Building Incident Response Workflows

Outcome Security

November 2023

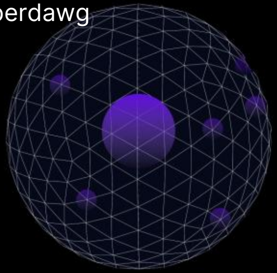
credentials.exe

Ryan Warns

Founder, Outcome Security

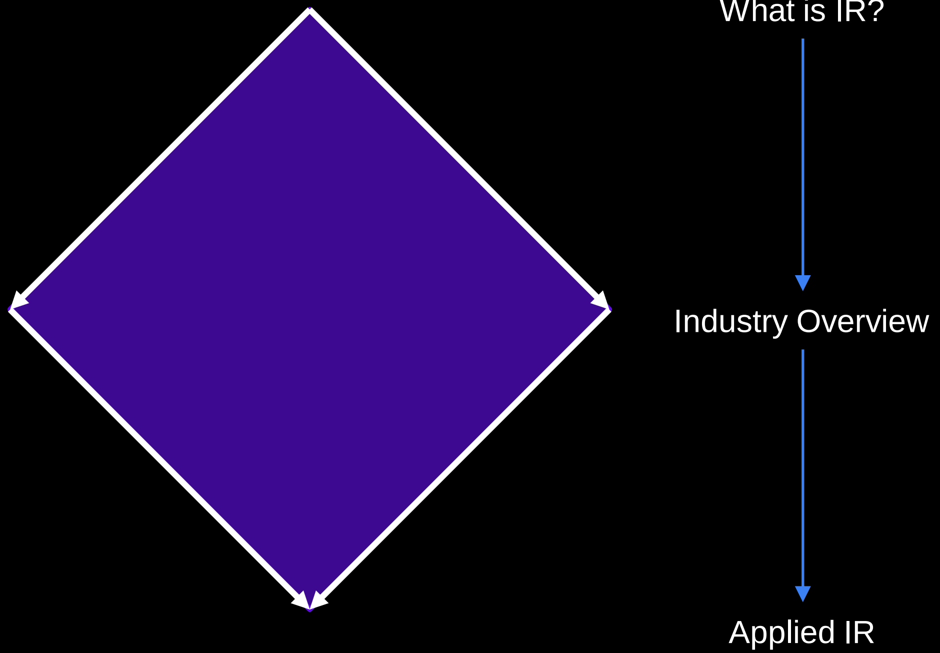
ryan.warns@outcomesecurity.com
https://www.outcomesecurity.com

- Government CNO R&D for offensive stealth tool development
- Technical Director @ Mandiant (Innovation)
- Red Teaming, Incident Response, Reverse Engineering, Vulnerability Research
- Now, building a security operations platform to assist with cyber investigations
- UMBC Grad ’13, Gen 1 Cyberdawg



Agenda

- What is IR?
- An overview of Commercial Cybersecurity Tools and Data
- Breaking tools down
- Building a proper Incident Response Workflow
- Practical examples along the way



What is IR?

Industry Overview

Applied IR

What is Incident Response?

Responding to an Incident!

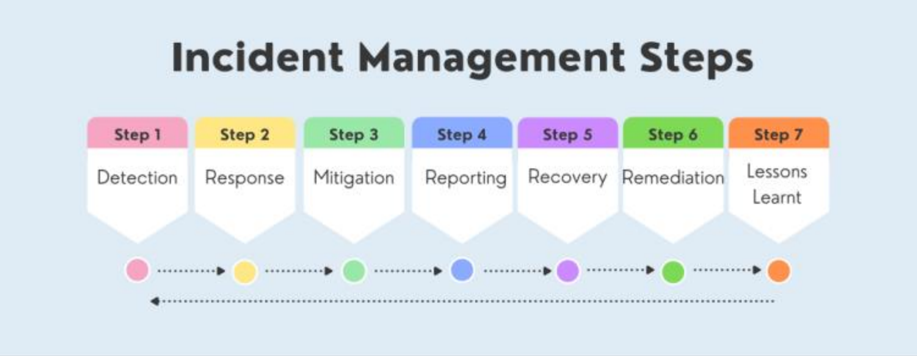
- How to we react to malicious activity targeting our teams?
- Cybersecurity analysts are stuck on tools like Excel as a general-purpose catch-all
- For every incident, cybersecurity teams need to deconflict multiple data sources

IRs start with (some) events

- Events are *can be* bad and need to be qualified
- Qualified means different things to different organizations
- Generally, "is this IOC present" and "does this apply to my company/team/etc."

IR != DFIR

- An "incident" can be anything from an e-mail, to a signature hit, to a tweet
- DF integrates and emphasizes Digital Forensics as part of the analysis
- For many incidents (e.g. phishing) the "forensics" requirements are low



Incident Management Steps

Step 1 Detection

Step 2 Response

Step 3 Mitigation

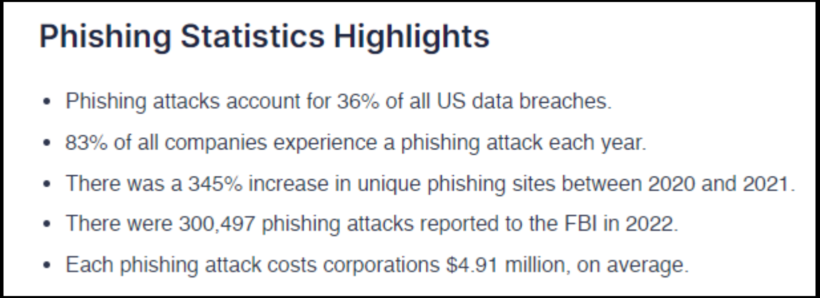
Step 4 Reporting

Step 5 Recovery

Step 6 Remediation

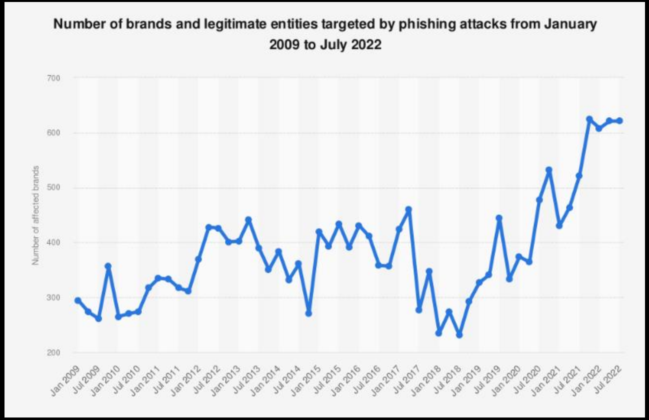
Step 7 Lessons Learnt

WHY Phishing?



Phishing Statistics Highlights

- Phishing attacks account for 36% of all US data breaches.
- 83% of all companies experience a phishing attack each year.
- There was a 345% increase in unique phishing sites between 2020 and 2021.
- There were 300,497 phishing attacks reported to the FBI in 2022.
- Each phishing attack costs corporations $4.91 million, on average.



Source: https://www.techopedia.com/phishing-statistics

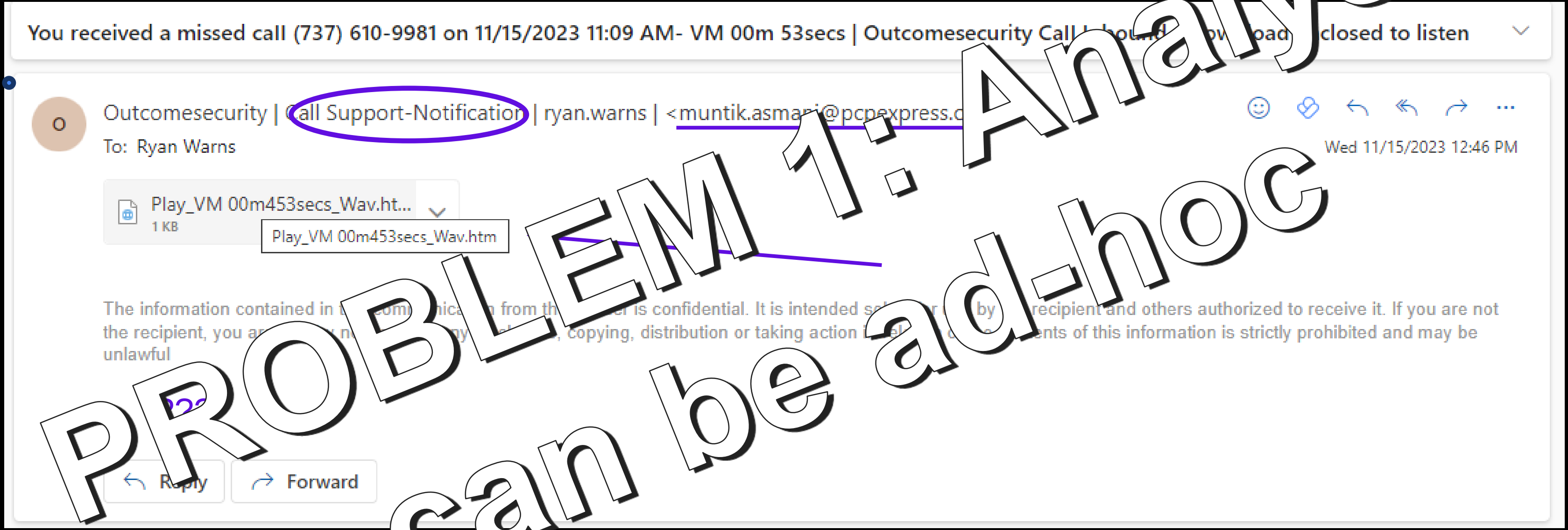
Despite appearances, phishing is the most common entry point for attacks

More sophisticated entry points (e.g. exploits) are too complicated for most attackers

Easy to implement + lots of attackers = lots of attacks

Not limited to just e-mails, although that’s still the most common

Baby's First Incident



You received a missed call (737) 610-9981 on 11/15/2023 11:09 AM- VM 00m 53secs | Outcomesecurity Call Inbound | Download Enclosed to listen

Outcomesecurity | Call Support-Notification | ryan.warns | <muntik.asmari@pcpexpress.c

To: Ryan Warns

Wed 11/15/2023 12:46 PM

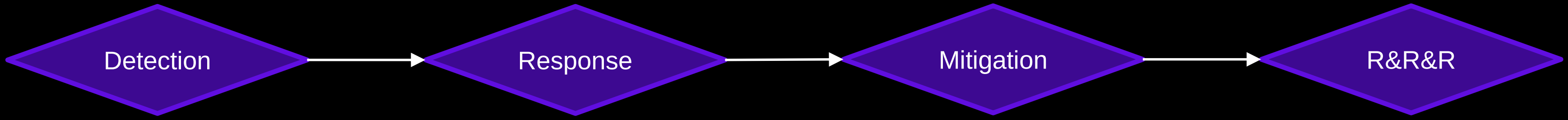
Play_VM 00m453secs_Wav.ht...
1 KB

Play_VM 00m453secs_Wav.htm

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful

PROBLEM 1: Analysis can be ad-hoc

Baby’s First Incident (as a process)



Detection

Something (a user, e-mail protection program, AV, etc.) says an e-mail is suspicious

Response

We create a case/ticket that represents analyzing this e-mail

To analyze- see steps on last slide

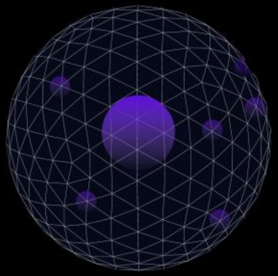
Mitigation

Delete the offending e-mail, notify affected users

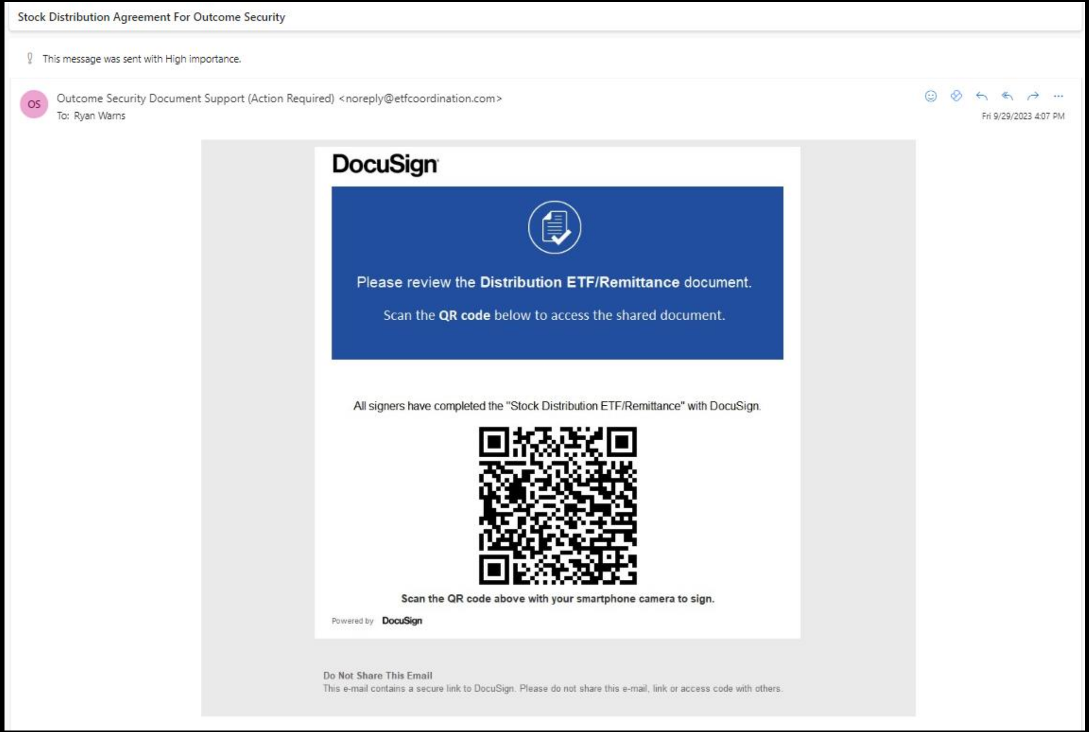
R&R&R

Summarize the analysis reports (report)

Purge e-mails from that sender from your organization (remediation)



Baby’s Second Incident



Stock Distribution Agreement For Outcome Security

This message was sent with High importance.

Outcome Security Document Support (Action Required) <noreply@etfcoordination.com>
To: Ryan Warns

Fri 9/29/2023 4:07 PM

DocuSign

Please review the **Distribution ETF/Remittance** document.

Scan the **QR code** below to access the shared document.

All signers have completed the "Stock Distribution ETF/Remittance" with DocuSign.

Scan the QR code above with your smartphone camera to sign.

Powered by DocuSign

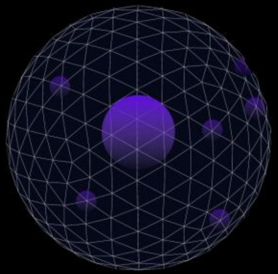
Do Not Share This Email
This e-mail contains a secure link to DocuSign. Please do not share this e-mail, link or access code with others.

No attachments

Real asset (images) in e-mail body

Sender *could* be real

External link probably goes somewhere bad



Not All IR is Created Equal

Sophistication

Detection	Response	Mitigation	R&R&R
User reports	Tickets	Automatic Quarantine	Ticket summaries
Static signatures	Case Management	Hash Blacklists	Full reports
Attachment scanning	E-mail metadata	Domain Takedowns	Malicious IOC knowledge management
Content heuristics	Domain reputation		Response playbooks
	Attachment RE		

If it’s so easy, why do we need a workflow?

Phishing *feels* like an easy problem to solve

- Check for attachments
- Check for typos/weird text
- Check domain against a bad list
- …done?

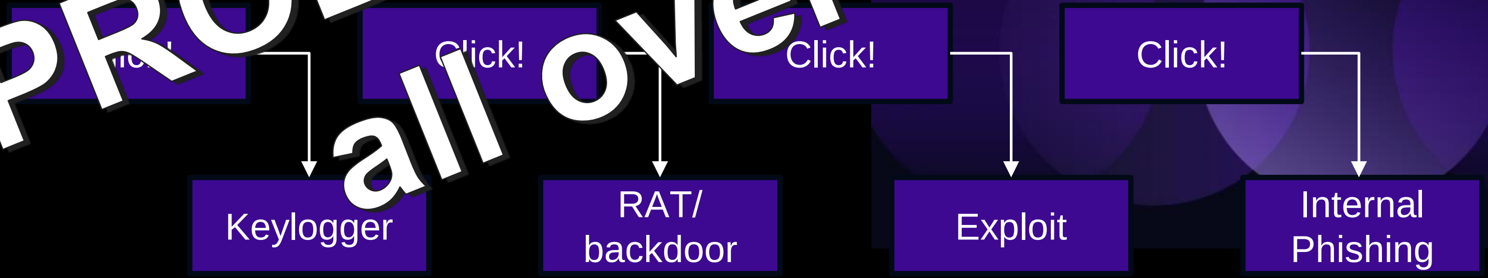
So, what happens when users click them?

- And they will!

Phishing is an extremely common point of entry for deeper breaches

- A large part of initial the IR process it to determine the extent to which an attacker penetrated an org or a network
- For Phishing: did they install malware? Did they harvest credentials? Are they targeting other users internally? Something else?
- To do this, defenders need to use additional technologies

PROBLEM 2: Evidence is all over the place



Cybersecurity Tools

Many Cybersecurity Tools Available

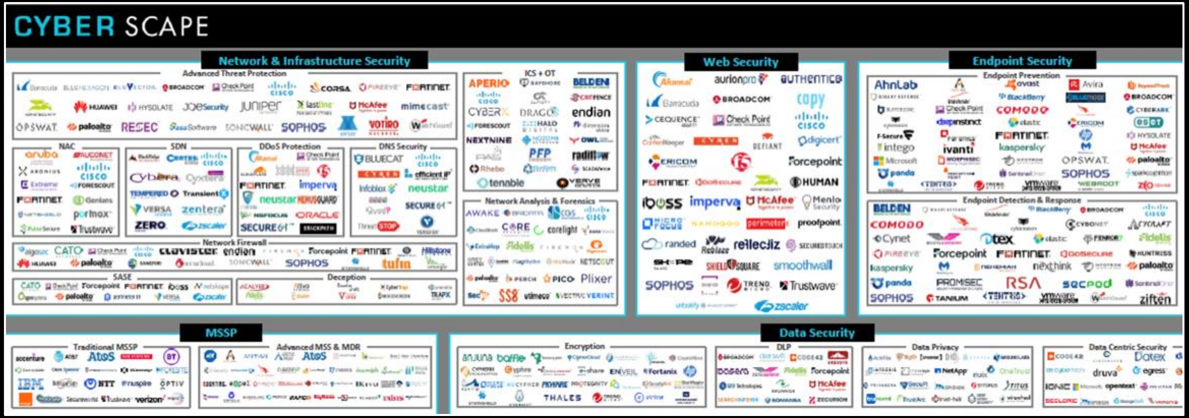
- Some provider data
- Some create and action signatures, detection, etc.
- Some are unified views that combine output from different tools

Tools help at Different Stages of IR

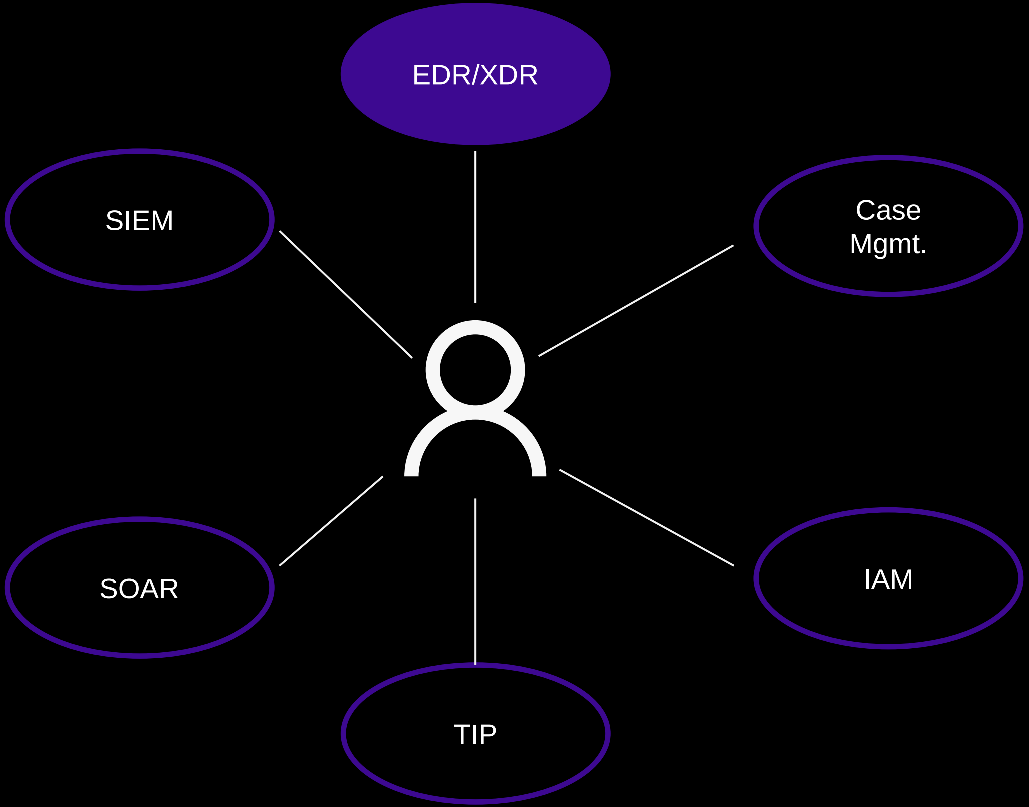
- Some tools help with initial detection
- Some tools help with data enrichment during the investigation
- Some tools make it easier to centralize logs and other internal data

Tools Are *Usually* Specialized

- Specific problems or teams within an organization
- Over the past few years, more examples of bigger companies “unifying” products
- This means that product categories are “squishy”



A Whirlwind Tour of Cybersecurity Products



Endpoint Detection and Response (EDR) tools are endpoint-focused tools for collecting Telemetry, monitoring machines, and handling follow-up alerts

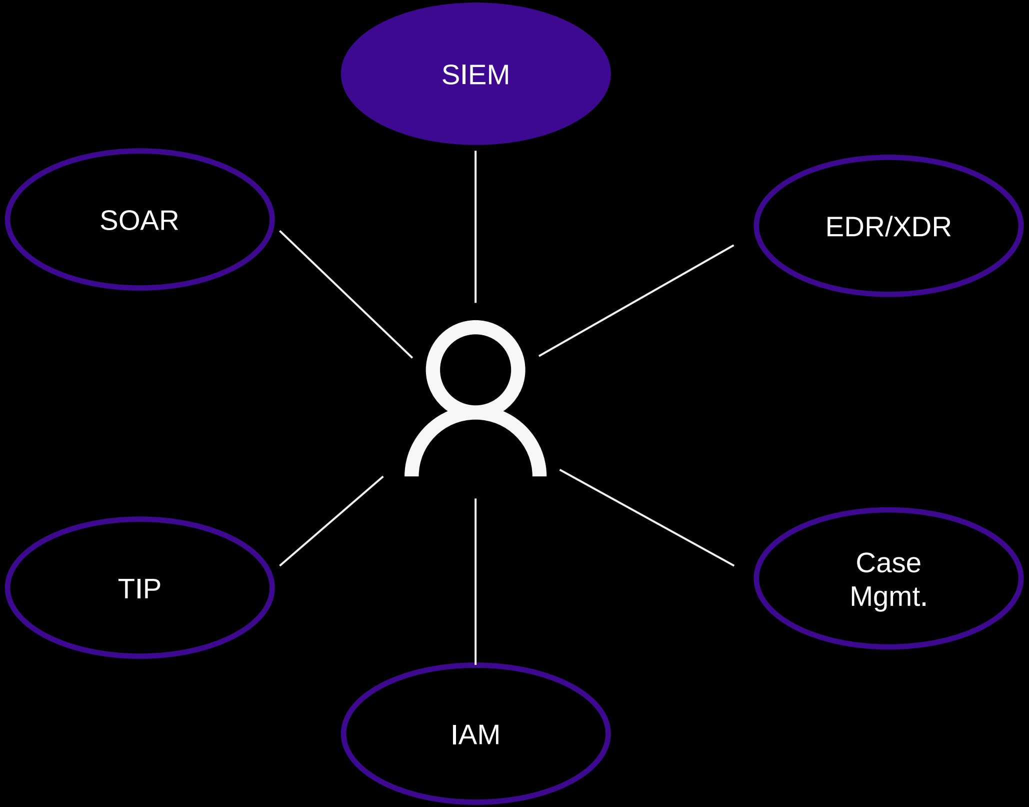
Network Detection and Response (NDR) tools perform similar functions but for network data

Extended Detection and Response (XDR) attempts to consolidate this data alongside other information sources like cloud assets, identity, e-mail, etc.

This evolved out of what we used to call Antivirus (AV)

Many EDR solutions include a sandbox

A Whirlwind Tour of Cybersecurity Products

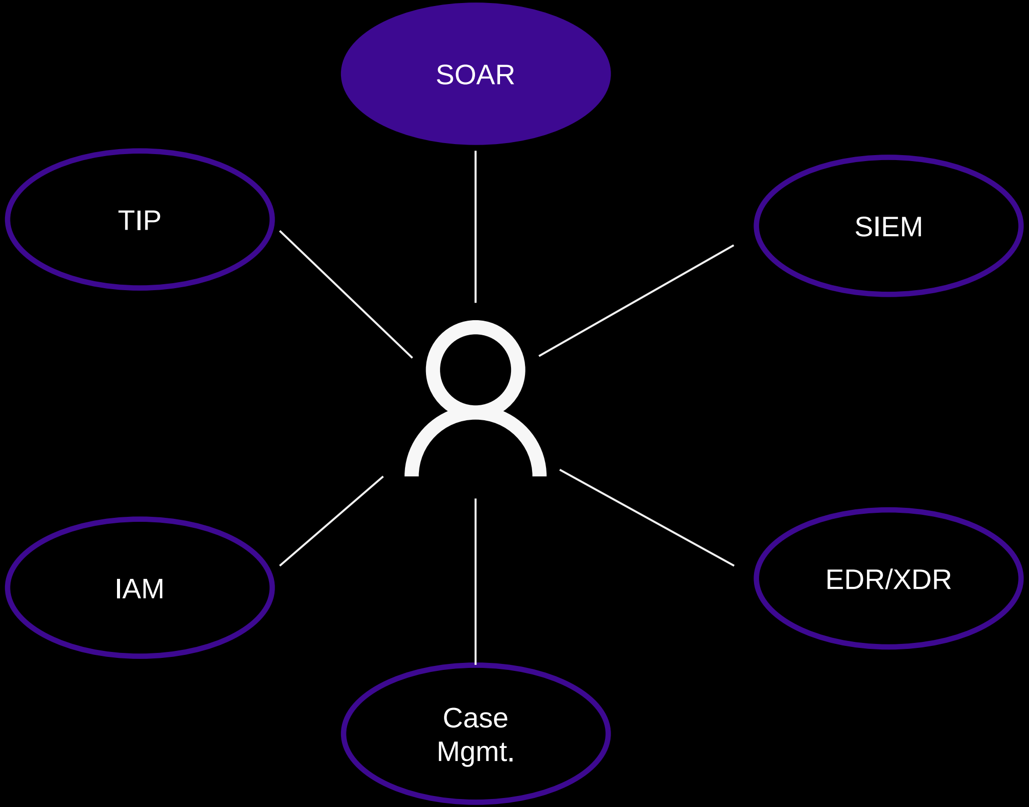


Security Information and Event Management (SIEM) tools gather and track events across an organization’s internal assets

In practice, this means centralizing various logs into a single place and indexing them in a way that is searchable to find Indicators of Compromise (IOCs) within an organization

SIEMs do not generally involve actioning incidents or producing alerts, although some products can turn query results into tickets, alerts, etc.

A Whirlwind Tour of Cybersecurity Products

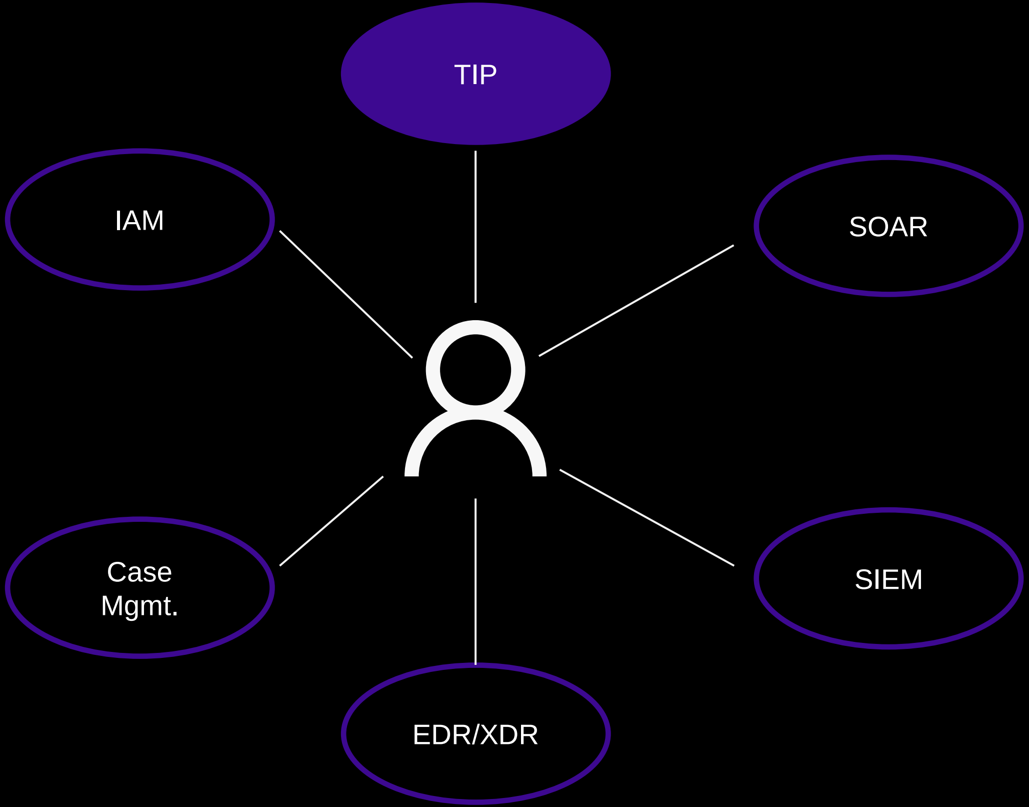


Security Orchestration Automation and Response (SOAR) platforms are most often used to action policies and Deployments, and automate common security processes

Functionally a lot of SOARs focus on taking an alert, gathering context, and sending that alert to another System or tool

We mentioned that most organizations get overwhelmed by alerts – this is one mechanism that teams can use to try to automate some of their security processes

A Whirlwind Tour of Cybersecurity Products



Threat Intelligence Platforms (TIPs) are designed to source, Aggregate, and deconflict threat intelligence data

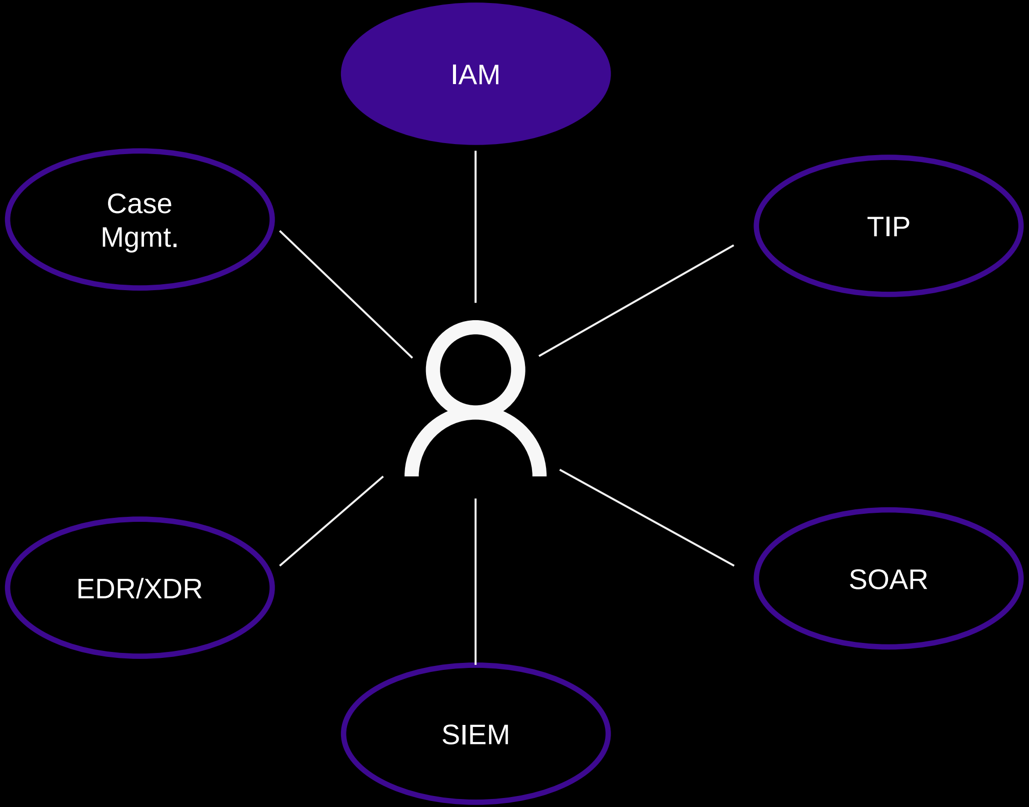
Threat Intelligence data is usually focused on:

- IOCs – IPs, domains, hashes, etc. known to be malicious
- Attribution information – connecting malicious activity to known malicious groups
- Threat Actor clustering – the “human side” of malicious operations, e.g. who they tend to target

TIPs may (usually) aggregate data from multiple data sources

The primary goal of threat intelligence is to help teams prioritize alerts

A Whirlwind Tour of Cybersecurity Products

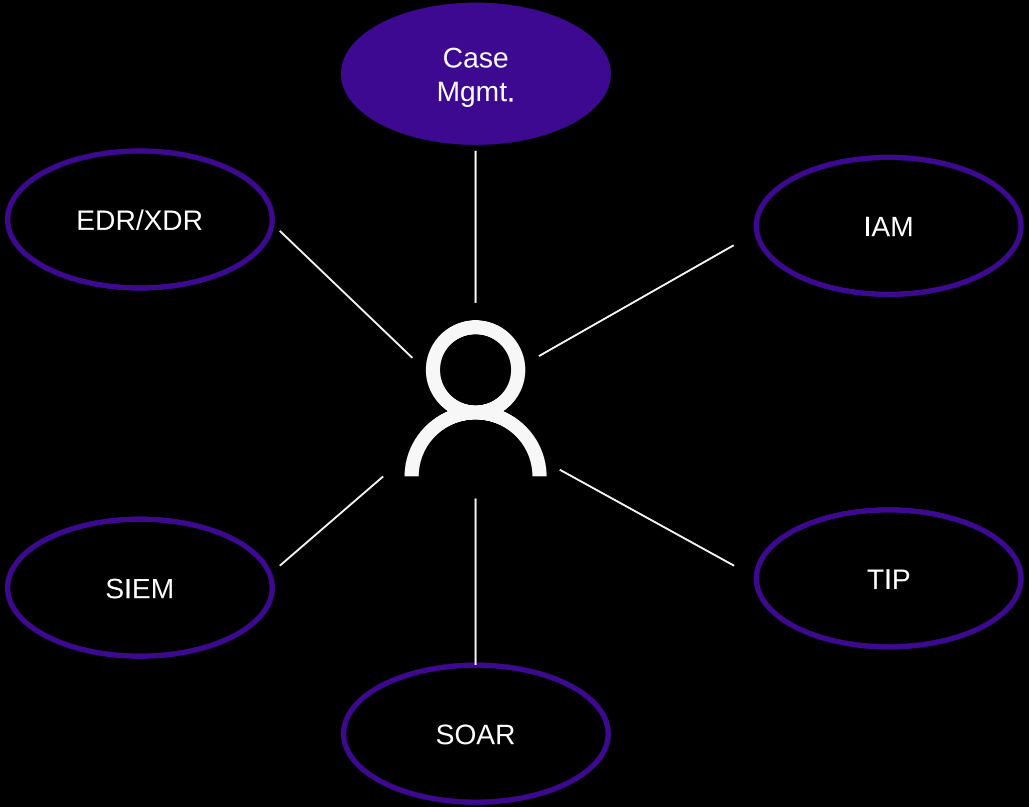


Identity and Access Management (IAM) tools help manage, deploy and monitor user information, access privileges, and credentials across an organization

Meant to restrict and monitor access policies related to different assets

Nowadays, a lot of these solutions are discussed in the context of Zero Trust

A Whirlwind Tour of Cybersecurity Products



Case management tools associate alerts with tasks in order to track how analysis is going, whether it has been resolved, etc.

At its simplest form, it's a collection of tickets tracking different parts of triaging alerts

This is not cyber *specific* but good rules for cyber tasks:

- Context (source, supporting data, etc.) should be present at ticket creation or very early
- Ticket resolution should connect to something "cyber" – created a rule, blocked an IOC, etc.
- Resolution needs to be justified somehow – "we took action <x> because of <y>"

Zooming Out: IR, In Reality

What are we doing for an IR?

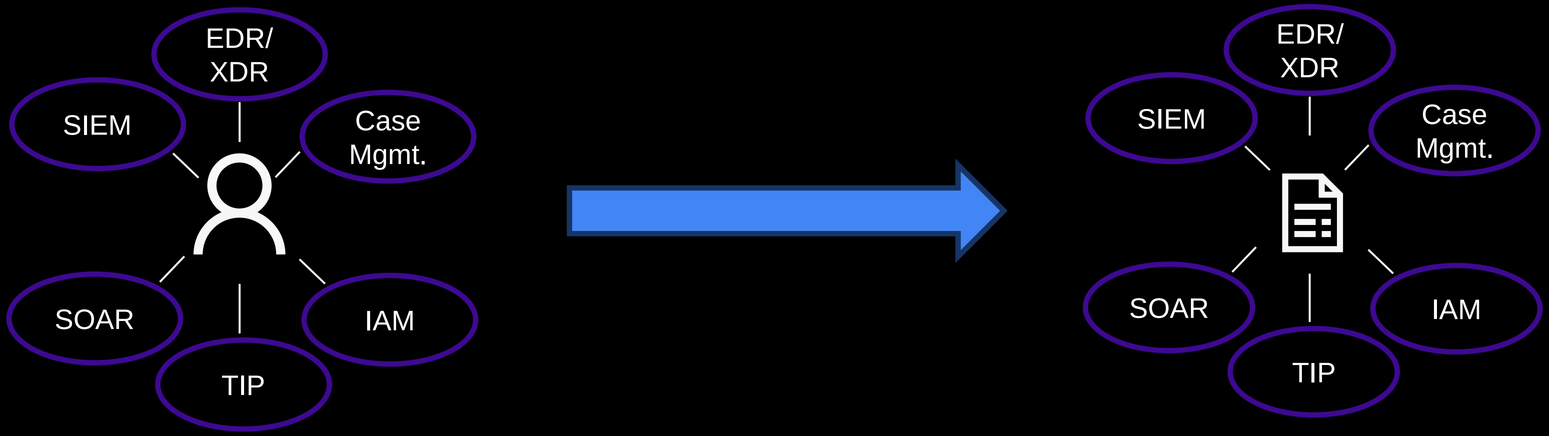
- Raw alert
- Does this alert affect my organization (not a FP, is present in our environment, etc.)
- Fix it

HOW do I decide if something affects my organization?

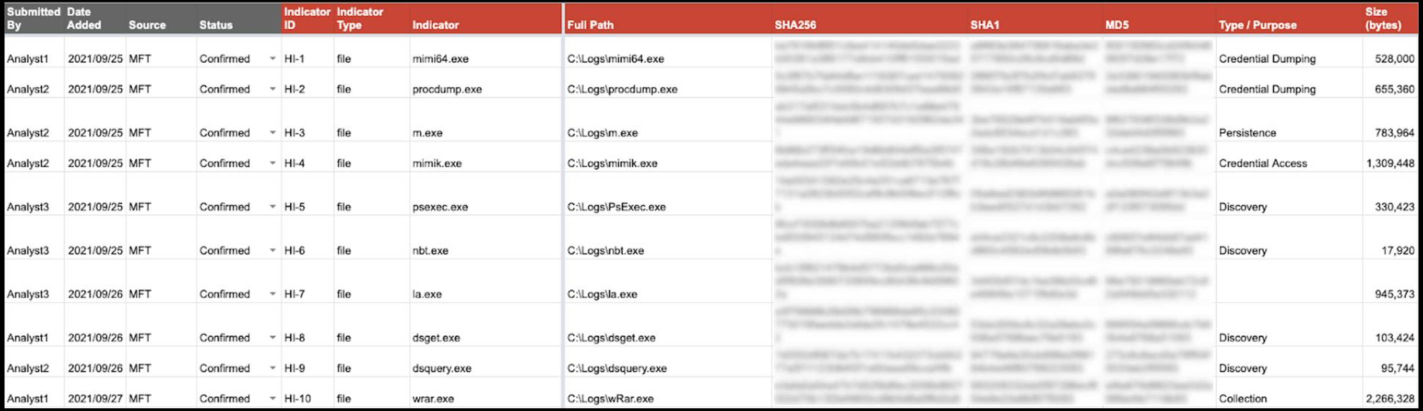
- Contextualize it with external data (TIPs, data feeds, etc.)
- Find it in our environment (logs, SIEM, etc.)
- Mitigate it (EDR/NDR, SOAR, etc.)

So where's the workflow come from?

- I have all the tools, right?



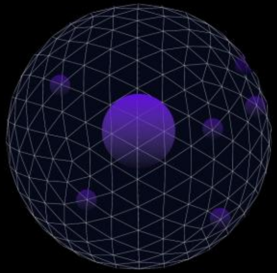
IR In Reality: Spreadsheets of Doom



Submitted By	Date Added	Source	Status	Indicator ID	Indicator Type	Indicator	Full Path	SHA256	SHA1	MD5	Type / Purpose	Size (bytes)
Analyst1	2021/09/25	MFT	Confirmed	HI-1	file	mimi64.exe	C:\Logs\mimi64.exe	[illegible]	[illegible]	[illegible]	Credential Dumping	528,000
Analyst2	2021/09/25	MFT	Confirmed	HI-2	file	procdump.exe	C:\Logs\procdump.exe	[illegible]	[illegible]	[illegible]	Credential Dumping	655,360
Analyst2	2021/09/25	MFT	Confirmed	HI-3	file	m.exe	C:\Logs\m.exe	[illegible]	[illegible]	[illegible]	Persistence	783,964
Analyst2	2021/09/25	MFT	Confirmed	HI-4	file	mimik.exe	C:\Logs\mimik.exe	[illegible]	[illegible]	[illegible]	Credential Access	1,309,448
Analyst3	2021/09/25	MFT	Confirmed	HI-5	file	psexec.exe	C:\Logs\PsExec.exe	[illegible]	[illegible]	[illegible]	Discovery	330,423
Analyst3	2021/09/25	MFT	Confirmed	HI-6	file	nbt.exe	C:\Logs\nbt.exe	[illegible]	[illegible]	[illegible]	Discovery	17,920
Analyst3	2021/09/26	MFT	Confirmed	HI-7	file	la.exe	C:\Logs\la.exe	[illegible]	[illegible]	[illegible]		945,373
Analyst1	2021/09/26	MFT	Confirmed	HI-8	file	dsget.exe	C:\Logs\dsget.exe	[illegible]	[illegible]	[illegible]	Discovery	103,424
Analyst2	2021/09/26	MFT	Confirmed	HI-9	file	dsquery.exe	C:\Logs\dsquery.exe	[illegible]	[illegible]	[illegible]	Discovery	95,744
Analyst1	2021/09/27	MFT	Confirmed	HI-10	file	wrar.exe	C:\Logs\wRar.exe	[illegible]	[illegible]	[illegible]	Collection	2,266,328

IR professionals usually use spreadsheets to track data of interest during an engagement

- Need a catchall place to store data
- Need to cross reference internal and external data feeds
- Spreadsheets are easy
- Passed upstream to other tools later



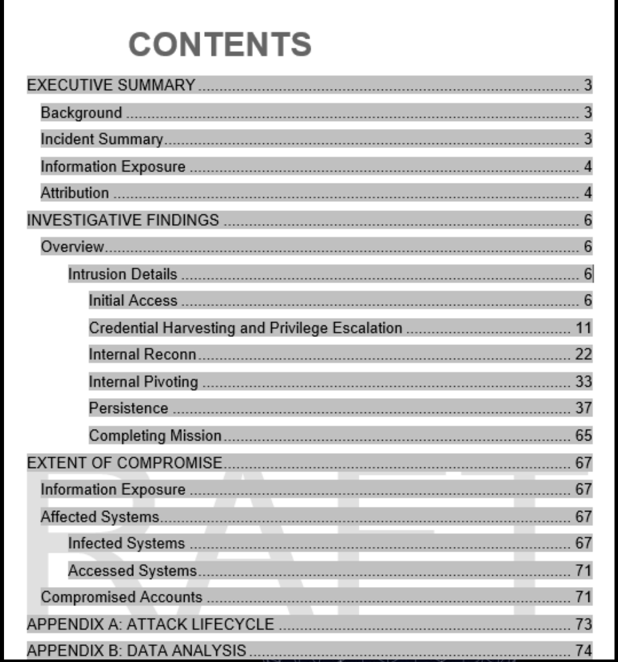
Source: https://www.crowdstrike.com/blog/crowdstrike-releases-digital-forensics-and-incident-response-tracker/

IR In Reality: Building Effective Reports

All tools and evidence gathering are in support of creating a complete report/summary of the incident, even if that report is just for an internal ticket

What is a “complete” report?

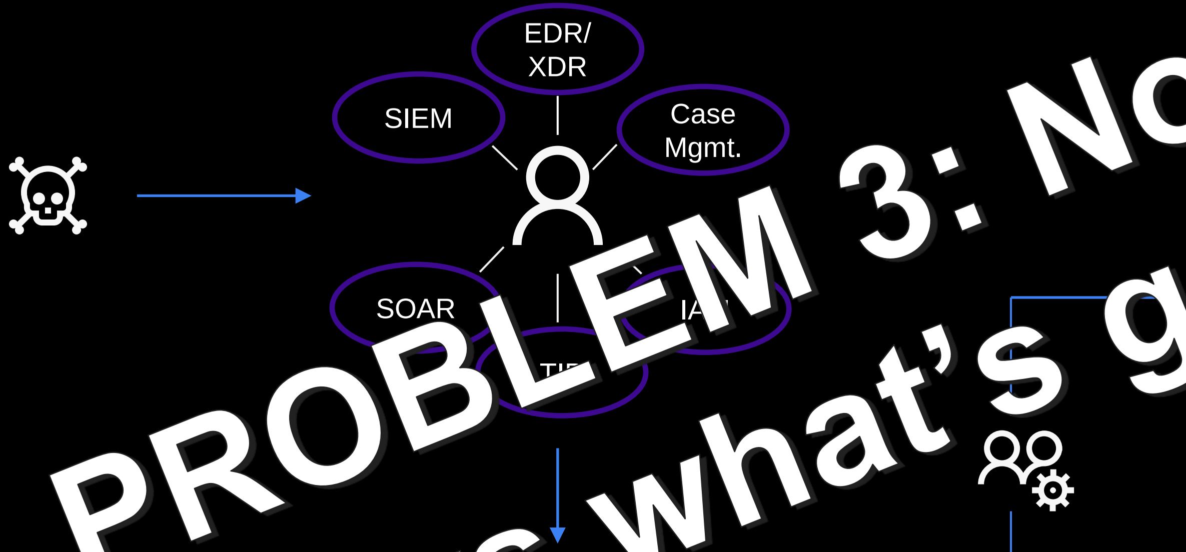
- Summary – was the good or bad?
- Extent – How severe was any compromise?
- Recommendations or Remediations
- Investigation Process – show your work
- Supporting Evidence – IOCs, data, etc.

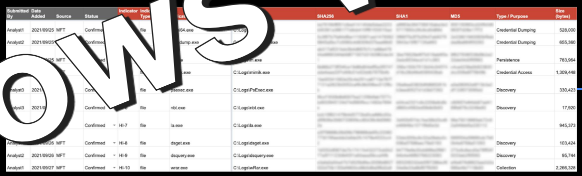


CONTENTS

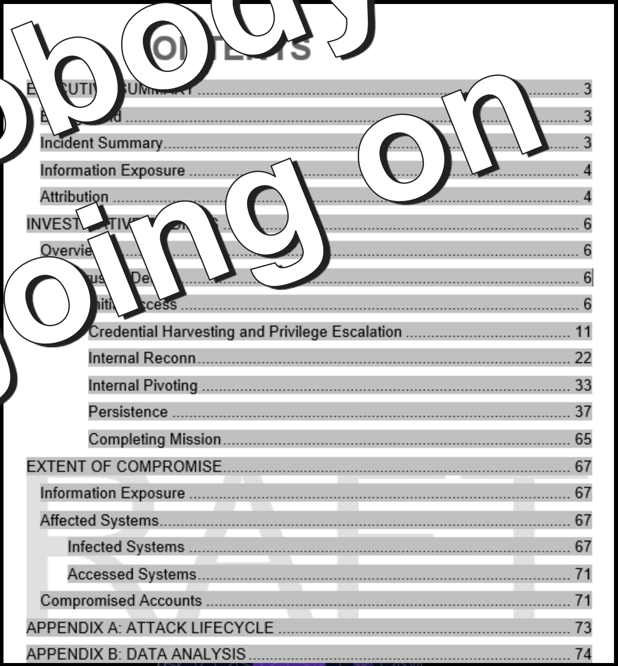
IR In Reality

PROBLEM 3: Nobody knows what's going on





Submitted By	Date Added	Source	Status	Indicator	Indic Type	icat		SHA256	SHA1	MD5	Type / Purpose	Size (bytes)
Analyst1	2021/09/25	MFT	Confirme		file	i64.exe	C:\Log	[illegible]	[illegible]	[illegible]	Credential Dumping	528,000
Analyst2	2021/09/25		Confirmed			dump.exe	C: exe	[illegible]	[illegible]	[illegible]	Credential Dumping	655,360
	25	MFT	ed			e	C:\Logs\ m.exe	[illegible]	[illegible]	[illegible]	Persistence	783,964
		FT			fi	exe	C:\Logs\mimik.exe	[illegible]	[illegible]	[illegible]	Credential Access	1,309,448
nalyst3	2021/		Con		file	psexec.exe	C:\Logs\PsExec.exe	[illegible]	[illegible]	[illegible]	Discovery	330,423
nalyst3	2021/0		Confirmed		file	nbt.exe	C:\Logs\nbt.exe	[illegible]	[illegible]	[illegible]	Discovery	17,920
			Confirmed	HI-7	file	la.exe	C:\Logs\la.exe	[illegible]	[illegible]	[illegible]		945,373
Analyst	09/26	MFT	Confirmed	HI-8	file	dsget.exe	C:\Logs\dsget.exe	[illegible]	[illegible]	[illegible]	Discovery	103,424
Analyst2	2021/09/26	MFT	Confirmed	HI-9	file	dsquery.exe	C:\Logs\dsquery.exe	[illegible]	[illegible]	[illegible]	Discovery	95,744
Analyst1	2021/09/27	MFT	Confirmed	HI-10	file	wrar.exe	C:\Logs\wRar.exe	[illegible]	[illegible]	[illegible]	Collection	2,266,328



O TENTS

E CUTIV SUMMARY 3
B d 3
Incident Summary 3
Information Exposure 4
Attribution 4
INVEST TIVE 6
Overvie 6
us De 6
nitia ccess 6
Credential Harvesting and Privilege Escalation 11
Internal Reconn 22
Internal Pivoting 33
Persistence 37
Completing Mission 65
EXTENT OF COMPROMISE 67
Information Exposure 67
Affected Systems 67
Infected Systems 67
Accessed Systems 71
Compromised Accounts 71
APPENDIX A: ATTACK LIFECYCLE 73
APPENDIX B: DATA ANALYSIS 74

Tenants of an Effective IR Workflow

1

A Variety of Incidents

We know that there can be different kinds of incidents, and each incident has different complexity

2

Proper Tool Usage

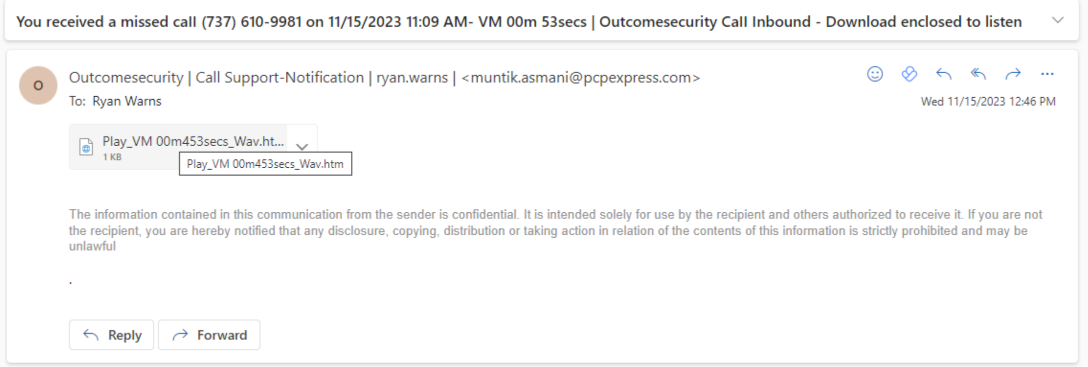
We might have access to different types of tools that can help us with different stages of the analysis process

3

Analysis Tracking

The more we can track about *how* we analyze different alerts the more we can improve over time and the better our incident reports will be

IR Workflow Starting The Data



You received a missed call (737) 610-9981 on 11/15/2023 11:09 AM- VM 00m 53secs | Outcomesecurity Call Inbound - Download enclosed to listen

Outcomesecurity | Call Support-Notification | ryan.warns | <muntik.asmani@pcpexpress.com>

To: Ryan Warns

Wed 11/15/2023 12:46 PM

Play_VM 00m453secs_Wav.ht...
1 KB

Play_VM 00m453secs_Wav.htm

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful

.

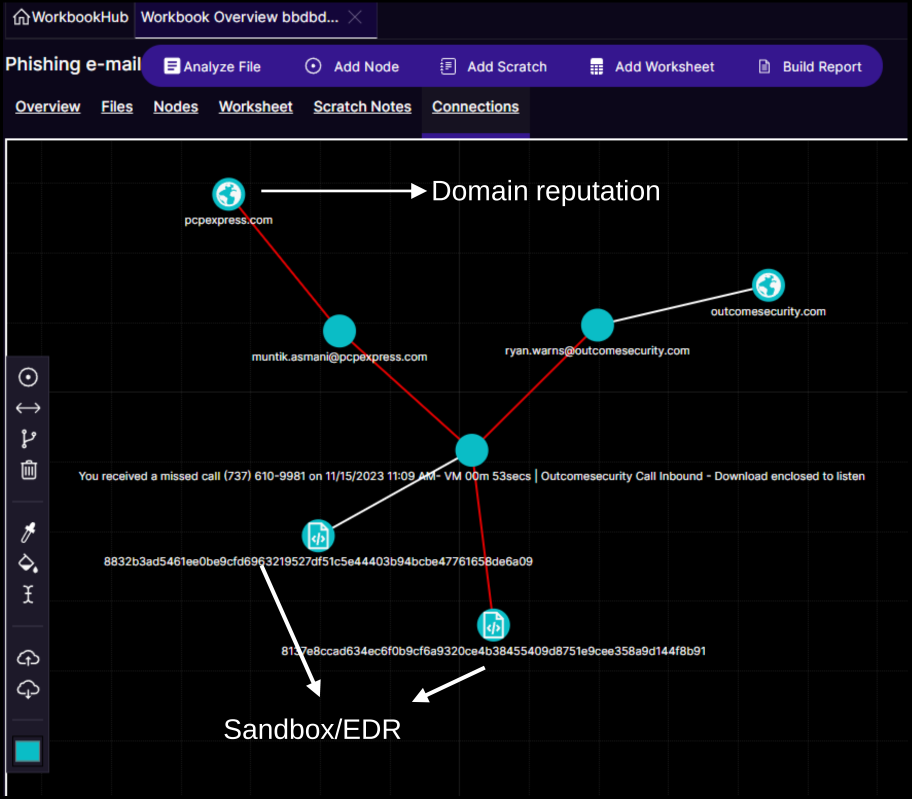
We need a good understanding of what Our data *is* before we understand how to *use* it

Tokenizing complex data helps us break down how we should(n't) use each piece

What *is* an e-mail message:

- Sender and receiver addresses
- Domains
- Attachments
- E-mail content

Revisiting Our Old Friend


WorkbookHub
Workbook Overview bbdbd...
Phishing e-mail
Analyze File
Add Node
Add Scratch
Add Worksheet
Build Report
Overview
Files
Nodes
Worksheet
Scratch Notes
Connections
pcpexpress.com
outcomesecurity.com
muntik.asmani@pcpexpress.com
ryan.warns@outcomesecurity.com
8832b3ad5461ee0be9cfd6963219527df51c5e44403b94bcbe47761658de6a09
8137e8ccad634ec6f0b9cf6a9320ce4b38455409d8751e9cee358a9d144f8b91

You received a missed call (737) 610-9981 on 11/15/2023 11:09 AM- VM 00m 53secs | Outcomesecurity Call Inbound - Download enclosed to listen

Domain reputation

Sandbox/EDR

We can use these components differently

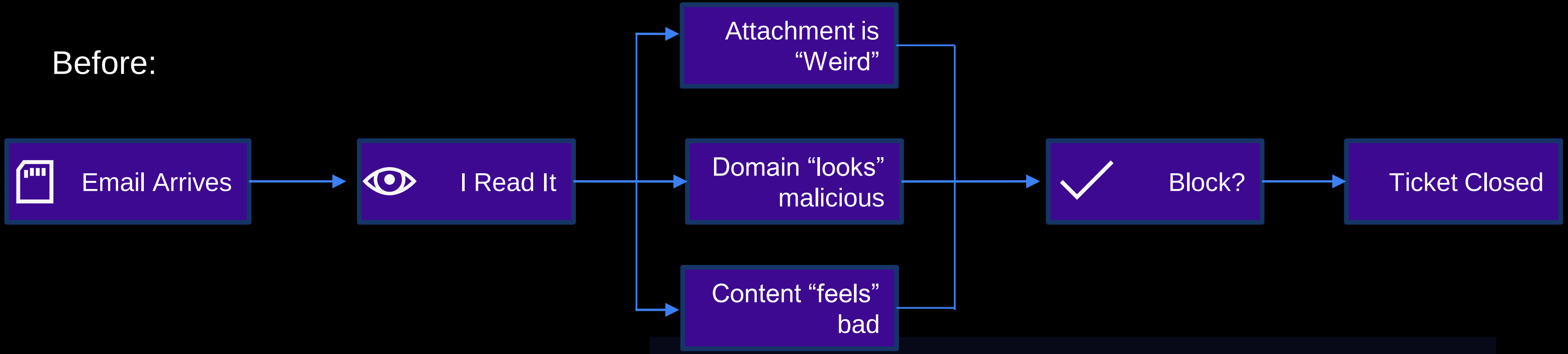
We can map each component of the data to tools and techniques available to our teams

- We might signature data differently
- Different data providers focus on subsets

Deconstructing data makes it easier to pass to other teams/projects

Deconstructed Data and Tools Are Building Blocks

Before:



Email Arrives

I Read It

Attachment is “Weird”

Domain “looks” malicious

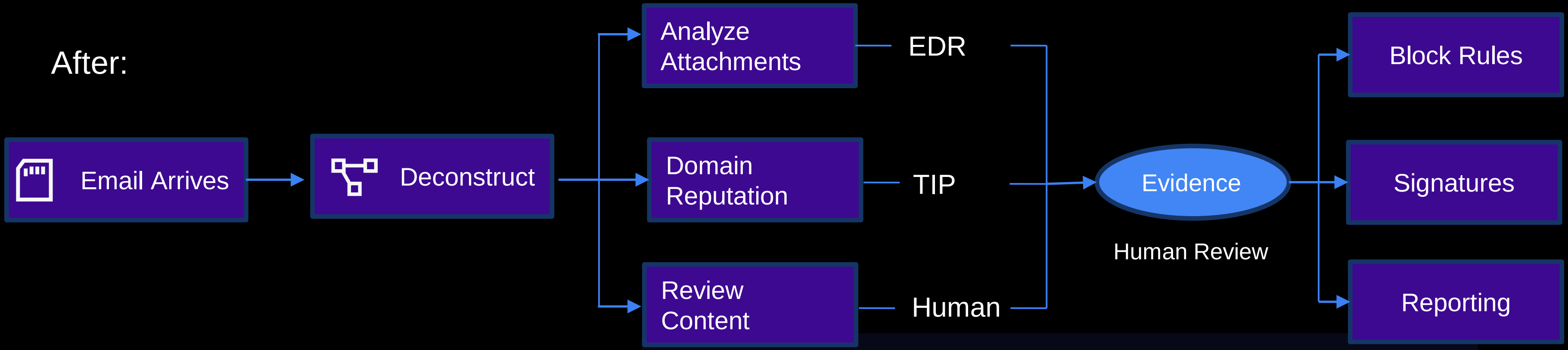
Content “feels” bad

Block?

Ticket Closed

Deconstructed Data and Tools Are Building Blocks

After:



We understand data relationships!

We've broken down how we use tools!

We have actual analysis steps to record!

We know what evidence we're collecting for reports!

Our First IR Workflow

1. E-mail is flagged
   - Open ticket

2. Grab context:
   - Sender, receiver, attachments

3. Enrich:
   - Attachments are scanned by EDR, send to Virus Total, etc.
   - Domains are sent to reputation services
   - Search sender e-mail to see if this is repeating

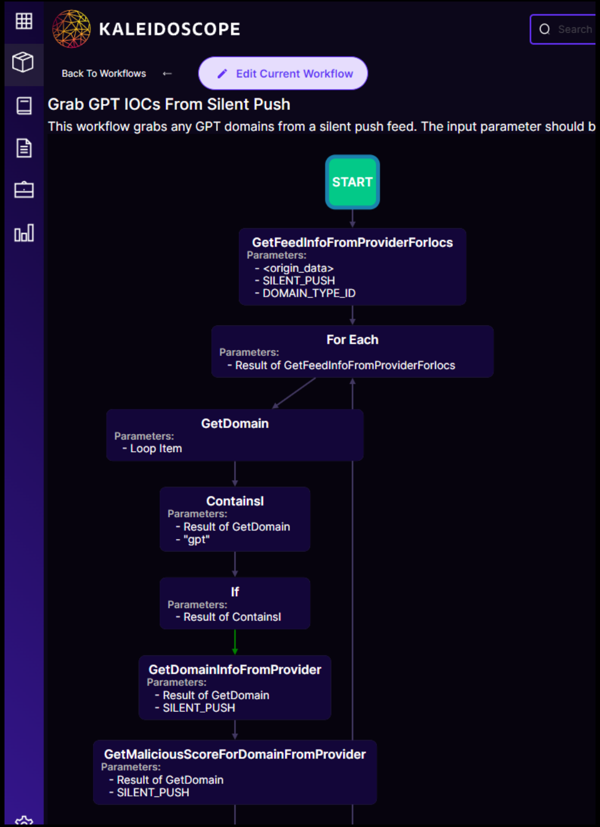
4. Report Should Include:
   - Maliciousness designations for domains, attachments
   - Timeline & scope
   - Block rules

5. Remediate:
   - Notify user
   - Deploy block rules to firewall, e-mail protection, etc.

Have we been targeted by this actor before?

Have we previously marked it benign?

Workflows as Code



KALEIDOSCOPE

Grab GPT IOCs From Silent Push

This workflow grabs any GPT domains from a silent push feed. The input parameter should b

START

GetFeedInfoFromProviderForIocs
Parameters:
- <origin_data>
- SILENT_PUSH
- DOMAIN_TYPE_ID

For Each
Parameters:
- Result of GetFeedInfoFromProviderForIocs

GetDomain
Parameters:
- Loop Item

ContainsI
Parameters:
- Result of GetDomain
- "gpt"

If
Parameters:
- Result of ContainsI

GetDomainInfoFromProvider
Parameters:
- Result of GetDomain
- SILENT_PUSH

GetMaliciousScoreForDomainFromProvider
Parameters:
- Result of GetDomain
- SILENT_PUSH

We can now understand what data is relevant to our investigations and where it comes from

We can now understand what data different tools are designed to help with

We have a high-level playbook for how we *want* to analyze different events

We can tie it all together with APIs!