



Help! We Need an Adult!

Engaging an External IR team

Liz Waddell, Incident Commander, Talos Incident Response

July 17, 2020

Speaker Background



Liz Waddell



Incident Commander, Talos Incident Response



Professional consultant leading incident response engagements along with years of experience helping companies do IR better.



Located in Dripping Springs, Texas (not Austin.)



Crazy cat owner.



Agenda

1

Engaging an IR Firm

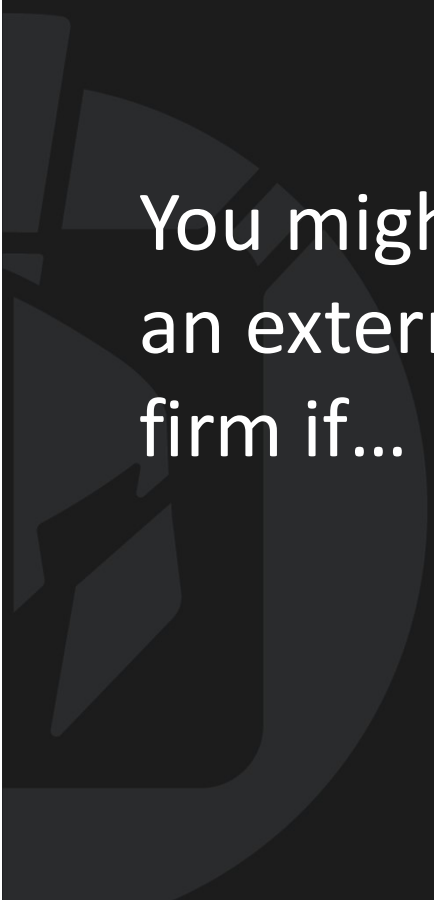
2

Scoping an Engagement

3

Deploying the Engagement

Engaging an IR Firm



You might need an external IR firm if...

Your Incident Response Plan should guide you in determining when you need to ask for help. But when should that be?

- To confirm what you know
- To determine what you don't know
- If there is the potential for litigation
- If you are going to invoke your cyber insurance policy
- To leverage someone else's expertise
- To alleviate your tired analysts
- To get written findings
- To get someone your C-Suite will listen to
- To learn to get better
- You just need help

But who should I choose?

- Reputation (www.lmgty.com)
- References
- Marketplace Analysts (Gartner, IDC, Forrester)
- Previous partnerships
- Infrastructure
- Cost (Tech fees? Travel?)

“The main reasons to choose a provider is their technical acumen, reputation for security technology, security operational management, and threat visibility.” - **IDC MarketScape**

SOURCE: "IDC MarketScape: U.S. Incident Readiness, Response, and Resiliency Services 2018 Vendor Assessment, Beyond the Big 5 Consultancies" by Christina Richmond and Pete Lindstrom, September 2018, IDC # US44257117

One Time Engagement

Pros

- No commitment
- One-time purchase
- May work for those who have limited funding

Retainer

Pros

- Guaranteed Service Level Objectives
- Understanding of expectations
 - Terms and conditions
 - Technology
 - Legal
 - Cyber Insurance
- Opportunity to build relationships
- Variety of service packages available (including proactive services)

Scoping the Engagement

First the Incident Overview



Explain your capabilities

People



- Information security team members
- Network team
- System admins
- Desktop support
- Application specific subject matter experts
- Disaster recovery
- Legal team
- PR/Communications

Process



- Incident Response Plan
- Crisis management plan
- Disaster recovery
- Business continuity plan

Technology



- Backup technology
- Network detection capability
- Centralized logging
- Endpoint security



Determine Your Objectives!



Root Cause?



Data Exfiltration?



Lateral Movement?



Containment, Eradication & Recovery?



Determine Communications



Key Contacts - Is there a dedicated person coordinating Incident Response efforts?



Cadence - Daily updates? Open bridge?



Method - Out of band, Chat apps, Encrypted email, Secure Document Exchange



Determine Access



VPN Access, remote system, or other, and any credentials needed to access systems



Security tool access (IDS, logs, endpoint security consoles)



Access and Address of Facility, Best access airport and hotel



Security badge, escort concerns and procedures



Background check or security clearance needed



Legal Considerations

(Not a lawyer, Not Legal Advice)

- To help preserve privilege, it is recommended legal counsel be involved for any cyber related incident.
- If personal data is potentially involved or for internal investigations, it recommended that counsel engage directly with the IR firm.
- This may influence how communication occurs (e.g. all communications flow through counsel).

Preserve Privilege?

Check with your counsel, but consider...

- How/through whom should you communicate?
- Internal/External Counsel?
- Written/Oral Communication?
- How should written communications be marked ?

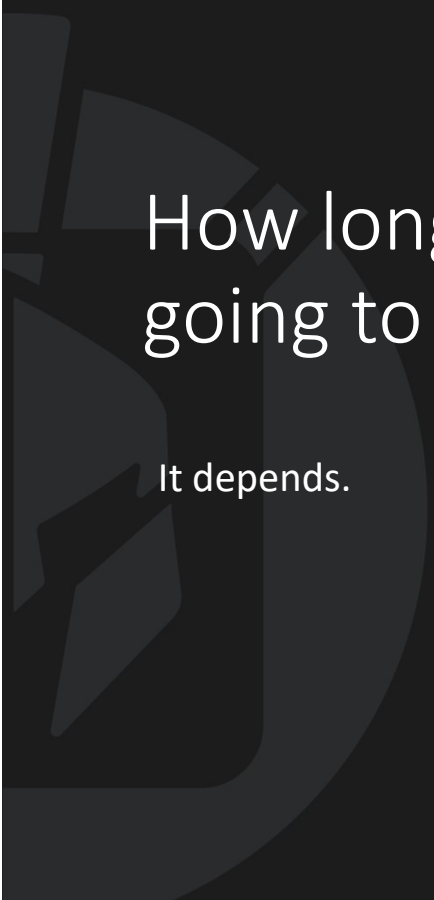
Cyber Insurance

Proactively connect the insurer and the IR firm if possible, to ensure a smoother interaction if the time comes.

- Preferred vendors (pre-negotiated rates)
- Approval for non-preferred vendors
- When do you give notice?
- How do you give notice?
- What data needs to be captured? (e.g., costs, expenses, labor)
- Policies generally only cover emergency related costs but could include:
 - Data loss or destruction
 - Forensics
 - Loss of Income
 - Extortion Costs (Ransomware/DDOS)
 - Notification Costs
 - Privacy Regulation
 - Credit monitoring
 - Public Relations
 - Legal Costs
 - Crisis management

The Engagement





How long is this going to take?

It depends.

The quicker tools can be deployed, and evidence collected, the faster this can go; however:

- This is a marathon, not a sprint.
- Prepare your stakeholders that recovery can take time.
- While the goal is to get things up and running, rushing can mean mistakes or tipping off adversaries (and then you must start all over again)

Prepping for the (virtual) arrival..



Preservation of evidence



Segmenting affected systems if possible



Begin initial data collection

We have come for your evidence

An IR firm cannot determine what happened without evidence. The more data there is to look at, the better chance you have of getting answers.

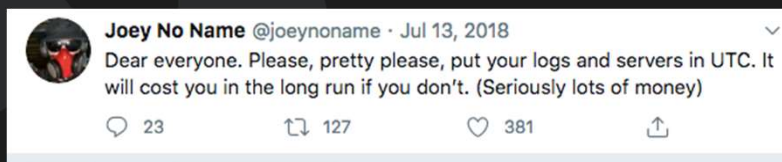
- Collection through tool deployment
- Access to SIEM and technology stack
- Forensic image collection
- Script deployment
- File collection
- Log collection

Tool Deployment

The tools deployed will vary by vendor; however, successful deployment for any relies on preparation.

- Know your assets. Who can identify critical/key systems?
- Know your network, especially ingress/egress points.
- What are your emergency change management requirements?
- Can you push agents/software (SCCM, etc.)?
- System requirements?
- Network requirements?

Logs, logs, logs



- Are logs forwarded into a centralized utility (e.g., SIEM)?
- Are logs stored locally?
- Are logs stored in the cloud? Can you access them?
- What is your data retention policy?
- Are you logging in UTC or local time?
- Are the logs time synchronized using NTP?

The Network

Know your current capabilities
and your visibility gaps.

- Do you have a network assets list?
- Do you have network diagrams?
- Do you have packet capture capabilities?
- What network logs are you keeping?
 - NetFlow (ingress and egress traffic, internal to internal traffic)
 - DNS logs (query/transfer, client requests, answers/responses, zone transfers)
 - DHCP logs (ability to map leased IP addresses and corresponding host names)
 - Firewall logs
 - Network device logs (routers, switches, etc.)
 - IDS logs and alerts (Internal and Perimeter)
 - Proxy logs
 - VPN connections (user, source and destination IP, etc.)
 - Corporate Email connections
 - Cloud connections

Endpoints and the Users

Know your current capabilities and your visibility gaps.

- Do you have an asset list for your Servers and Workstations?
- What OS and versions are your endpoints?
- Do you have any AV/EDR solutions? What is the coverage?
- Are there any remote access applications used in the environment?
- What type of logs are you collecting?
 - Authentication (success and failures)
 - Authorization changes
 - Service (startup, shutdown, and status change)
 - User account creation
 - PowerShell
 - Changes to privilege
 - Adding or deleting tokens
 - Use of administrative privileges
 - Access to regulated or confidential data
 - Encryption key changes
 - Creating or deleting system level objects
 - Application events

But why?

Example of partial evidence collection for an Emotet investigation

Tactic	Technique	Artifact	Tool
Initial Access	Spear phishing	Email (clients, archives) Email Gateway Email server logs Cloud email logs	Email Gateway Console/Logs
Credential Access	Brute Force	Windows Security Logs	Skadi/Event Log Explorer/ELK/Splunk
	Credential Dumping	PowerShell Logs	EVTXExplorer (EVTXCmd)
	Local Administrator account compromise usage	Azure Account Config/Security Log	RegCmd, RegRipper
	Credentials in Registry	MFA system logs	Volexity Surge/Volcano (Volatility)
	Credentials in Files	Windows Registry	GREP/AWK/SED
Program Execution	Local Job Scheduling	Windows Event Logs	Timeline Explorer
	Scheduled Tasks	EDR/AV	Binary analysis tool
	Process Injection	Sysmon	Skadi/Event Log Explorer/ELK/Splunk
	PowerShell	Memory/Pagefile	EVTXExplorer (EVTXCmd)
	Service Execution	Shim/AmCache	X-Ways



Containment and Eradication


Something which should be determined at the onset of an engagement is if there will be hands on keyboards to facilitate containment and eradication or if another partner needs to be engaged.

- Can you do a password reset? Enterprise wide? Local? Service Accounts? Don't forget the golden ticket.
- What if your domain was compromised? How would you rebuild your DCs?
- Can you create isolated networks?
- Vulnerability/Patch management?
- Blocking at the perimeter?
- How are you communicating what is happening?

Recovery

Getting back to business is the goal, but it cannot happen until containment and eradication is done.

- Do you have backups? Are they secure? How far back can you go?
- Leverage Business Continuity/Disaster Recovery Plans if possible.
- Get plans in place for monitoring and long-term improvements.



Post-Incident Activities

Are we done yet?

- Do you have a process to remove deployed agents/software?
- Is there a need for evidence retention?
- Reports should guide you through the incident. Good reports should help you determine strategies to prevent the incident from happening again.
- Are you sharing your report with others? Consider privilege.
- Are you sharing your IOCs and experience with the security community?

Thank
you!



TALOS
INCIDENT
RESPONSE



blog.talosintelligence.com



[@talossecurity](https://twitter.com/talossecurity)



IncidentResponse@cisco.com



Email Contact
IRSalesSupport@cisco.com

Twitter
[@vlsin](https://twitter.com/vlsin)
[@talossecurity](https://twitter.com/talossecurity)

White papers, articles & other information
talosintelligence.com

CTIR Sales Information
go2.cisco.com/CTIRSales

Instructional Videos
cs.co/talostube

Beers with Talos Podcast
talosintelligence.com/podcasts