CREATE YOUR CYBERSECURITY WITH OFFICE365 LOGS

"HOW CAN YOUR ORGANIZATION CREATE CYBERSECURITY VALUE FROM REGULAR OFFICE 365 LOGGING WITHOUT AZURE SENTINEL OR AN EXPENSIVE SEIM ?"

RYAN CLARK

SENIOR CYBERSECURITY ADVISORY CONSULTANT

RYAN CLARK @RYANSNOTAHACKER /TWITTER

UP FRONT

Record away. All recording of me and this presentation is approved.

All references, slides, and code will be in github after the conference.

Find me here:

@RyansNotAHacker

Github.com/ corkster919

Arabic Linguist

Network Intelligence Development

Lead Network Intel - Iraq

CyperOps Capabilities Development

Cyber Intelligence Development Instructor

Test System Engineer

Implementation Architect

Principal Security Analyst

Sr. Cybersecurity Advisory Consultant

RYAN CLARK @RYANSNOTAHACKER /TWITTER

AUDIENCE && GOALS

Intended Audiences

- 1-Person "SOC"
- Small IT + No Security
- Analyst's that have only worked in SOCs or with fancy SEIMs

Expected Goals to Meet

- Create value streams from logs
- Use Office365 json data

*for examples

GET YOUR LOGS!

So you don't have Sentinel or fancy SEIMs?

YOUR logs are still YOURS

Go get them!

Ref: Export, configure, and view audit log records - Microsoft 365 Compliance | Microsoft Docs

- Here --> https://docs.microsoft.com/en-us/microsoft-365/compliance/export-view-audit-log-records?view=o365-worldwide

```
{
  "CreationTime": "2019-09-01T22:18:05",
  "Id": "3d2e4a09-570c-416e-ddf6-08d72f7a42ec",
  "Operation": "FileAccessed",
  "OrganizationId": "d3654362-5d1f-428d-1234-ec95e74c18af",
  "RecordType": 6,
  "UserKey": "i:0h.f|membership|10033fff9889f581@live.com",
  "UserType": 0,
  "Version": 1,
  "Workload": "SharePoint",
  "ClientIP": "155.135.13.15",
  "ObjectId": "https://theplace.sharepoint.com/_catalogs/them
  "UserId": "aperson@theplace.net",
  "CorrelationId": "4f88009f-001b-9099-080b-ffb11234de99",
  "EventSource": "SharePoint",
  "ItemType": "File",
  "ListId": "5f7c1115-c19b-422b-bd6c-b1f00e4f466c",
  "ListItemUniqueId": "5e854b097-6a92-4d66-8fd7-d7adba318440"
  "Site": "175613fd-afed-4903-a878-d44df8008ead",
  "UserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) App
  "WebId": "7f50e7b8-cafc-4ca5-a19d-8600efa79a0c",
  "SourceFileExtension": "spcolor",
  "SiteUrl": "https://theplace.sharepoint.com/",
  "SourceFileName": "theme.spcolor",
  "SourceRelativeUrl": "_catalogs/theme/Themed/86DFB0FA"
}
```


LOGS CAN BE PAINFUL

"Where is there value among all these fields?"

….

"Wait, there are hundreds more fields in the Extended Options for certain operations and assets?"

Ref: Detailed properties in the audit log - Microsoft 365 Compliance | Microsoft Docs

Here --> https://docs.microsoft.com/en-us/microsoft-365/compliance/detailed-properties-in-the-office-365-audit-log?view=o365-worldwide

GOOGLE IT

- **For real, google it**

Office 365 is a massive resource that orgs use across the globe.

"Someone has already asked your question." - Me

WHAT MATTERS IS SUBJECTIVE

Determine what matters most for your organization within your Office365 environment

- Incident Response ?
- SharePoint metrics ?
- Security Alerts ?
- User Behavior Monitoring* ?

"What if they breach an Admin account?"

"What's the most active document each day?"

"Can we stop fake logins?"

"We shouldn't let regular users create new Teams."

* = Non-creepy

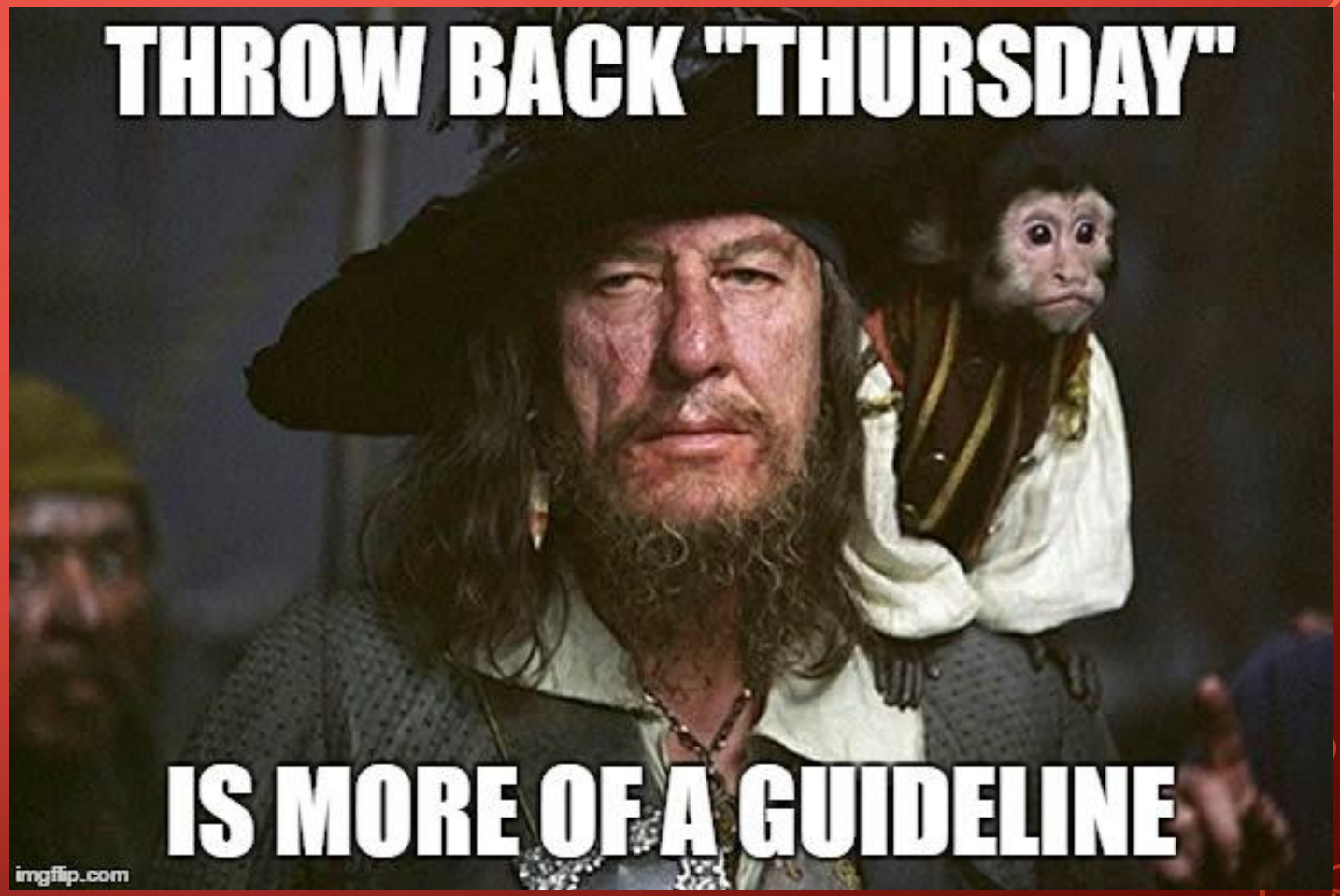
OUR EXAMPLES HERE

- Baseline your environment
  - Quick wins
  - 100% fidelity results
- Profile a User*
  - Was there a breach?
  - Did the user's conduct merit a deep look into their activity logs?
  - Do. Not. Creep. You are a professional.
- "This will never occur" alerting
  - "...but when it does, let me know about it"

METHODOLOGY

!= "WHAT"

== "HOW"



BASELINE EXAMPLES

"IS THIS ACCOUNT IN OUR ORG?"

HOW TO ANSWER

1. Find what field means "in your org"

The Microsoft docs highlight this field for "your org"

- "**OrganizationId**": "abc54362-5d1f-428d-1234-ec95e74c18af"*f*

2. Add a query to find them and create an easy tag to identify "us vs them"

BASELINE EXAMPLES (CONT)

"IS THIS ACCOUNT IN OUR ORG?"

Don't let an unknown stop you!

But what if I don't know what our org IP is supposed to be ?

- *"I bet ~99% of logs have the same id. I'd also bet that's your id."*

How do I know what the other org Ids are linked to ?

- *"That doesn't matter. Just identify 'not us' and start analyzing the other datapoints."*

BASELINE EXAMPLES (2)

"WHAT ACTIONS DO ADMINS TAKE ?"

HOW TO ANSWER

1. Find what actions mean "admin"
2. Find what groups use those actions
3. Make sure those groups are supposed to do admin stuff

BASELINE EXAMPLES (2) (CONT)

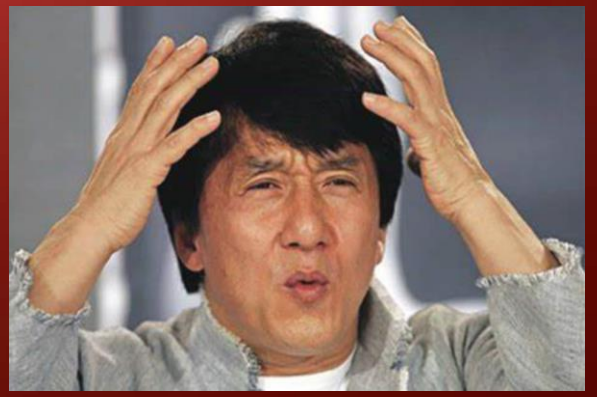
"WHAT ACTIONS DO ADMINS TAKE ?"

The items here under "**User Admin Activities**" is a good place to start.

- "Add user." ….. Do all your admins use this ? Probably not, so who does ?
- "Change user license." …. Are they able to add new software for other users ?
- "Change user password." … They didn't just reset it, they *chose* the password
- "Delete user." … Any admin using this privilege better have a good reason!

"Admin activity should be consistent and predictable!"

"But admins also test new things a lot..."



USERS DO THINGS

Sometimes you have to look up activities for a user.

"What's the value in that? " - You

"There isn't any. It's on you to create that value from the data." - Me

Break it down by key metrics

1) Physical == Geo Location by Time
2) Professional == Logins by Time
3) Activity == Operation counts per Day

Nothing is perfect. Make *simple-but-effective* your new 'good enough'.

"IT DOESN'T HAPPEN" ALERTING

What should never happen ?

Why should it never happen ?

What attacker tactic *'makes'* that happen ?

If you can answer these three questions, you can create a value-stream from your logs!

FIND THE HACKS!

Did you find a new hack thing on twitter|reddit|otherplace ?
Do you want to defend against it ?

….. NOW WHAT ?

HACKER TACTICS THAT CREATE EASY WINS

- " The program isn't supposed to do this. I just made it do this."

WHY IS THIS EASY ?

- The tester gives the security control you need in the title itself.

How do we turn this into a valuable alert?

BARE KNUCKLE BRAWL WITH YOUR LOGS

What program did they use?

- Where does it log the thing they did ?

What does the hacked attack action look like ?

- How does this appear in that log ?

What does the intended (I.e. normal, not-hacked) action do ?

- How does this appear in the log ?

LAST QUESTION

Which do you think will be the best between those two alerts ?

1. IF

does_hack(log) == "true"

2. IF

log_action_
matches_expectations(log) == "false"

TRUST YOURSELF

HAVE CONFIDENCE IN YOUR CHOICE

WRITE DOWN WHY YOU CHOSE IT

The organization that reads what you wrote down is paying you because they find your words valuable.

Trust that expectation.

EXAMPLE SCENARIO

SETTING:

You are a 22-person startup, all located in an Austin, TX office.

ATTACKER GOAL:

FIUO SharePoint Docs

ATTACKER TACTIC:

Login with credentials from new 3rd-party breach

Step 1. Identify attacker actions that leave traces.

- login attempts for users

Step 2. Find a log that matches that specific attack type.

- if you don't have one, the google does. I'd bet my house it does.

Step 3. Identify datapoints that give attribution to the attacker.

- MUST be "datapoint is 100% attacker-only"

Step 4. Identify datapoints that are "never-an-expected-datapoint" that gives attribution to NOT 'Our Org'

- Datapoint CANNOT be created by your organization or your users.

Step 5. Create a value-stream from steps 1-4.

- Also known as ADD YOUR RULES !!

RULES

**in order of greatest fidelity for incident responses*

Attacker Matches:

IF attacker_unique_datapoint_value.in(log) == "true": ALERT!

Attacker-Only Possibilities:

IF attacker_datapoint_key.in(log) AND datapoint_value.for(key) != defender_datapoint_value: ALERT!

Defender-Impossible Matches:

IF defender_datapoint_value == "A Unique Thing" AND datapoint_value.in(log) == "false": ALERT!

REAL SCENARIO

"WHALING BEC ATTEMPTS"

ATTACKER TACTIC: Added keyword matches to delete email responses that would trigger suspicion in the user after breaching the email access remotely.

Log Identified – office365 Mail logging

Find the specific logs – Update Inbox Rules

Find attacker log -- "keyword updates to rules; auto-delete 'compromise|hack|re:<this_email>|account|phish|security'

"WELL YEA OF COURSE THAT'S BAD. NOW WHAT ? "

Attacker Match – ALERT:

IF update_inbox_rules + keywords 'compromise|hack|etc'

Attacker-Only – ALERT:

IF update_inbox_rules + Non-US geo_country

Never Our Org – ALERT:

IF update_inbox_rules + IP_never_seen_before

RYAN CLARK @RYANSNOTAHACKER /TWITTER

LORDY THERE WAS REGEX

[^\.\da-zA-Z_-]+?(?<capture>[1-2^0]?[0-9]?[0-9]\.[1-2^0]?[0-9]?[0-9]\.[1-2^0]?[0-9]?[0-9]\.[1-2^0]?[0-9]?[0-9])[^a-zA-Z\.\w\+]

RYAN CLARK @RYANSNOTAHACKER /TWITTER