1/4)	Abuse Elevation Control Mechanism (1/4)	Brute Force (3/4)	Account Discovery (1/4)	Exploitation of Remote Services	Archive Collected Data (1/3)	Application Layer Protocol (3/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (1/5)	Access Token Manipulation (1/5)	Credentials from Password Stores (1/5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (2/3)	Compromise Infrastructure (2/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (2/14)	Boot or Logon Autostart Execution (2/14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (1/2)	Exfiltration Over Alternative Protocol (3/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (2/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (1/5)	Boot or Logon Initialization Scripts (1/5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (1/2)	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (2/2)	Phishing (3/3)	Inter-Process Communication (1/2)	Browser Extensions	Create or Modify System Process (1/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2/2)	Cloud Service Dashboard	Remote Services (4/6)	Data from Configuration Repository (2/2)	Data Obfuscation (2/3)	Dynamic Resolution (1/3)	Defacement (0/2)
Phishing for Information (1/3)	Obtain Capabilities (1/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (1/2)	Deploy Container	Input Capture (1/4)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (1/2)	Encrypted Channel (2/2)	Exfiltration Over Other Network Medium (0/1)	Disk Wipe (1/2)
Search Closed Sources (0/2)	Stage Capabilities (2/5)	Supply Chain Compromise (2/3)	Scheduled Task/Job (2/7)	Create Account (1/3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (2/2)	Container and Resource Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Physical Medium (0/1)	Endpoint Denial of Service (4/4)
Search Open Technical Databases (0/5)		Trusted Relationship	Shared Modules	Create or Modify System Process (1/4)	Event Triggered Execution (3/15)	Domain Policy Modification (1/2)	Modify Authentication Process (0/4)	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Exfiltration Over Web Service (3/3)	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (3/4)	Software Deployment Tools	Event Triggered Execution (3/15)	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Network Sniffing	Network Service Scanning	Use Alternate Authentication Material (4/4)	Data from Removable Media	Multi-Stage Channels	Inhibit System Recovery	
Search Victim-Owned Websites			System Services (1/2)	External Remote Services	File and Directory Permissions Modification (1/2)	Hide Artifacts (3/7)	OS Credential Dumping (4/8)	Network Share Discovery		Data Staged (2/2)	Non-Application Layer Protocol	Exfiltration Over Physical Medium (0/1)	Network Denial of Service (2/2)
			User Execution (2/3)	Hijack Execution Flow (1/11)	Hijack Execution Flow (1/11)	Hijack Execution Flow (1/11)	Steal Application Access Token	Network Sniffing		Email Collection (2/3)	Non-Standard Port	Scheduled Transfer	Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Impair Defenses (3/7)	Impair Defenses (3/7)	Steal or Forge Kerberos Tickets (1/4)	Password Policy Discovery		Input Capture (1/4)	Protocol Tunneling	Transfer Data to Cloud Account	Service Stop
				Modify Authentication Process (0/4)	Indicator Removal on Host (3/6)	Indicator Removal on Host (3/6)	Steal Web Session Cookie	Peripheral Device Discovery		Man in the Browser	Proxy (4/4)		System Shutdown/Reboot
				Office Application Startup (1/5)	Indirect Command Execution	Indirect Command Execution	Two-Factor Authentication Interception	Permission Groups Discovery (1/3)		Man-in-the-Middle (2/2)	Remote Access Software		
				Pre-OS Boot (2/5)	Masquerading (4/8)	Masquerading (4/8)	Unsecured Credentials (5/7)	Process Discovery		Screen Capture	Traffic Signaling (1/1)		
				Scheduled Task/Job (2/7)	Modify Authentication Process (0/4)	Modify Authentication Process (0/4)		Query Registry		Video Capture	Web Service (1/3)		
				Server Software Component (1/3)	Modify Cloud Compute Infrastructure (0/4)	Modify Cloud Compute Infrastructure (0/4)		Remote System Discovery					
				Traffic Signaling (1/1)	Modify Registry	Modify Registry		Software Discovery (0/1)					
				Valid Accounts (3/4)	Modify System Image (0/2)	Modify System Image (0/2)		System Information Discovery					
					Network Boundary Bridging (1/1)	Network Boundary Bridging (1/1)		System Location Discovery					
					Obfuscated Files or Information (4/5)	Obfuscated Files or Information (4/5)		System Network Configuration Discovery (1/1)					

Getting Started

You want to get started using ATT&CK, but where do you begin? Regardless of what you want to accomplish, it's important to understand what ATT&CK is and why MITRE created it.

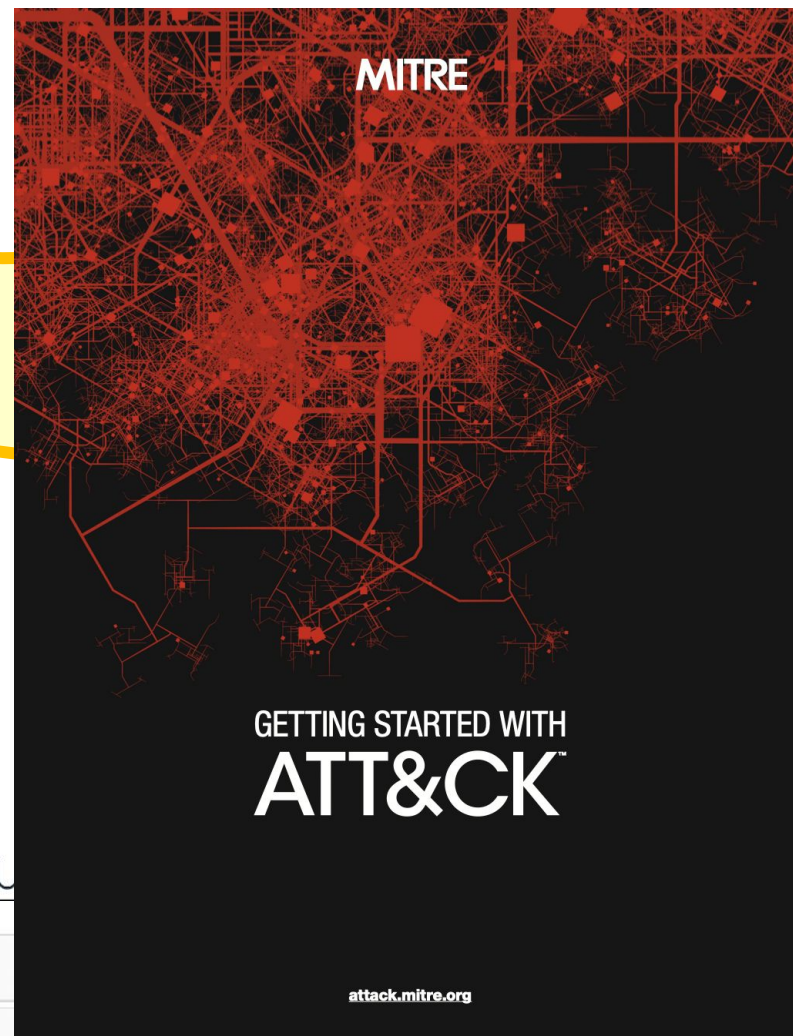
- [ATT&CK 101 Blog Post](#)
A quick overview of key points to know about ATT&CK.
- [Getting Started with ATT&CK Blog Series](#)
Provides an overview of how to use ATT&CK at different levels of sophistication for four use cases: [Threat Intelligence](#), [Detection and Analytics](#), [Adversary Emulation and Red Teaming](#), and [Assessments and Engineering](#).
- [Getting Started with ATT&CK eBook](#)
Pulls together the content from our four Getting Started blog posts on [Threat Intelligence](#), [Detection and Analytics](#), [Adversary Emulation and Red Teaming](#), and [Assessments and Engineering](#) onto a single convenient package.
- [Philosophy Paper](#)
An in-depth look at why MITRE created ATT&CK, how we update and maintain it, and what the community commonly uses it for.
- [Sp4rkcon Presentation: Putting MITRE ATT&CK™ into Action with What You Have, Where You Are](#)
Presents an overview of ATT&CK as well as ideas for how you can put it into action for four use cases. [Slides are also available](#).
- [Finding Cyber Threats with ATT&CK-Based Analytics](#)
Presents a methodology for using ATT&CK to build, test, and refine behavioral-based analytic detection capabilities.

Common U

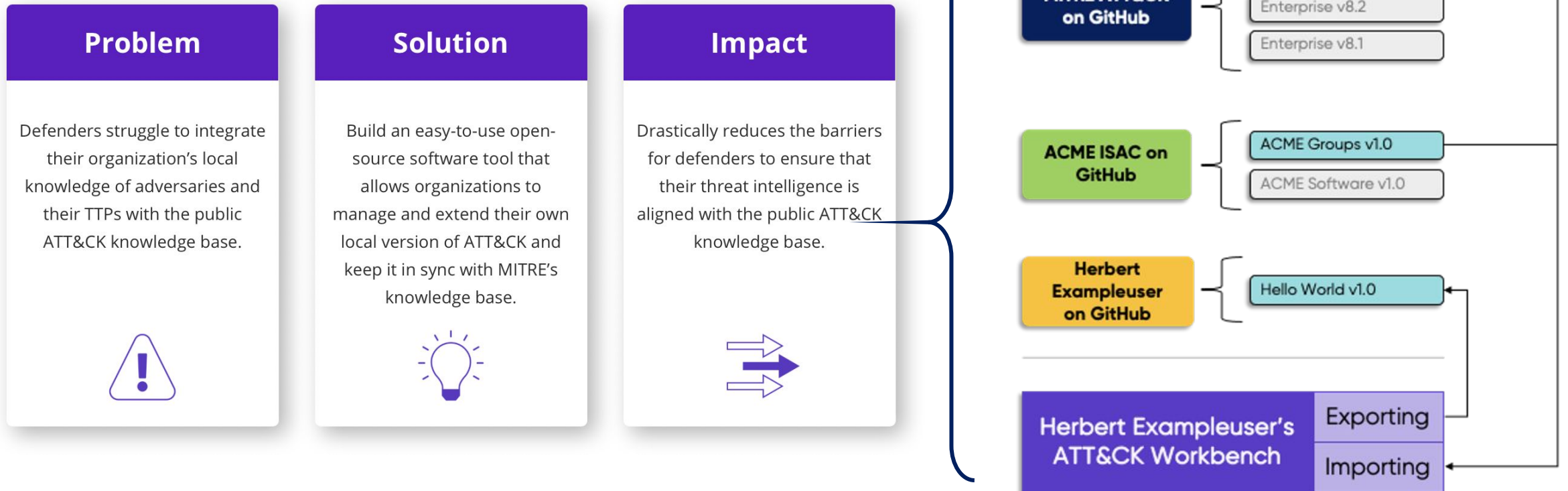
Detections and Analytics

Threat Intelligence

Adversary Emulation and Red Teaming



MITRE ATT&CK Workbench



How can you use the MITRE ATT&CK matrix?

- **Map to your scope** e.g. cloud, K8s, Enterprise
- **Assess Coverage** using Navigator (mitigations)
- **Prioritize Gaps** (Navigator, Groups and Threats)
- **Gather analytics** and baseline
- **Tune detection**
- **Actively attempt to bypass** (purple team testing)

The 5 quickest wins:

1. Vulnerability Scanning in Production
2. Process and shell/ssh monitoring
3. File Integrity monitoring
4. Authentication logs
5. Packet Capture and Analysis

Correlate and Learn



ATT&CK and DEF3ND



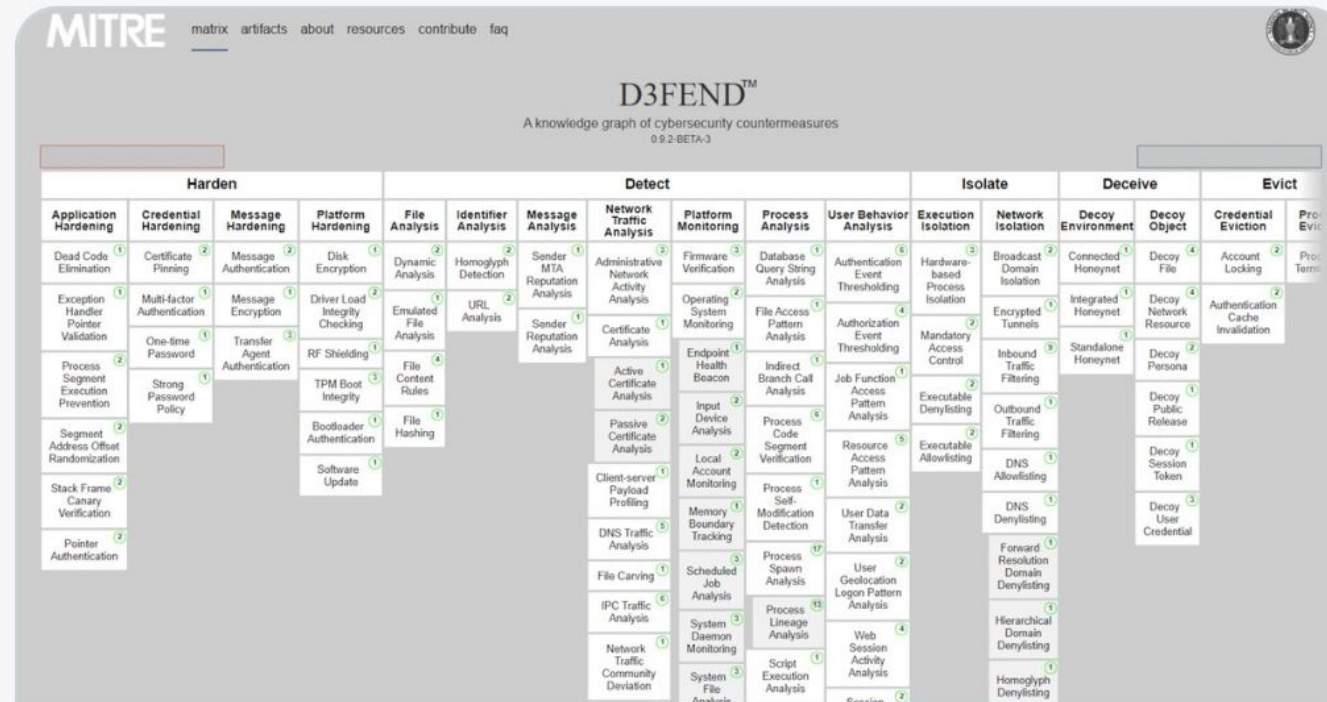
Brian in Pittsburgh @arekfurt · 22 Jun



Sweet!

"The D3FEND technical knowledge base of defensive countermeasures for common offensive techniques is complementary to MITRE's ATT&CK, a knowledge base of cyber adversary behavior."

In other words, see what stops what.

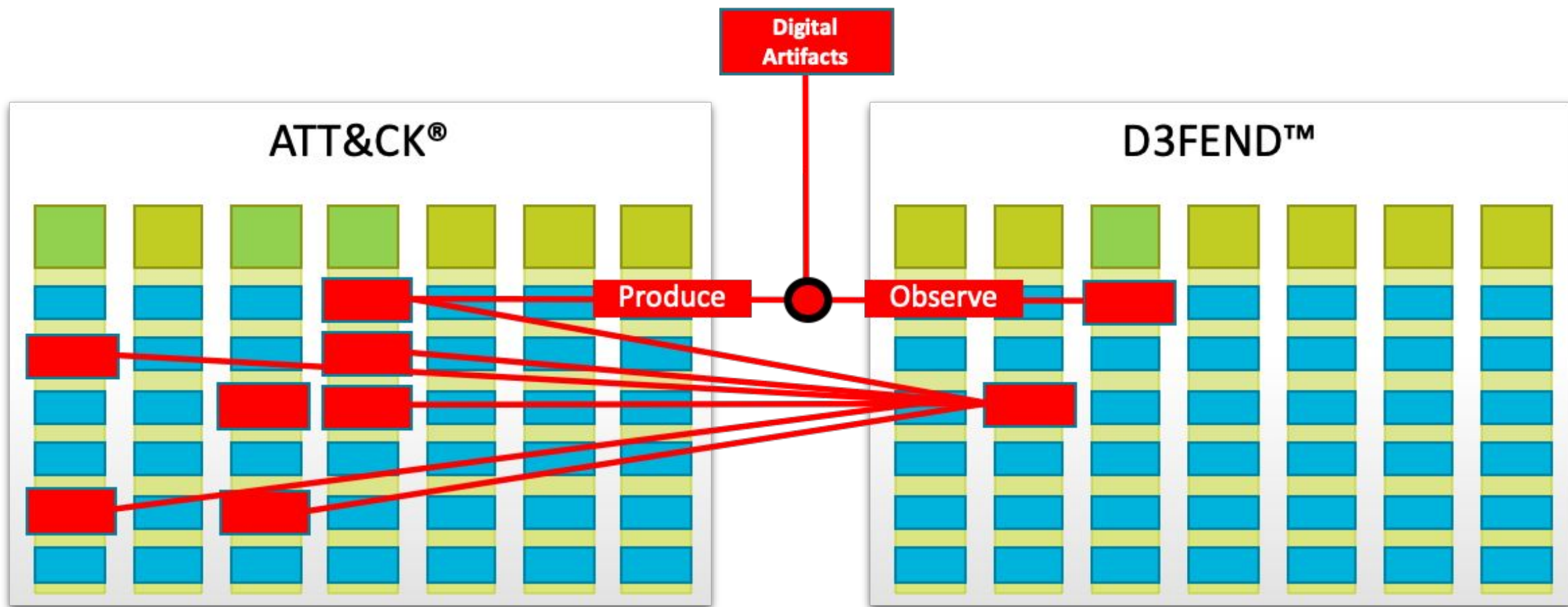


NSA Funds Development, Release of D3FEND

D3FEND, a framework for cybersecurity professionals to tailor defenses against specific cyber threats is now available through ...

nsa.gov

MITRE D3FEND

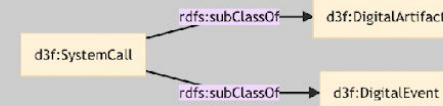


Artifact Details: System Call

Object Properties

name System Call
identifier d3f:SystemCall
definition A system call is the programmatic way in which a computer program requests a service from the kernel of the operating system it is executed on. This may include hardware-related services (for example, accessing a hard disk drive), creation and execution of new processes, and communication with integral kernel services such as process scheduling. System calls provide an essential interface between a process and the operating system.
defined by http://dbpedia.org/page/System_call

Parent Classes



Inferred Relationships

Note: the inference is not fully transitive in this release. This page is experimental and will change significantly in future releases.

Sub Classes:

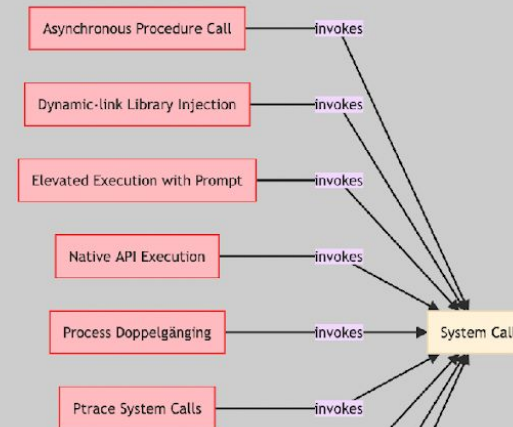
filtered

- System Call
- Create Process
- Get System Time
- Move File

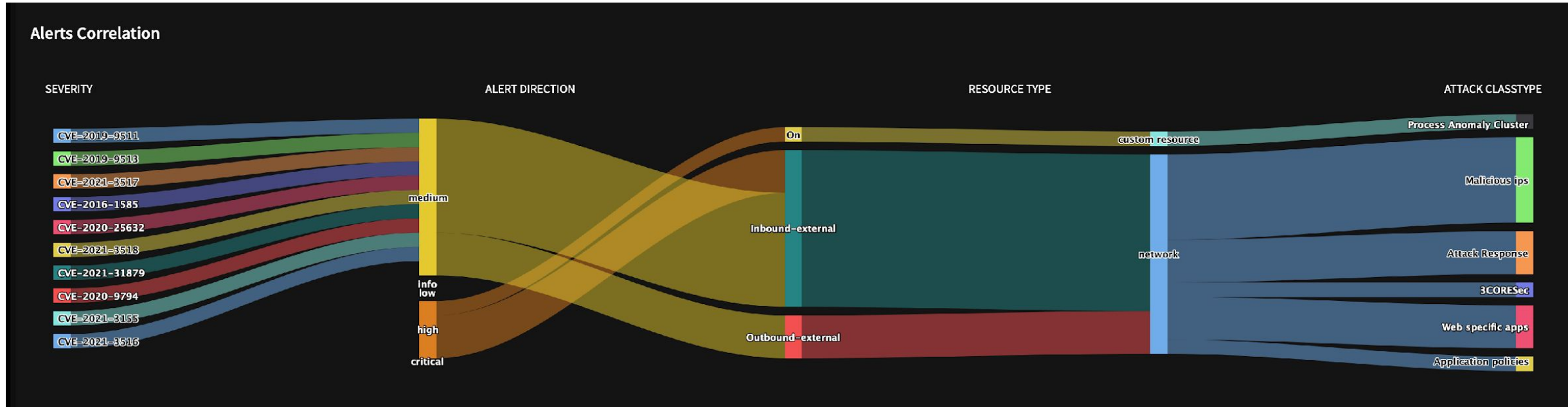
Related Countermeasure Techniques:





Related Offensive Techniques:

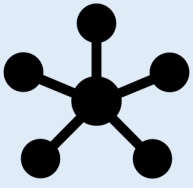


Deepfence Attack Correlation



 **Map the Attack Surface**
Topology and vulnerabilities

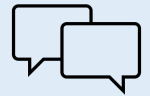
 **Monitor Application Behavior**
Monitor for traffic and anomalies

 **Correlate Signals**
Identify attack risks
Automated and guided remediation

The future brings...



A sophisticated categorization of cybersecurity concepts



A common approach and language for SecOps and DevOps



Automated tools to prioritize risks, assess coverage, test measures



Common frameworks to build higher-quality solutions



The job of a security professional is
never done

You are the star of your movie

- Production Platforms are a vibrant, growing city
- Complex, fluid, open, with many valuable assets
- Sophisticated attackers know to infiltrate and spread
- Deepfence empowers you to secure this 'city' of apps



Discover and maintain the city map



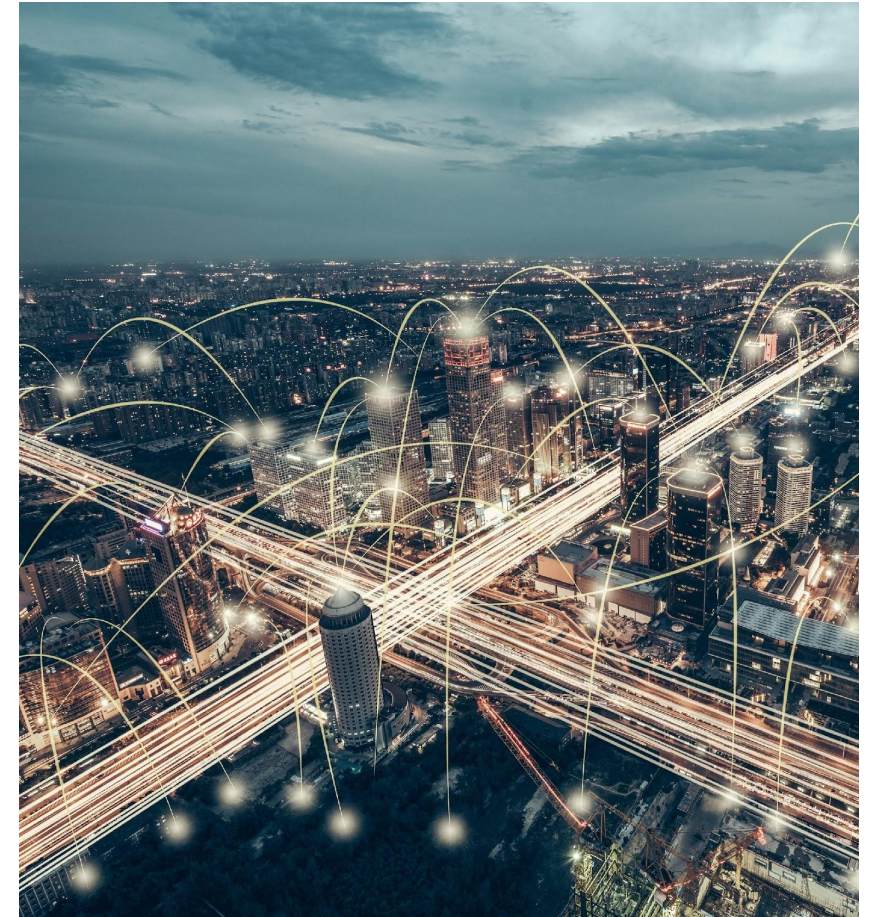
Annotate it with potential security vulnerabilities



Observe activity and alert to suspicious behavior



Deploy targeted defense when needed





deepfence

Appendix – Useful Resources

- Who is exposing services they should not (use for fun, not profit):
 - <https://www.exploit-db.com/google-hacking-database>
 - Search for (e.g.) [Network or Vulnerability Data](#) and submit the search to Google
- OpenSCAP: <https://www.open-scap.org> compliance profiles
- [MITRE ATT&CK framework](#)
 - [MITRE ATT&CK Navigator](#) and [Overview](#)
- [MITRE D3FEND](#)
- [Deepfence.io](#) and [live demo](#)
- Me ([Owen Garrett](#))