Making Incident Response Suck Less

Jake Williams
BreachQuest
www.breachquest.com
@BreachQuest

$whoami

- Founder and CTO of BreachQuest
- IANS Faculty, former SANS Instructor
- Former NSA Hacker, endorsed by Shadow Brokers
  - aka Russian Intelligence
- Breaker of software, responder of incidents, reverser of malware, injector of code, spaces > tabs
- **Dislikes:** those who call themselves “thought leaders,” “crypto bros,” and anyone who **needlessly adds blockchain** to a software solution

Agenda

- Collection Management Frameworks
- Establishing Incident Command Structures
- Securing Incident Communications
- Working With Breach Counsel
- Bonus (??)
  - Okay, sure, there's a bonus
  - Because of course there is…

Blatant Disclaimer

- This talk is less than an hour long and incident response is an extremely complex topic
  - Necessarily, we won't cover everything

- Some of you have pet peeves about best IR preparation tactics
  - Inevitably, I won't cover most of them
  - And some of you will be mad at me

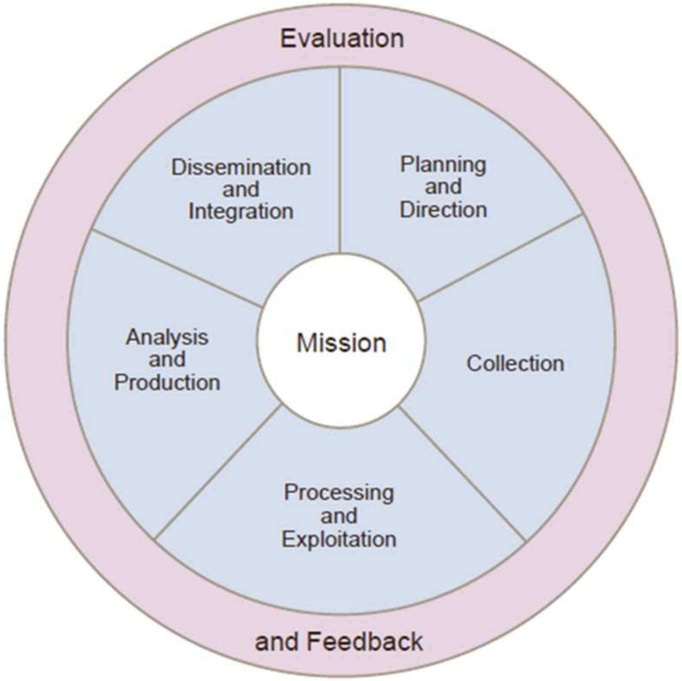
- This talk will focus on some of the ***lesser-discussed*** tactics that orgs can ***realistically*** employ

Building a Collection Management Framework

It’s an inventory – for your data sources

The Intelligence Lifecycle

- The intelligence lifecycle is a model used by most agencies to formalize the intelligence process
  - – You can’t analyze what you don’t collect
- Without a model, you’re unlikely to identify collection gaps
  - – Until those turn into intelligence gaps…
- Start with requirements, then determine the collection needed to satisfy
  - – Then identify collection gaps with a CMF!



Collection Management Frameworks

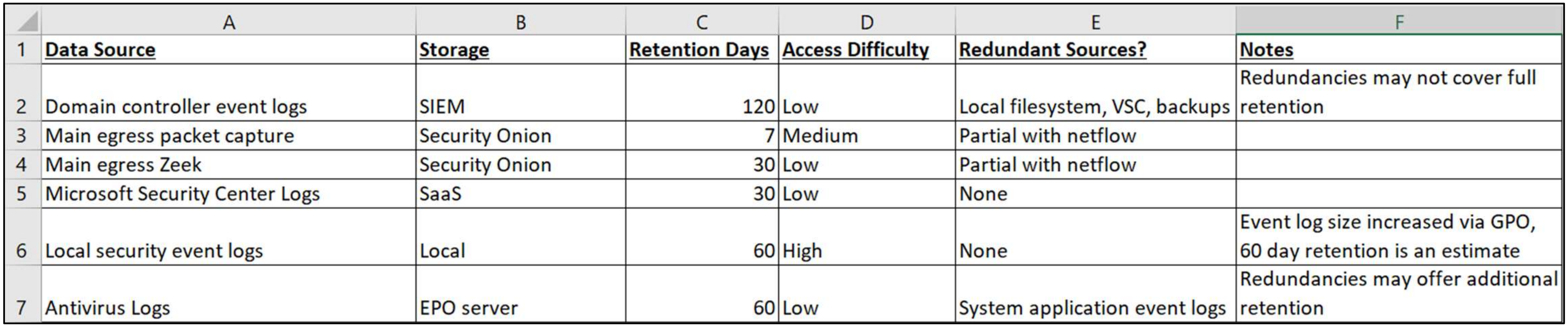
- A Collection Management Framework (CMF) is an inventory of data that is available (or can be made available) to help investigate a cybersecurity event

- The term is taken from intelligence collection to inform analysts about the types of data available to fulfill new intel requirements and balance tasking priorities

- But the term (and process) works well in incident response too

Collection Management Frameworks

- Here's the beginning of an example CMF
- If you don't have something like this, create it today
- Even if you know all your data sources, new employees and surge incident response staff won't



	A	B	C	D	E	F
1	**Data Source**	**Storage**	**Retention Days**	**Access Difficulty**	**Redundant Sources?**	**Notes**
2	Domain controller event logs	SIEM	120	Low	Local filesystem, VSC, backups	Redundancies may not cover full retention
3	Main egress packet capture	Security Onion	7	Medium	Partial with netflow	
4	Main egress Zeek	Security Onion	30	Low	Partial with netflow	
5	Microsoft Security Center Logs	SaaS	30	Low	None	
6	Local security event logs	Local	60	High	None	Event log size increased via GPO, 60 day retention is an estimate
7	Antivirus Logs	EPO server	60	Low	System application event logs	Redundancies may offer additional retention

Justifying a Collection Management Framework

- There are numerous benefits to implementing a CMF:
  - Using a CMF quickly identifies collection gaps
  - Auditors love knowing you have a plan and a CMF **is** a plan
  - You might know what your collection looks like, but new employees and surge incident response staff don't
  - A CMF makes sure you know what you **don't** have so investigators don't wait for "best evidence"
  - Combatting the "blinkenboxen effect" is easiest with a CMF
  - Collection gaps are the #1 reason that incident responders fail to identify the source of an intrusion
    - Did we mention identifying collection gaps?

Establish Incident Command Structures

Chain of Command Matters

Mea Culpa

- Despite almost 18 years in the military and intelligence community, when the term “incident commander” came into common usage, I **hated** it

- Like there are not words for how much I hated it
- That was dumb
- Yeah… I was wrong

Building an Incident Command Structure

- Identify an incident commander who is ultimately responsible for ensuring incident communication and coordination occurs

- If the incident investigation is running 24x7 (or extended hours in general), identify lieutenants/deputies to support the incident commander so they can take breaks
  - Even in smaller investigations, at least one lieutenant should be appointed to facilitate coordination while the incident commander is inevitably busy briefing stakeholders

Set Expectations on the Team

- All high-level tasks will be directed by the incident commander, but implementation details are generally left to practitioners
  - e.g., “analyze server X for IOCs” but not detailing how
- Explain that if the incident commander told you to do X, don’t rabbit hole working on Z
  - This applies even if you think Z is more important
  - Priorities can change, but before acting unilaterally - discuss

- For those who served in the military, this won’t be difficult
  - For infosec peeps used to more autonomy, it sometimes (often) is

Securing Incident Communications

Oh boy is this one contentious…

Secure Communications Matter

- If it’s on a tee shirt, it’s probably happening

Is This Really Happening?

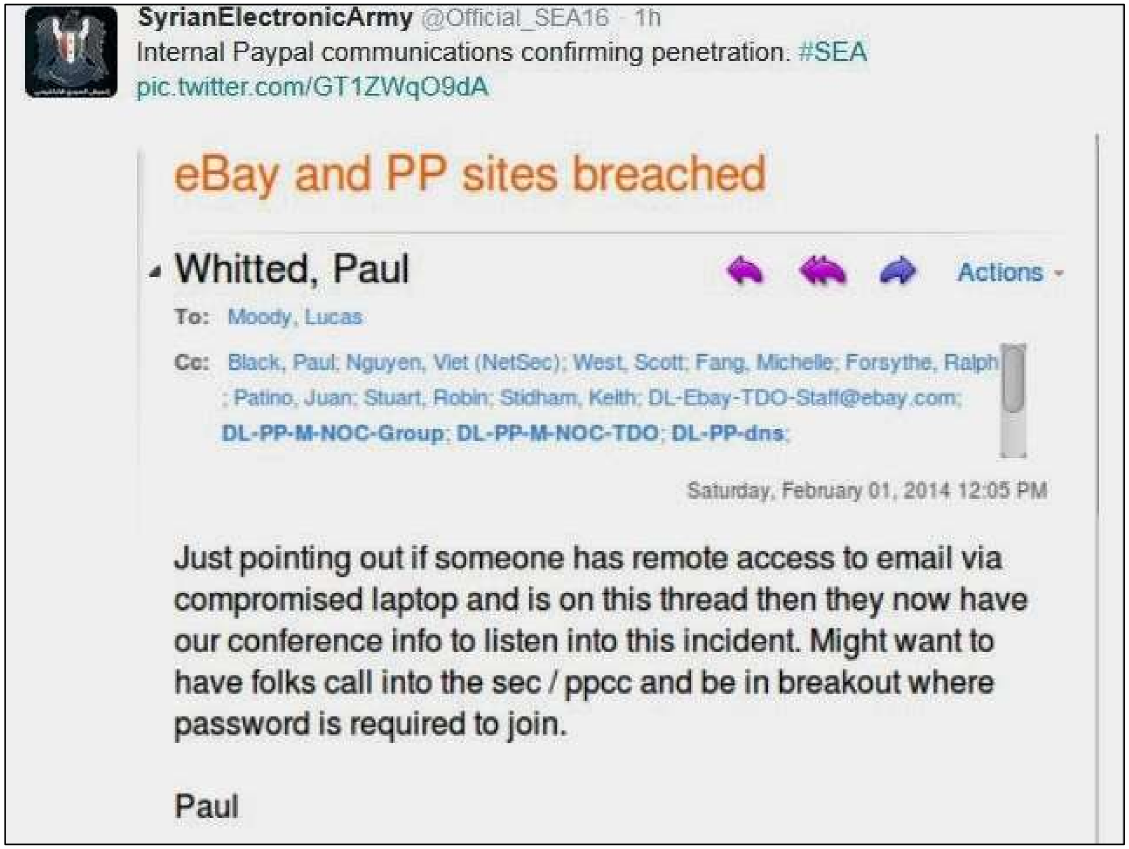
- Oh yeah, it’s DEFINITELY happening

- I can point to multiple incident response remediations that we got to repeat (in one case several times) because the threat actor was watching us plan

- An incident need not be a resume updating event
  - But a failed remediation usually is…

Then There's This…

- You don't want to be in this situation…



SyrianElectronicArmy @Official_SEA16 · 1h
Internal Paypal communications confirming penetration: #SEA
pic.twitter.com/GT1ZWqO9dA

eBay and PP sites breached

Whitted, Paul

To: Moody, Lucas

Cc: Black, Paul; Nguyen, Viet (NetSec); West, Scott; Fang, Michelle; Forsythe, Ralph; Patino, Juan; Stuart, Robin; Stidham, Keith; DL-Ebay-TDO-Staff@ebay.com; DL-PP-M-NOC-Group; DL-PP-M-NOC-TDO; DL-PP-dns;

Saturday, February 01, 2014 12:05 PM

Just pointing out if someone has remote access to email via compromised laptop and is on this thread then they now have our conference info to listen into this incident. Might want to have folks call into the sec / ppcc and be in breakout where password is required to join.

Paul

How to Secure Incident Communications

- We often stand up a new tenant in GSuite for this
  - A domain not related to the victim is newly registered and accounts for those involved in the investigation are provisioned
  - Don’t skimp on licensing, you want eDiscovery and GDrive logging
- You can use MSFT too, but I’ve found the process to be more difficult and MSFT collaborative document editing is **horrible**
- Some organizations also want a dedicated Slack tenant
  - Slack is a bit more of a pain to configure for capturing all communication, especially private messages

Benefits of GSuite

- If desired, email can be limited to inside the domain
- Chat and conferencing functionality are built-in
- Mandatory MFA for everyone!
- Collaborative document editing makes reporting easier
- Google Drive can handle most evidence storage requirements
- Full auditing (at higher license levels)
- Takeout at the end of the investigation retains all data for the domain, simplifying many eDiscovery tasks
  - Because you know, litigation…

Tactical vs. Strategic (aka Just Because You Can…)

- I used to do tactical work and we didn’t always use encrypted comms in the field
  - We used them when they mattered
- But isn’t it always better to be secure?!
  - Sure, but if it hinders your ability to operate, then maybe it’s the wrong time to be stressing over OPSEC
- When you first engage in the incident, coordination over potentially insecure channels is usually better than waiting for secure channels to be fully established

Working With Breach Counsel

What do you call a bus full of lawyers driving off a cliff?

First, Check the Lawyer Jokes At The Door

- Most breach counsel have heard every lawyer joke there is
  - What sounds clever to you is likely coming off old and tired (**at best**) to breach counsel
- Sort of like when someone says:
  - "You mean Jake from State Farm?"
  - "Are you wearing khakis?"

Breach Counsel Are Incident Response **EXPERTS**

- Breach counsel (not in-house counsel, those whose dedicated practice area is **breach response**) know more about the mechanics of incident response than you do
  - Listen to them
  - Seriously
  - They are the experts
- You might have done IR once or twice
  - They **LIVE** it…

Breach Counsel Are NOT Investigators

- While breach counsel are experts in what needs to be done for incident response, they are usually not experts in the technicalities of performing digital forensic investigations
  - Clarify whether directives from breach counsel are specifying a method or a desired outcome
  - Are you telling me you need this question answered or directing how specifically it should be answered?
- Don't pretend breach counsel have no idea about the technical side either – I like to think of them like the IT project manager
  - They can't build a server, but know a LOT about the process

Breach Counsel Doesn’t Work For Your Insurer

- Breach counsel is typically recommended by your insurer and in most cases, you’ll pick from a list
  - But your org will retain breach counsel directly
- Breach counsel (typically? always?) cannot speak on behalf of the insurer, but can offer advice about how the insurer will handle or interpret a situation
  - But this is no more a guarantee than a lawyer explaining what they believe a jury will do in a particular situation
- Accusing breach counsel of being a shill for the insurer is always a losing move – don’t do it

A Lawyer, But Not Your Lawyer…

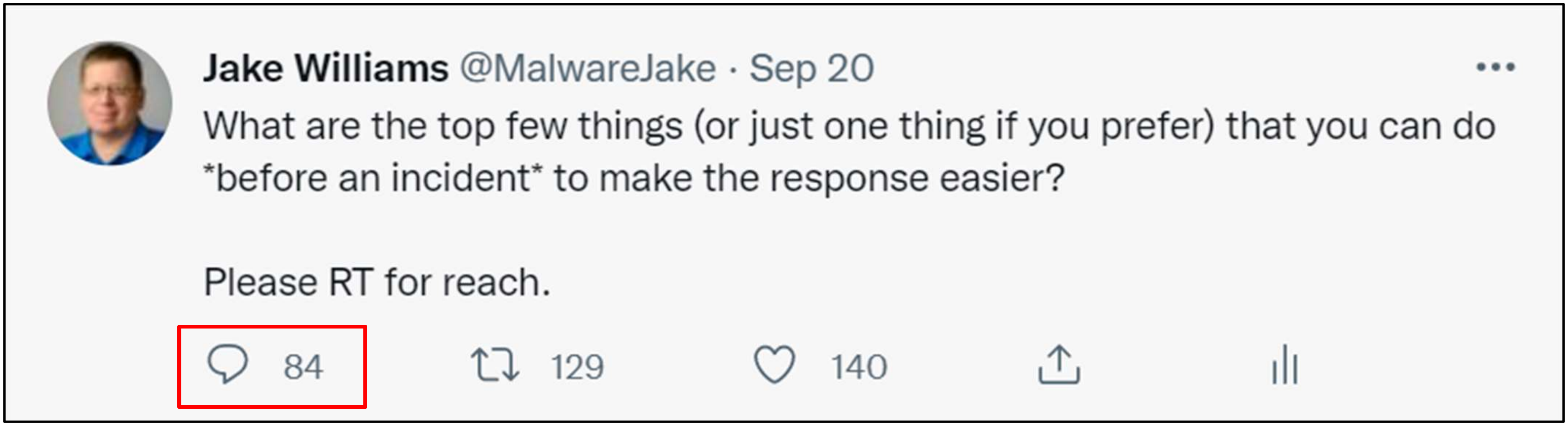
- Breach counsel works for the organization, not you
  - This shouldn't need to be said (and yet it does), but don't ask breach counsel for legal opinions on matters not directly related to the IR
  - Especially for personal matters (duh)
- If you think you may have personal liability in an incident, remember that breach counsel **<u>does not represent you</u>**
  - Or your interests
- The easiest way to figure out whose interests a lawyer is looking out for is to look at who is paying the bill
  - If it's not you, I have some uncomfortable news…

Bonus!!!

Because I **KNOW** I’m not the smartest person in the room…

Phone a Friend (Or 90,000 Friends…)

- So I did a thing…
  - https://twitter.com/MalwareJake/status/1439942963858223106

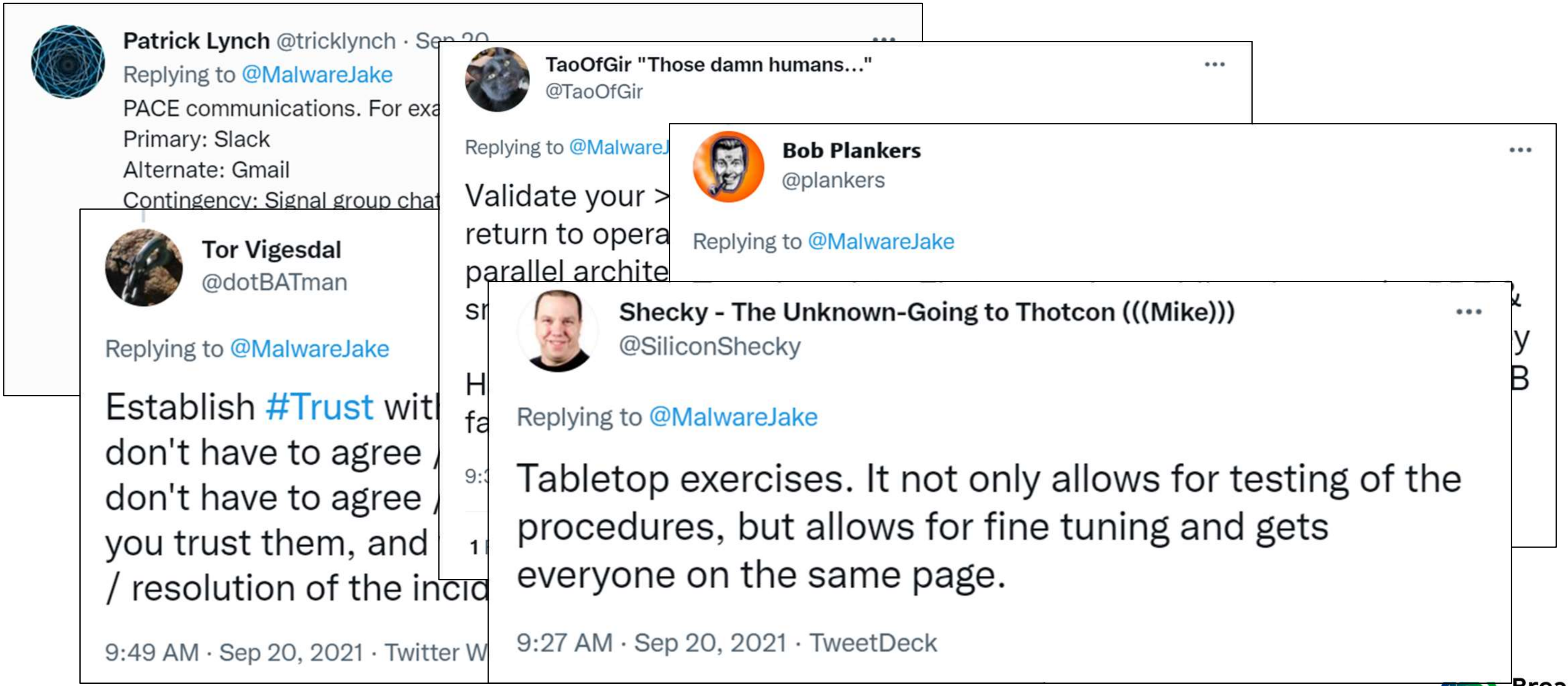


Jake Williams @MalwareJake · Sep 20

What are the top few things (or just one thing if you prefer) that you can do *before an incident* to make the response easier?

Please RT for reach.

So Many Awesome Responses



Patrick Lynch @tricklynch · Sep 20
Replying to @MalwareJake
PACE communications. For exa
Primary: Slack
Alternate: Gmail
Contingency: Signal group chat

TaoOfGir "Those damn humans..."
@TaoOfGir
Replying to @MalwareJ
Validate your >
return to opera
parallel archite
sr
H
fa
9:
1

Bob Plankers
@plankers
Replying to @MalwareJake
&
y
B

Tor Vigesdal
@dotBATman
Replying to @MalwareJake
Establish #Trust wit
don't have to agree /
don't have to agree /
you trust them, and
/ resolution of the incid
9:49 AM · Sep 20, 2021 · Twitter W

Shecky - The Unknown-Going to Thotcon (((Mike)))
@SiliconShecky
Replying to @MalwareJake
Tabletop exercises. It not only allows for testing of the procedures, but allows for fine tuning and gets everyone on the same page.
9:27 AM · Sep 20, 2021 · TweetDeck

Closing Thoughts

- Setting expectations up front can make your incident response suck **significantly** less
- Most incident response preparation focuses on increasing visibility and building IR plans
  - That's important – definitely start there
- But preparation is about more than just technical
  - Set expectations before the incident
- Setting expectations for how IR team members will interact is just as important
  - Maybe even more so…

Jake Williams

@MalwareJake

@BreachQuest

BreachQuest

breachquest.com