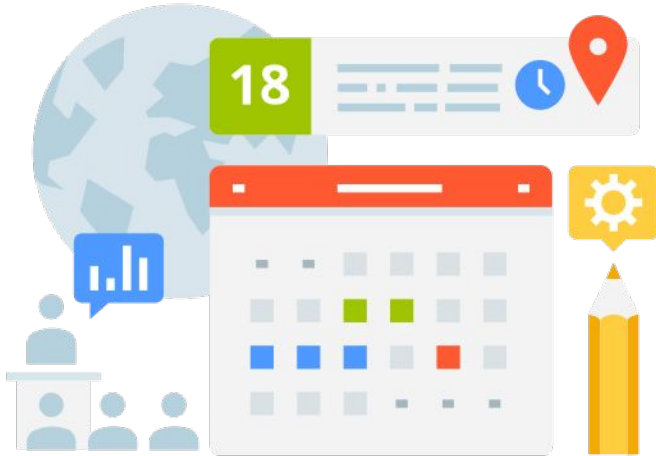




BLUE
TEAM
→ SECURITY INCIDENT RESPONSE

Incident Response
Google Cloud Platform

Agenda



- Hey - Pixies 03:31
- The Mission - Puscifer 03:43
- Panic Attack - Dream Theater 07:16
- Land of Confusion - Genesis 04:46
- Know Your Enemy - Rage Against The Machine 04:55
- Invincible - Tool 12:44
- On the Run - Pink Floyd 03:36

```
(dvirus@gondor)-[~]
```

```
$ whoami
```

Daniel Rodriguez

Security Consultant

Incident Response / Digital Forensics

Twitter @dvirus

Website: <https://dvirus.training/>

The Mission





The organization has your first assignment:

From: The Boss

To: Cloud Security Engineer

Sent: 2022-11-04T17:20

Your mission is to detect an attacker who is attacking our systems. Several sensitive files are being leaked from our GCP buckets.

Objects affected:

- Virtual machines
- Kubernetes cluster
- Cloud storage



Here we go!



- ☐ Built-in audit logs
- ☐ Platform Logs
- ☐ Host (VMs) Logs
- ☐ App Logs
- ☐ VPC Flow Logs
- ☐ Firewall Logs
- ☐ Network Capture
- ☐ Load Balancing Logs
- ☐ Google Cloud Storage Logs
- ☐ Google Cloud Storage Usage Logs
- ☐ GKS logs

Beautiful Disaster



Here we go!



- Built-in audit logs
- Platform Logs
- Host (VMs) Logs
- App Logs
- VPC Flow Logs
- Firewall Logs
- Network Capture
- Load Balancing Logs
- Google Cloud Storage Logs
- Google Cloud Storage Usage Logs
- GKS logs

Here we go!

Configure Data Access audit logs

[Send feedback](#)

This guide explains how to enable or disable some or all [Data Access audit logs](#) in your Cloud projects, billing accounts, folders, and organizations by using the Google Cloud console or the API.

Before you begin

Before you proceed with configuring Data Access audit logs, understand the following information:

★ **Important:** Data Access audit logs volume can be large. Enabling Data Access logs might result in your Cloud project being charged for the additional logs usage. For pricing information, see [Google Cloud's operations suite pricing: Cloud Logging](#).



★ **Important:** If you have configured Data Access logs to track access to objects, [authenticated browser downloads](#) from `storage.cloud.google.com` may result in a 403 response. For solutions to this issue, see the [Cloud Storage troubleshooting guide](#).



- Data Access audit logs—except for BigQuery—are disabled by default. If you want Data Access audit logs to be written for Google Cloud services other than BigQuery, you must explicitly enable them.
- Data Access audit logs are stored in the `_Default` bucket unless you've routed them elsewhere. For more information, see [Storing and routing audit logs](#).
- Data Access audit logs help Google Support troubleshoot issues with your account. Therefore, we recommend enabling Data Access audit logs when possible.



Mission Failed

From: The Boss

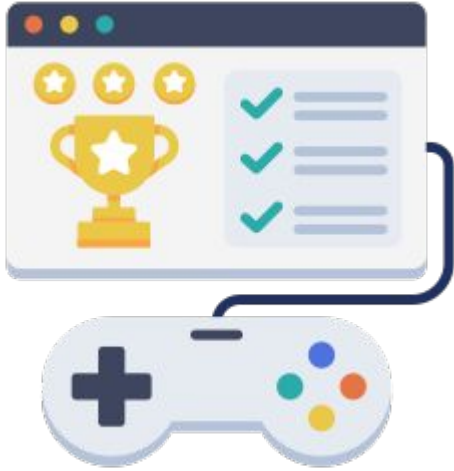
To: Cloud Security Engineer

Sent: 2022-11-04T17:28

You lost the mission, you're fired!!!



The Challenges

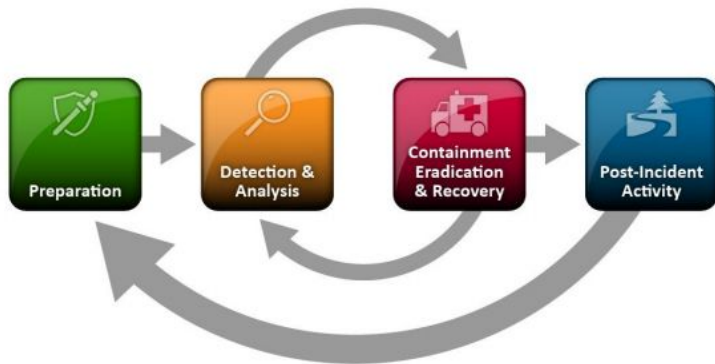


- Huge Ecosystem
- A lot of data (\$\$\$)
- No security budget
- No logs, no evidence
- Data transfer pricing (Logs and forensic images outside of GCP)
- Cloud Security Skills (AWS, Azure, GCP, Alibaba)
- Lack of preparation

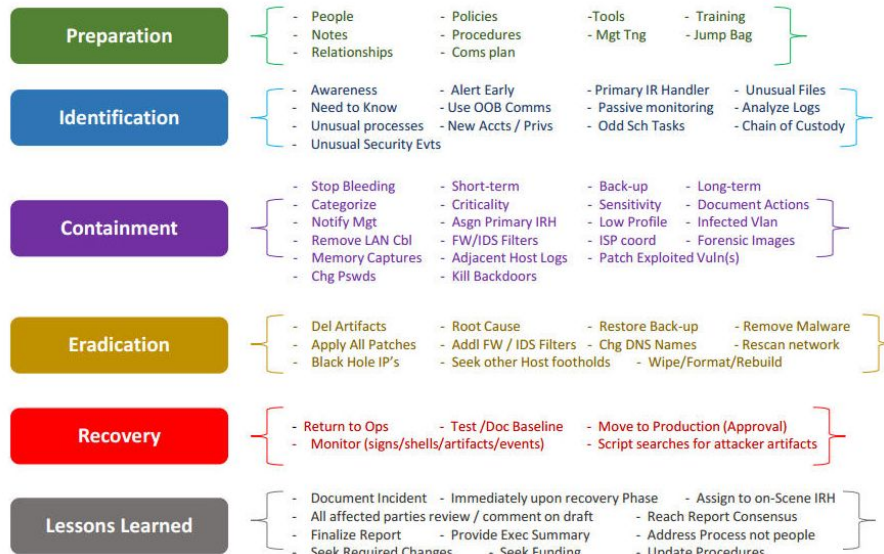


Land of
Confusion

Incident Response Process

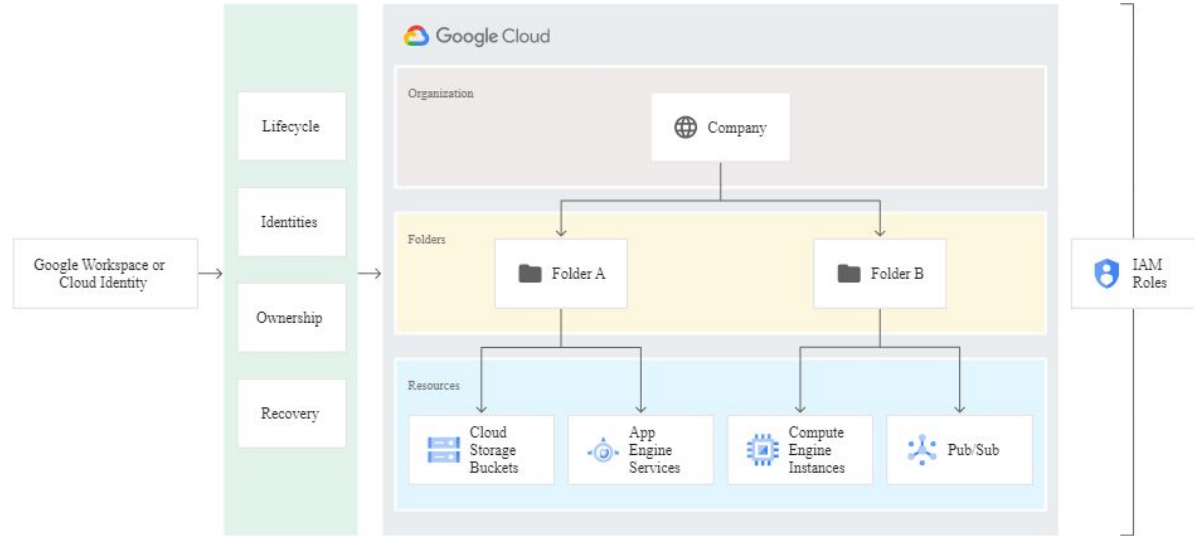
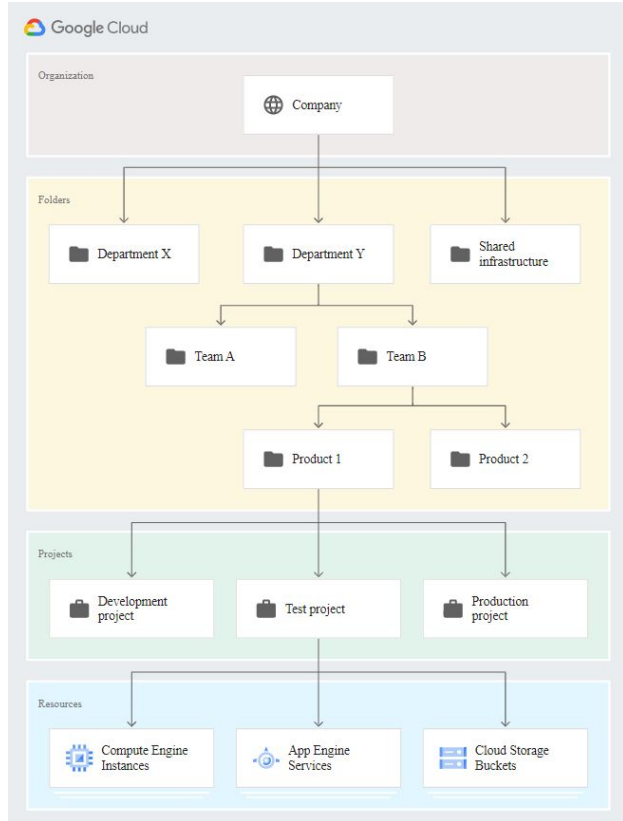


NIST SP 800-61



PICERL

What are we going to defend?



<https://cloud.google.com/resource-manager/docs/cloud-platform-resource-hierarchy>

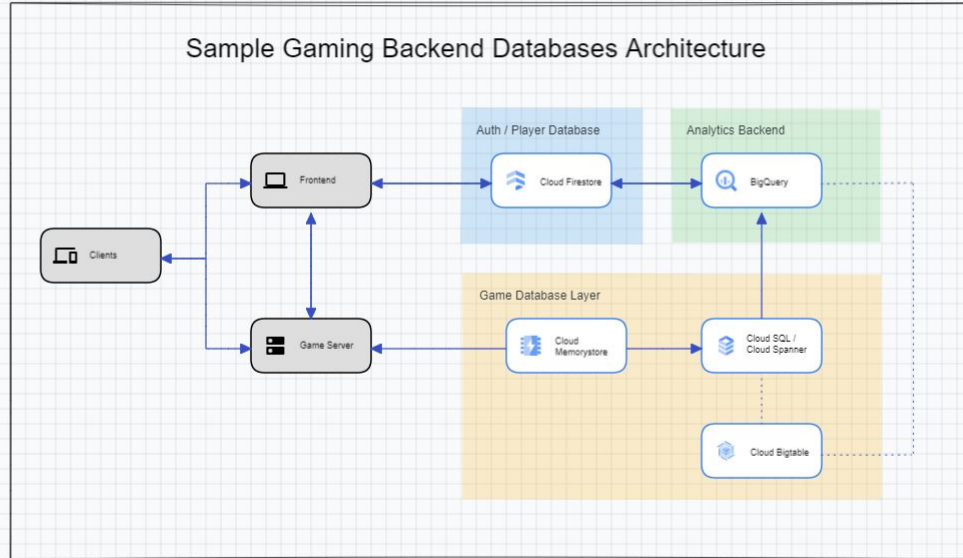
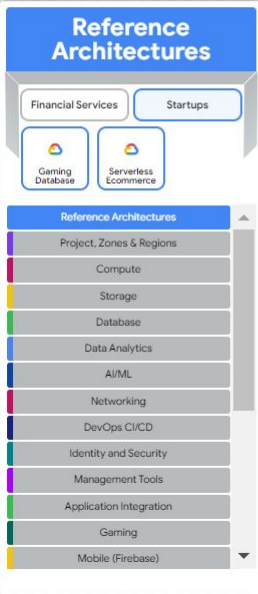
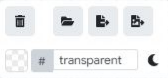
What are we going to defend?



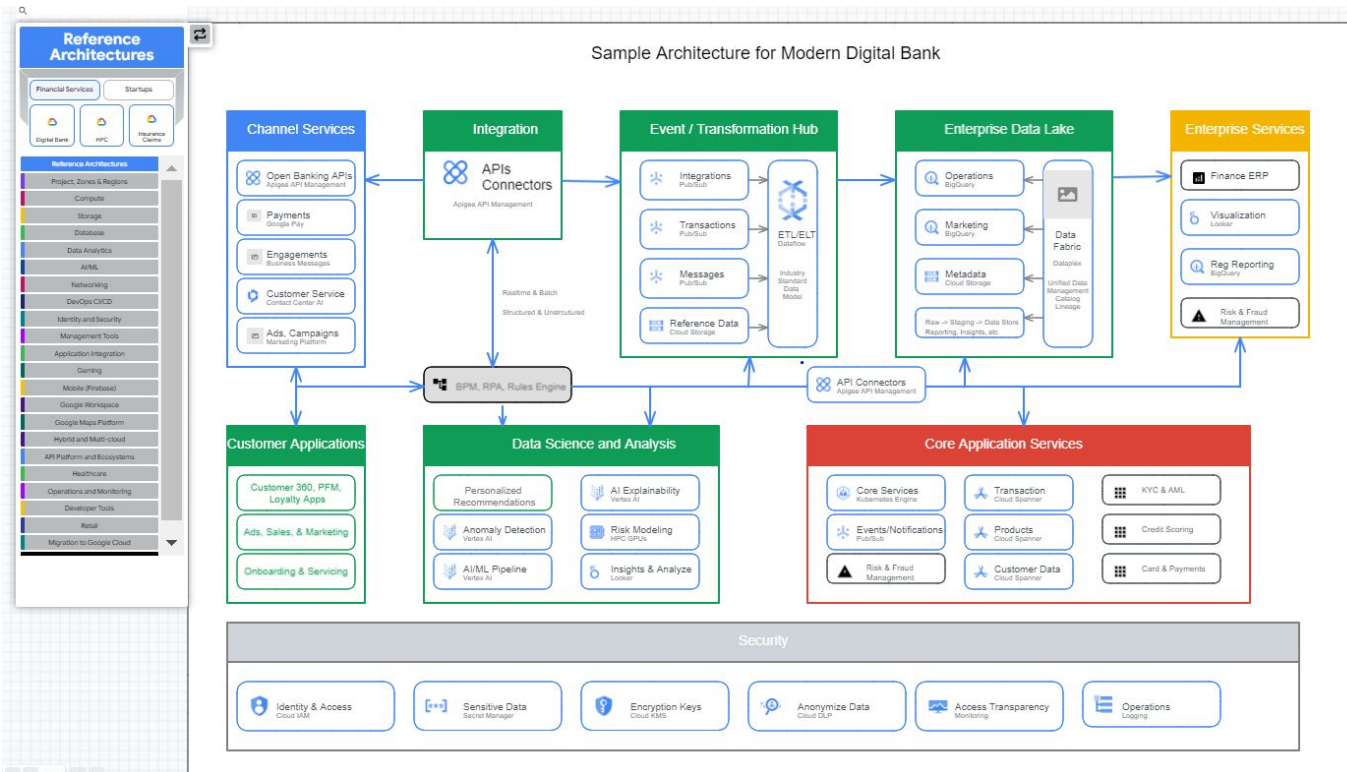
What are we going to defend?

Google Cloud

Developer cheat sheet



What are we going to defend?

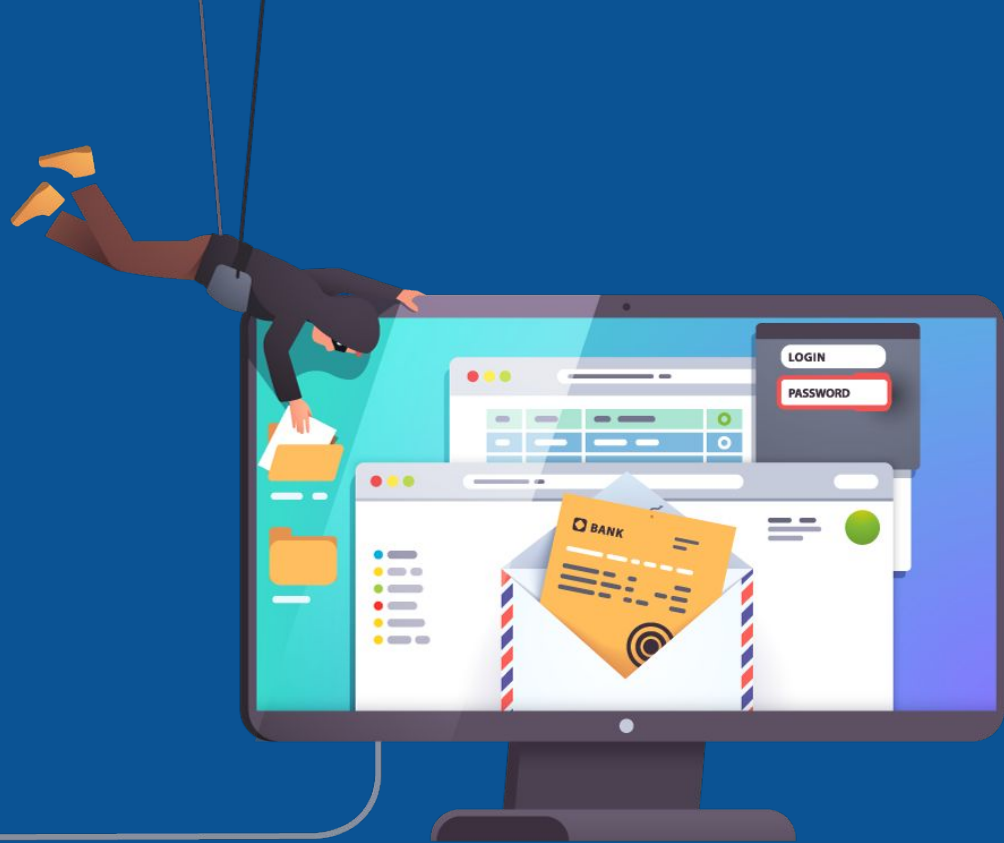


Let's build a Threat Model



1. We have a diagram
2. Set the scope
3. Zoom in on your scoped area. Model the data flows and trust boundaries between components in a data flow diagram
4. Analyze the system from the adversary perspective, think about how a Threat actor might try to attack components.
5. Now that we know who we are defending against, we can enumerate some threats / vulnerabilities / risk and countermeasure
6. Easy right?

Know
your Enemy



Threat Intel



1. Intelligence is information that is used to make a decision.
2. Threat intelligence is information about adversaries that is used to make a decision.

Profiling



- State-sponsored
- Organized Crime Groups
- Hacktivists
- Terrorists
- Malicious Insiders
- Competitive Organizations
- Script Kiddies

Their Motivations



Intellectual Property



Supply chain attacks



Financial Fraud



Extortion



Espionage

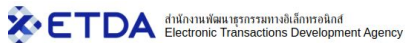


Hacktivism



Revenge

Threat Actors



Groups Tools Search Statistics




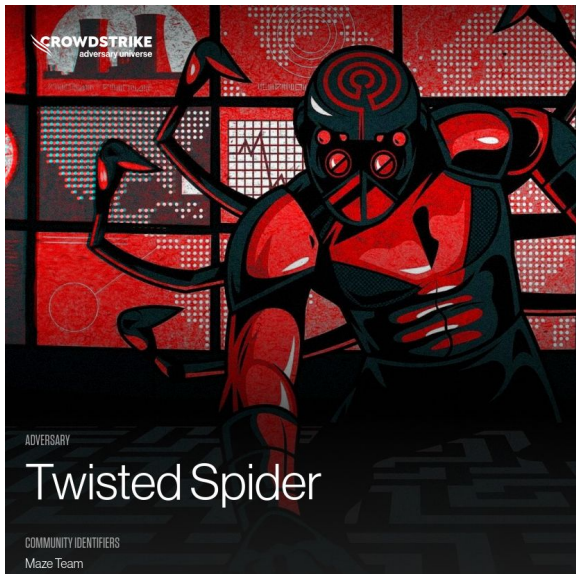
ome > List all groups > Anchor Panda, APT 14

Search

Threat Group Cards: A Threat Actor Encyclopedia

APT group: Anchor Panda, APT 14

Names	Anchor Panda (CrowdStrike) APT 14 (Mandiant) Aluminum (Microsoft) QAZTeam (?)
Country	 China
Sponsor	State-sponsored, PLA Navy
Motivation	Information theft and espionage
First seen	2012
Description	(CrowdStrike) Anchor Panda is an adversary that CrowdStrike has tracked extensively over the last year targeting both civilian and military maritime operations in the green/brown water regions primarily in the area of operations of the South Sea Fleet of the PLA Navy. In addition to maritime operations in this region, Anchor Panda also heavily targeted western companies in the US, Germany, Sweden, the UK, and Australia, and other countries involved in maritime satellite systems, aerospace companies, and defense contractors. Not surprisingly, embassies and diplomatic missions in the region, foreign intelligence services, and foreign governments with space programs were also targeted.
Observed	Sectors: Aerospace, Defense, Engineering, Government, Industrial and NGOs in the green/brown water regions primarily in the area of operations of the South Sea Fleet of the PLA Navy. Countries: Australia, Germany, Sweden, UK, USA and others.
Tools used	Gh0st RAT, Poison Ivy, Tom RAT.
Information	< https://www.crowdstrike.com/blog/whos-anchor-panda/ >



Identifying a Threat Actor Profile

Commercial threat intelligence providers and well-resourced government agencies often attribute malicious activity to a particular threat actor or actor group.

Scenario

In this scenario, a threat actor group named "Disco Team" is modeled using STIX Threat Actor and Identity objects. Disco Team operates primarily in Spanish and they have been known to steal credit card information for financial gain. They use the e-mail alias "disco-team@stealthemail.com" publicly and are known alternatively as "Equipo del Discoteca".

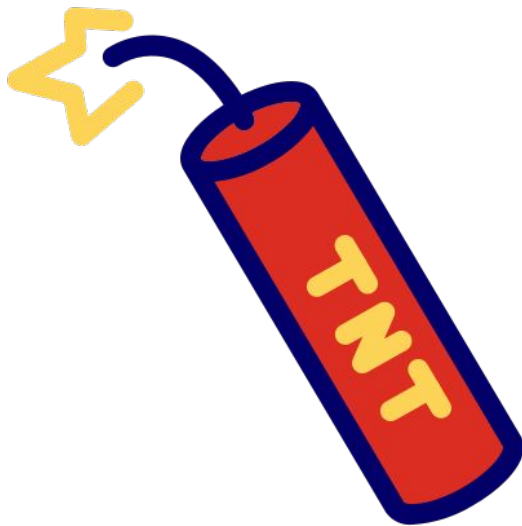
Data model

Threat actor identification is, as you would expect, represented using the [Threat Actor](#) STIX Domain Object (SDO). Information relevant to threat actors, such as goals and motivations, can be captured within this object. Other basic information not specific to threat actors, such as contact information, is best represented using an Identity SDO. Identity objects can also be used for more than threat actors in STIX. They can model organizations, government agencies, and information sources to name a few.

A diagram of this relationship below shows the Threat Actor and Identity SDO's and the Relationship SRO (An interactive version can be found [here](#)):



Threat Actors



<https://attack.mitre.org/groups/G0139/>

MITRE | **ATT&CK**

MatricesTacticsTechniquesData SourcesMitigationsGroupsSoftwareCampaignsResourcesBlogContributeSearch

ATT&CK v12 is now live! [Check out the updates here](#)

GROUPS

StriderSuckflyTA459TA505TA551**TeamTNT**TEMP.VelesThe White CompanyThreat Group-1314Threat Group-3390ThripTonto TeamTransparent TribeTropic TrooperTurlaVolatile CedarWhiteflyWindigoWindshiftWinnti Group

Home > Groups > TeamTNT

TeamTNT

TeamTNT is a threat group that has primarily targeted cloud and containerized environments. The group as been active since at least October 2019 and has mainly focused its efforts on leveraging cloud and container resources to deploy cryptocurrency miners in victim environments.^{[1][2][3][4][5][6][7][8][9]}

ID: G0139

Contributors: Will Thomas, Cyjax; Darin Smith, Cisco

Version: 1.2

Created: 01 October 2021

Last Modified: 19 October 2022

Version Permalink

ATT&CK® Navigator Layers

Domain	ID	Name	Use
Enterprise	T1098	.004 Account Manipulation: SSH Authorized Keys	TeamTNT has added RSA keys in <code>authorized_keys</code> . ^{[8][10]}
Enterprise	T1583	.001 Acquire Infrastructure: Domains	TeamTNT has obtained domains to host their payloads. ^[1]
Enterprise	T1595	.001 Active Scanning: Scanning IP Blocks	TeamTNT has scanned specific lists of target IP addresses. ^[6]

Threat Actors

ORKL

Search

Versions

Sources

About

API

Sources

- ☐ CyberMonitor (623)
- ☐ Malpedia (279)
- ☐ APTnotes (245)
- ☐ ETDA (151)
- ☐ MITRE (125)
- ☐ OTX (109)

Clear all filters

Most Recent (DB)

Q google

X

1,032 results found in 99ms



Threat Group-4127 Targets Google Accounts

Threat Group-4127 Targets Google Accounts Threat Group-4127 Targets Google Accounts secureworks.com/research/threat-group-4127-targets-google-accounts Author: SecureWorks Counter Threat Unit™ Threat Intelligence track the activities of Threat G

Q google cloud

409 results found in 134ms

Authors: Secureworks

APTnotes

MITRE:APT28

ETDA:Sofacy



Tracking the Activities of TeamTNT: A Closer Look at a Cloud-Focused Actor Group

...targeting customers of multiple cloud services and other services that potential victims might be present.13 16 | Tracking the Activities of TeamTNT: A Closer Look at a Malicious Actor Group...

Authors: EMPTY

Creation Date (PDF): 2021-07-15T15:48:25Z

MITRE

CyberMonitor

Malpedia

MITRE:TeamTNT

ETDA:Harvester

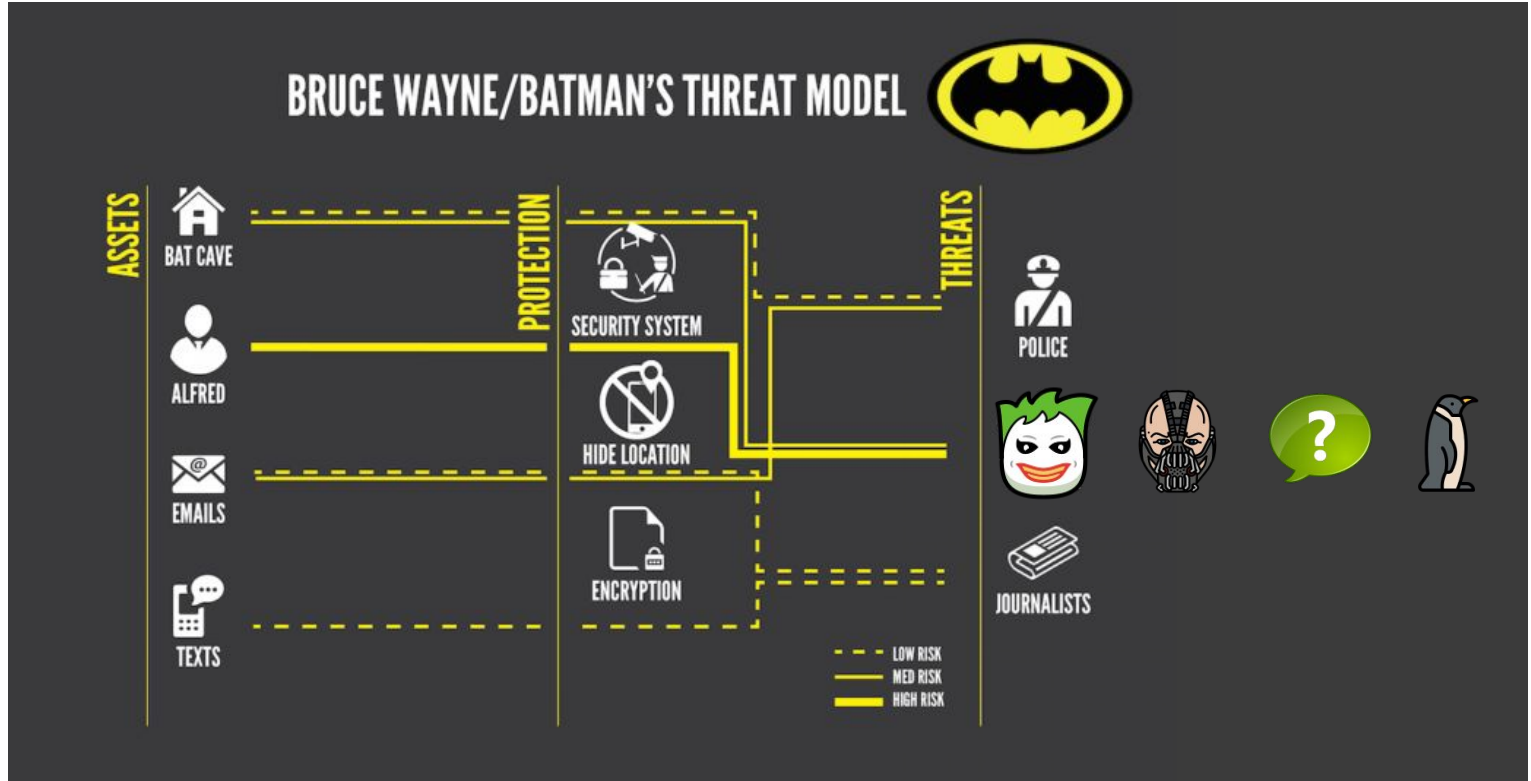
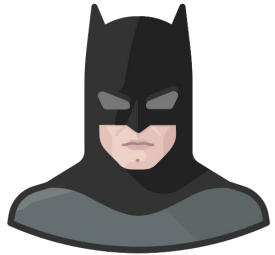
ETDA:Lead

ETDA:TA511

ETDA:Safe

Invincible

Threat Model 101



<https://arstechnica.com/information-technology/2017/07/how-i-learned-to-stop-worrying-mostly-and-love-my-threat-model/>

Attack Trees

Attack Trees

B. Schneier

Dr. Dobb's Journal, December 1999.

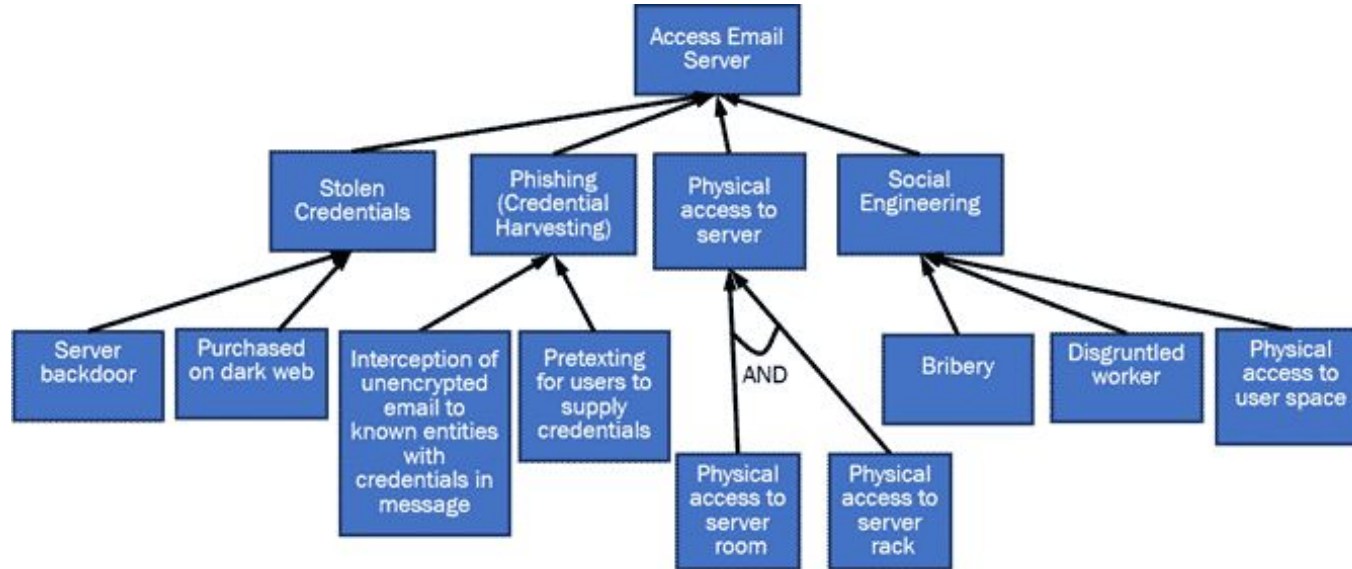
Modeling security threats

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

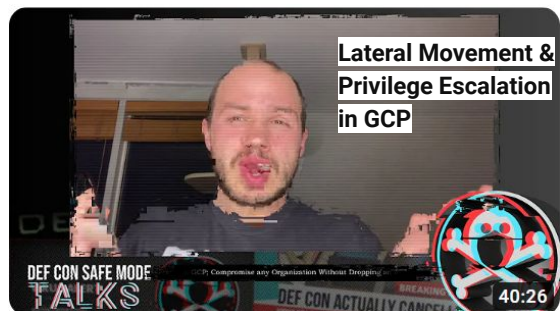
Goal: Read a specific message that has been sent from one Windows 95 computer to another.

1. Convince sender to reveal message. (OR)
 - 1.1. Bribe user.
 - 1.2. Blackmail user.
 - 1.3. Threaten user.
 - 1.4. Fool user.
2. Read message when it is being entered into the computer. (OR)
 - 2.1. Monitor electromagnetic emanations from computer screen. (Countermeasure: use a TEMPEST computer.)
 - 2.2. Visually monitor computer screen.
3. Read message when it is being stored on sender's disk. (Countermeasure: use SFS to encrypt hard drive.) (AND)
 - 3.1. Get access to hard drive. (Countermeasure: put physical locks on all doors and windows.)
 - 3.2. Read a file protected with SFS.
4. Read message when it is being sent from sender to recipient. (Countermeasure: use PGP.) (AND)
 - 4.1. Intercept message in transit. (Countermeasure: use transport-layer encryption program.)
 - 4.2. Read message encrypted with PGP.
5. Convince recipient to reveal message. (OR)
 - 5.1. Bribe user.
 - 5.2. Blackmail user.
 - 5.3. Threaten user.
 - 5.4. Fool user.
6. Read message when it is being read. (OR)
 - 6.1. Monitor electromagnetic emanations from computer screen. (Countermeasure: use a TEMPEST computer.)
 - 6.2. Visually monitor computer screen.
7. Read message when it is being stored on receiver's disk. (OR)
 - 7.1. Get stored message from user's hard drive after decryption. (Countermeasure: use SFS to encrypt hard drive.) (AND)
 - 7.1.1. Get access to hard drive. (Countermeasure: put physical locks on all doors and windows.)
 - 7.1.2. Read a file protected with SFS.
 - 7.2. Get stored message from backup tapes after decryption.
8. Get paper printout of message. (Countermeasure: store paper copies in safe.) (AND)
 - 8.1. Get physical access to safe.
 - 8.2. Open the safe.

Attack Trees



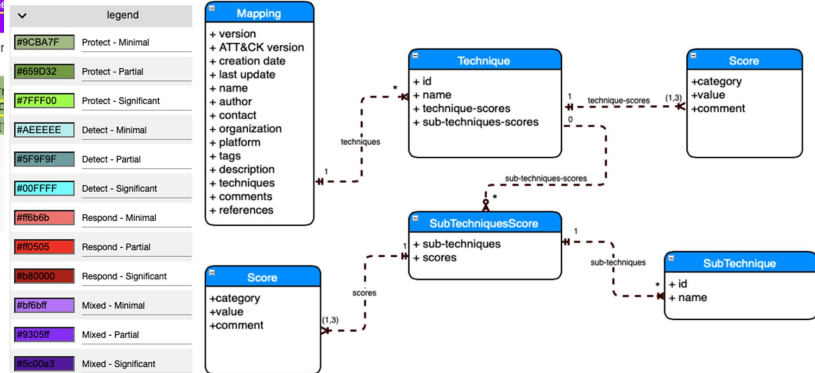
Tactics and Procedures



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Directly Cooperation	Create Administrative Command	Account Manipulation	Valid Accounts	Modify Cloud Configs Enumeration	Intercept Credentials	Account Enumeration	Software Deployment Tools	Direct on Cloud Storage Access	Applications Logs Forward	Exfiltrate Data (2 Channel)	Data Manipulation
Phishing	Deploy Container	Valid Accounts	Scheduled Task Job	Valid Accounts	Controlled User Password Storms	Cloud Storage Object Discovery	Exploitation of Remote Services	Direct on Information Persistence	Communication Through Removable Media	Cloud Data on Cloud Account	Data Distortion
Valid Accounts	Scheduled Task Job	Create Account	Account Taken Manipulation	Deploy Container	Valid Applications Account Taken	Cloud Metadata Discovery	Remote Services	Send Collection	Data Encoding	Account Exfiltration	Data E-merged for Impact
Command Processors Services	Software Deployment Tools	External Remote Services	Root or Logon Validation Sample	Unusual Unapproved Cloud Regions	Local Capture	Cloud Storage Download	Internal Spearfishing	Send Collection	Data Obfuscation	Data Transfer Raw Units	Network Bandwidth of Resource
Exploit Public Facing Application	Native API	Scheduled Task Job	Exploitation for Privilege Escalation	Account Taken Manipulation	Adversary in the Middle	Cloud Storage Discovery	Local Tool Transfer	Adversary in the Middle	Dynamic Resolution	Exfiltration Data Mitigation Forward	Service Stop
Supply Chain Compromise	Command and Control Integration on Cloud Services	Root or Logon Validation Sample	Abuse Elements Control Mechanism	Account Enumeration Control of Credentials	Steal Files	Container and Resource Discovery	Remote Service Session Hijacking	Arbitrary Collected Data	Encrypted Channel	Exfiltration Data Other Network Mediums	Account Access Potential
Hardware Assess	Exploitation for Cloud Execution	MTLS Job	Root or Logon Automated Execution	MTLS Job	Exploitation for Confidential Access	Application Workflow Discovery	Remote Service Application	Arbitrary Collection	Follows Channels	Exfiltration Data Physical Medium	Defacement
Exploitation Through Removable Media	Non Process Communication	Root or Logon Automated Execution	Control on Supply System/Process	Build Image on Host	Process Authentication	Browser Discovery	Remote Service Discovery	Automated Collection	Injects Tool Transfer	Exfiltration Over Wide Network	Data Wipe
Social Engineering	Shared Modules	Browser Enumeration	Domain Policy Modification	Debugger Execution	Forge Session	Debugger Execution	User Admin Authentication Material	Weapon Session Hijacking	Multi Stage Channel	Exfiltration Transfer	Endpoint Search of Resource
	System Services	Compromise Client Software Store	Enumerate Client	Code Injection/Script File or Information	Locally Authentication Process	Session Trust Discovery		Clipboard Data	Non Application Logon Forward	Forward Corruption	Process Corruption
	Start Execution	Create on Mobile System/Process	Send Fragment Execution	Device Malware Beacon	Steal Files Authentication Manipulation	File and Directory Discovery		Desktop/Configurations Registration	Non Standard File	Hidden System Recovery	Hidden System Recovery
	Windows Management Instrumentation	Event Triggered Execution	Event Execution Flow	Domain Policy Modification	Build File Authentication Registration/Enumeration	Group Policy Discovery		Desktop Local System	Forward Forwarding	Forward Forwarding	Forward Forwarding
		Inject Execution Flow	Process Injection	Enumeration Download	Network Sniffing	Network Sniffing		Desktop/Network Shared Drive	Proxy	System Shutdown/Reboot	System Shutdown/Reboot
		Inject Internal Image	Exploitation for Defense Evasion	OS-Confidential Enumeration for Defense Evasion	Steal Files Authentication Manipulation	Network Sniffing		Desktop Removable Media	Desktop Data Storage		
		Modify Authentication Process	Event Triggered Execution	File and Directory Permissions Modification	Steal Files Authentication Manipulation	Network Sniffing		Desktop Data Storage	Desktop Data Storage		
		Other Application Startup	Process Injection	Event Triggered Execution	Steal Files Authentication Manipulation	Network Sniffing		Desktop Data Storage	Desktop Data Storage		
		Process Injection	Process Injection	Event Triggered Execution	Steal Files Authentication Manipulation	Network Sniffing		Desktop Data Storage	Desktop Data Storage		
		Process Injection	Process Injection	Event Triggered Execution	Steal Files Authentication Manipulation	Network Sniffing		Desktop Data Storage	Desktop Data Storage		

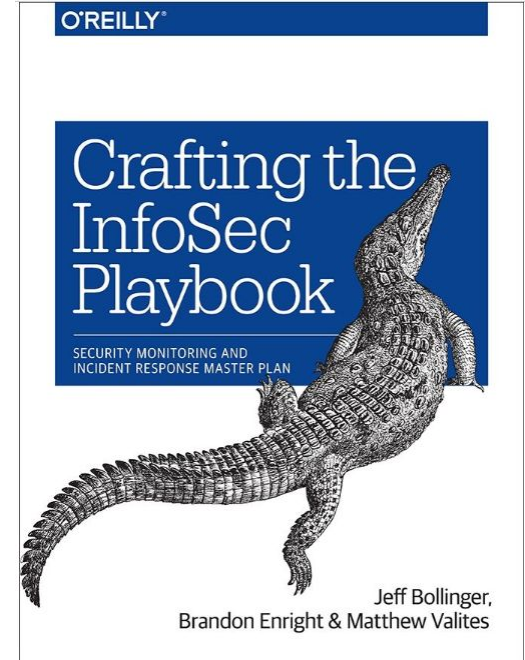
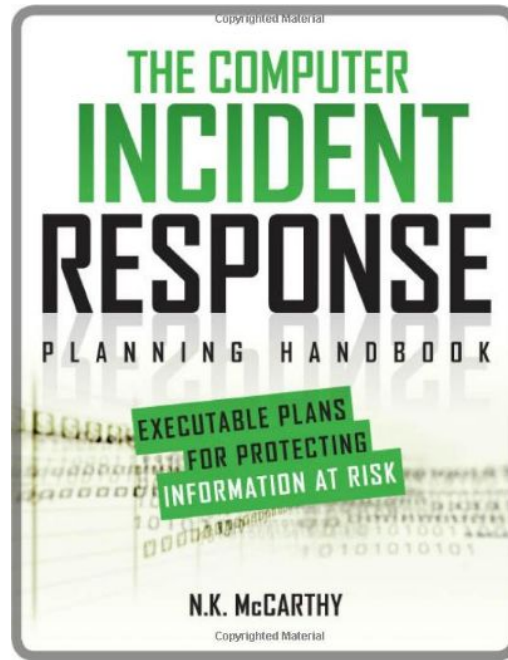
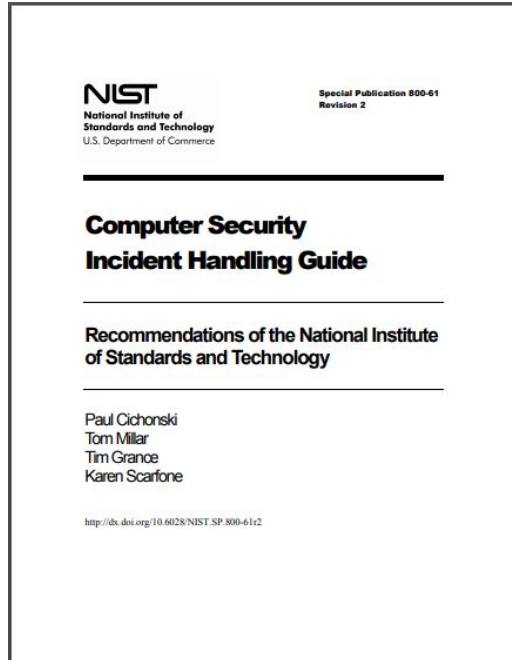
Mitre ATT&CK

Initial Access 9 techniques	Execution 10 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 38 techniques	Credential Access 15 techniques	Discovery 28 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
<ul style="list-style-type: none"> Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing Replication Through Removable Media Supply Chain Compromise Trusted Relationship Valid Accounts 	<ul style="list-style-type: none"> Command and Scripting Interpreter Exploitation for Client Execution Inter-Process Communication Native API Scheduled Task/Job Shared Modules Software Deployment Tools System Services User Execution Windows Management Instrumentation 	<ul style="list-style-type: none"> Account Manipulation BITS Jobs Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Browser Extensions Compromise Client Software Binary Create Account Create or Modify System Process Event Triggered Execution Exploitation for Privilege Escalation Hijack Execution Flow Process Injection Scheduled Task/Job 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism Access Token Manipulation BITS Jobs Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Create or Modify System Process Domain Policy Modification Escape to Host Event Triggered Execution Exploitation for Privilege Escalation Hijack Execution Flow Indicator Removal on Host Process Injection Scheduled Task/Job 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism Access Token Manipulation BITS Jobs Deobfuscate/Decode Files or Information Direct Volume Access Domain Policy Modification Execution Guardrails Exploitation for Defense Evasion File and Directory Permissions Modification Hide Artifacts Hijack Execution Flow Indicator Removal on Host Indirect Command Execution 	<ul style="list-style-type: none"> Adversary-in-the-Middle Brute Force Credentials from Password Stores Exploitation for Credential Access Forced Authentication Forge Web Credentials Input Capture Modify Authentication Process Network Sniffing OS Credential Dumping Steal Application Access Token Steal or Forge Kerberos Tickets 	<ul style="list-style-type: none"> Account Discovery Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device 	<ul style="list-style-type: none"> Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking Replication Through Removable Media Software Deployment Tools Taint Share Content Use Alternate Authentication Material 	<ul style="list-style-type: none"> Adversary-in-the-Middle Archive Collected Data Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Object Data from Configuration Repository 	<ul style="list-style-type: none"> Application Layer Protocol Communication Through Removable Media Data Encoding Data Obfuscation Dynamic Resolution Encrypted Channel Fallback Channels 	<ul style="list-style-type: none"> Automated Exfiltration Data Transfer Size Limits Exfiltration Over Alternative Protocol Exfiltration Over C2 Channel Exfiltration Over Other Network Medium Exfiltration Over Physical Medium 	<ul style="list-style-type: none"> Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation Defacement Disk Wipe Endpoint Denial of Service Firmware Corruption Inhibit System Recovery

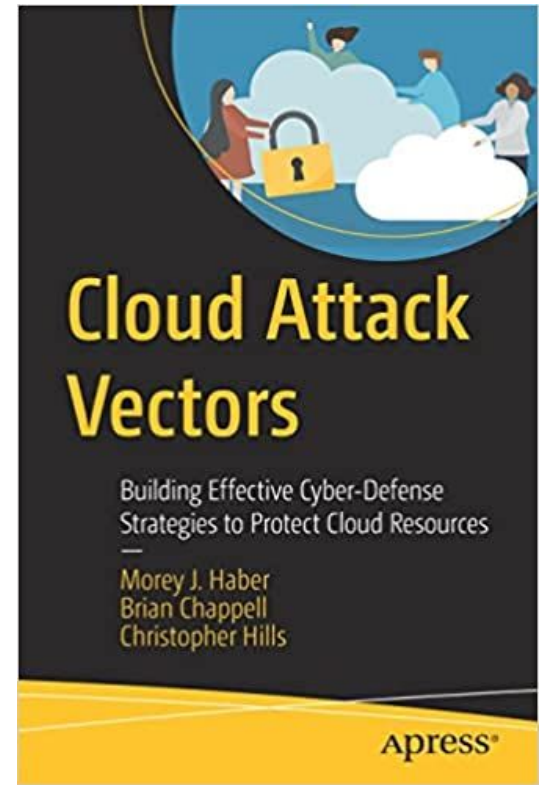
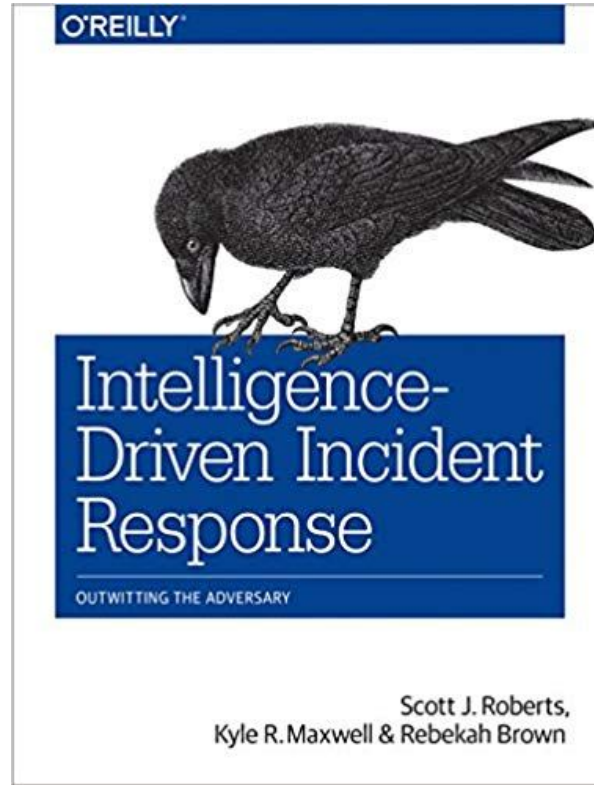
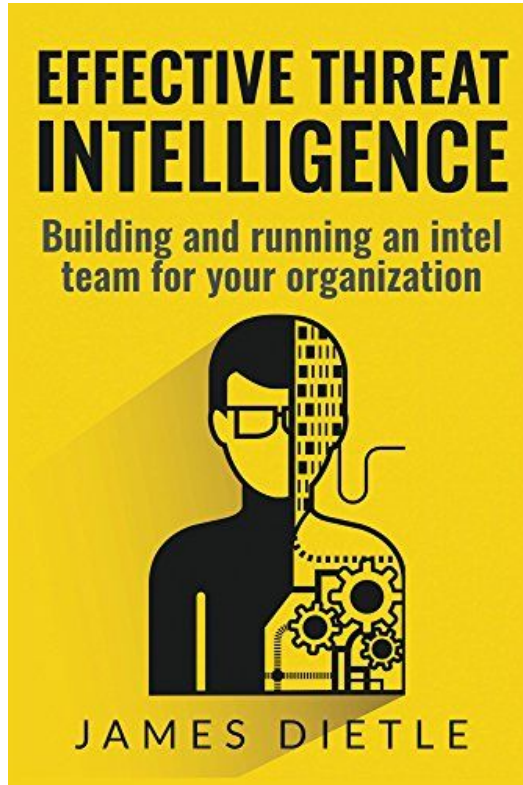


On the Run

Resources



Resources



—(dvirusⓈgondor)-[~]
\$ whoami

Daniel Rodriguez

Security Consultant

Incident Response / Digital Forensics

Twitter @dvirus

Website: <https://dvirus.training/>



FOOCAFE

Learn · Create · Share · Grow

2600
MALMO