exterro inform VIRTUAL CON

What Actually Matters in the First 60 Minutes of DFIR Triage

Exterro Inform 2026

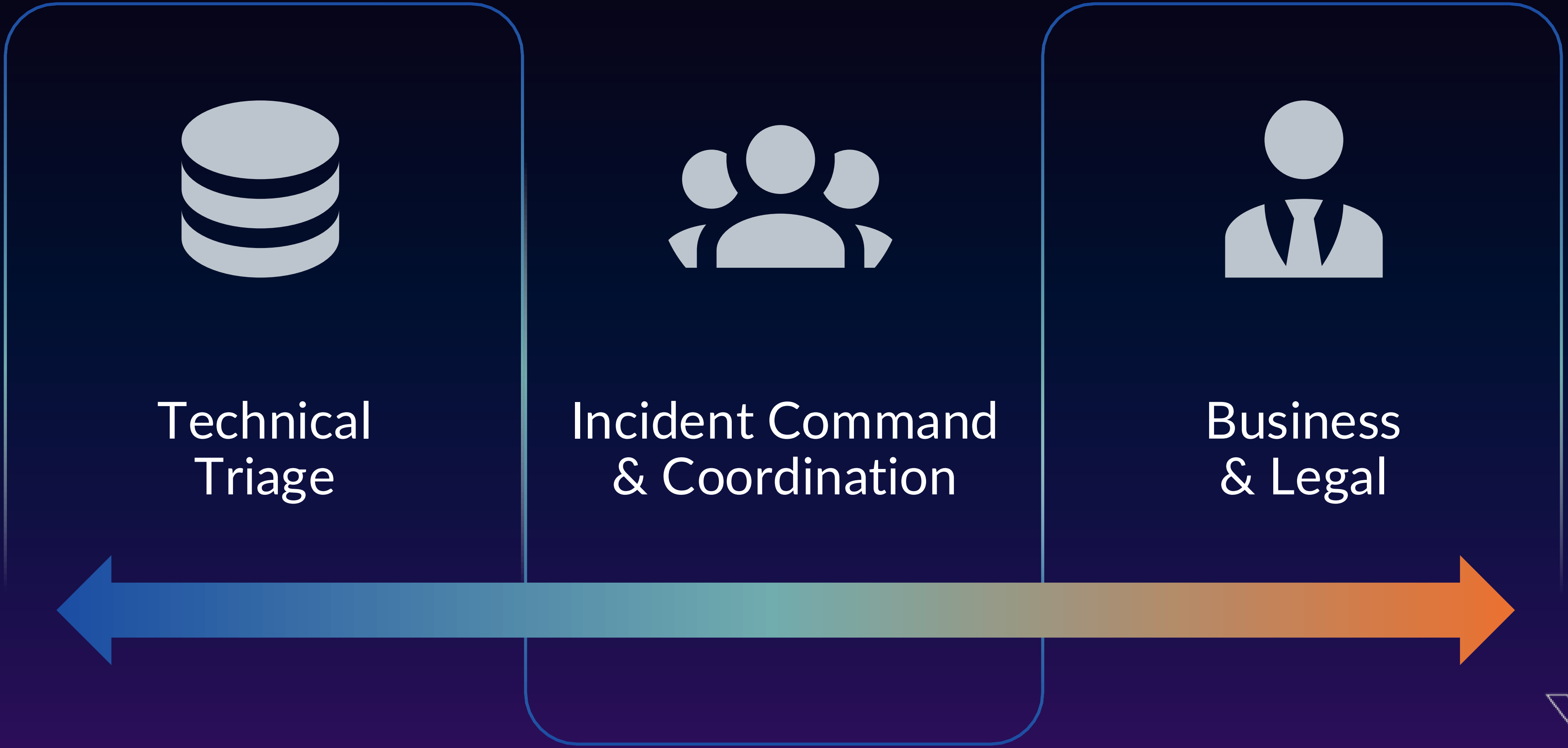
17th March 2026

- ✓ The Three DFIR Workstreams
- ✓ Identification & Containment
- ✓ Evidence Preservation
- ✓ Challenges & False Assumptions
- ✓ The “First-Hour Playbook”
- ✓ First Hour Narrative & Takeaways

exterro inform VIRTUAL CON

DFIR Workstreams

Understanding what's known



Technical Triage

Incident Command & Coordination

Business & Legal

Identification

Common Challenges

Hesitation

- *False positive?*
- *Noisy detection?*
- *Spin up the IRT?*

Premature certainty

- *Just one endpoint*
- *Just commodity malware*
- *Just a careless user*

Identification

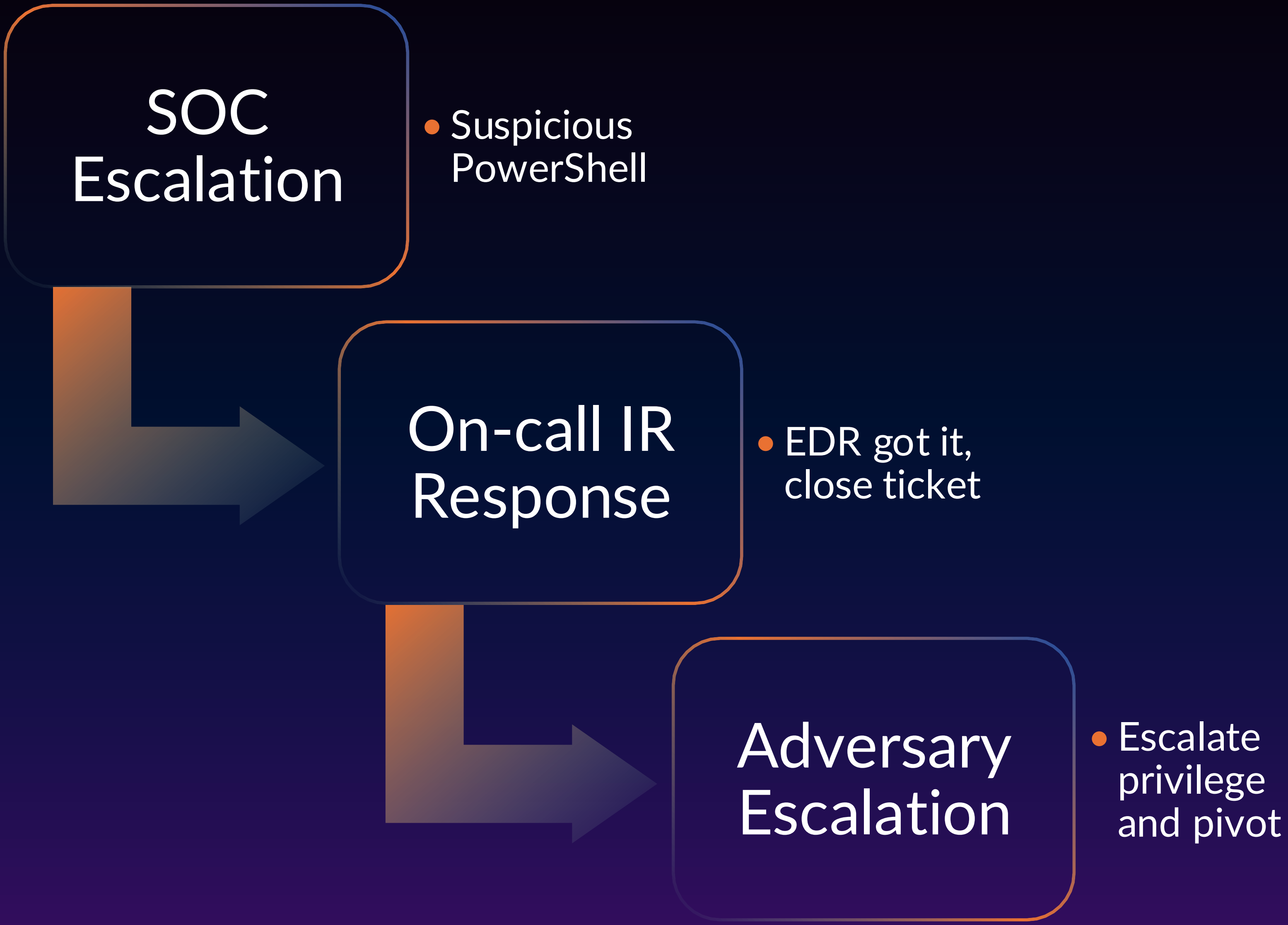
Modern Solutions

- Rapid confirmation with multiple independent signals → early decision to activate & triage
- At this stage, facts ≠ full root cause
- Do we have:
  - *Corroborating telemetry? Abnormal behaviour?*
  - *Persistence? Lateral movement?*
  - *Data access patterns / baseline?*

- Initial conditions
  - *What was reported?*
  - *When it was reported*
  - *Who saw what?*

exterro inform VIRTUAL CON

What Usually Unfolds



SOC Escalation

- Suspicious PowerShell

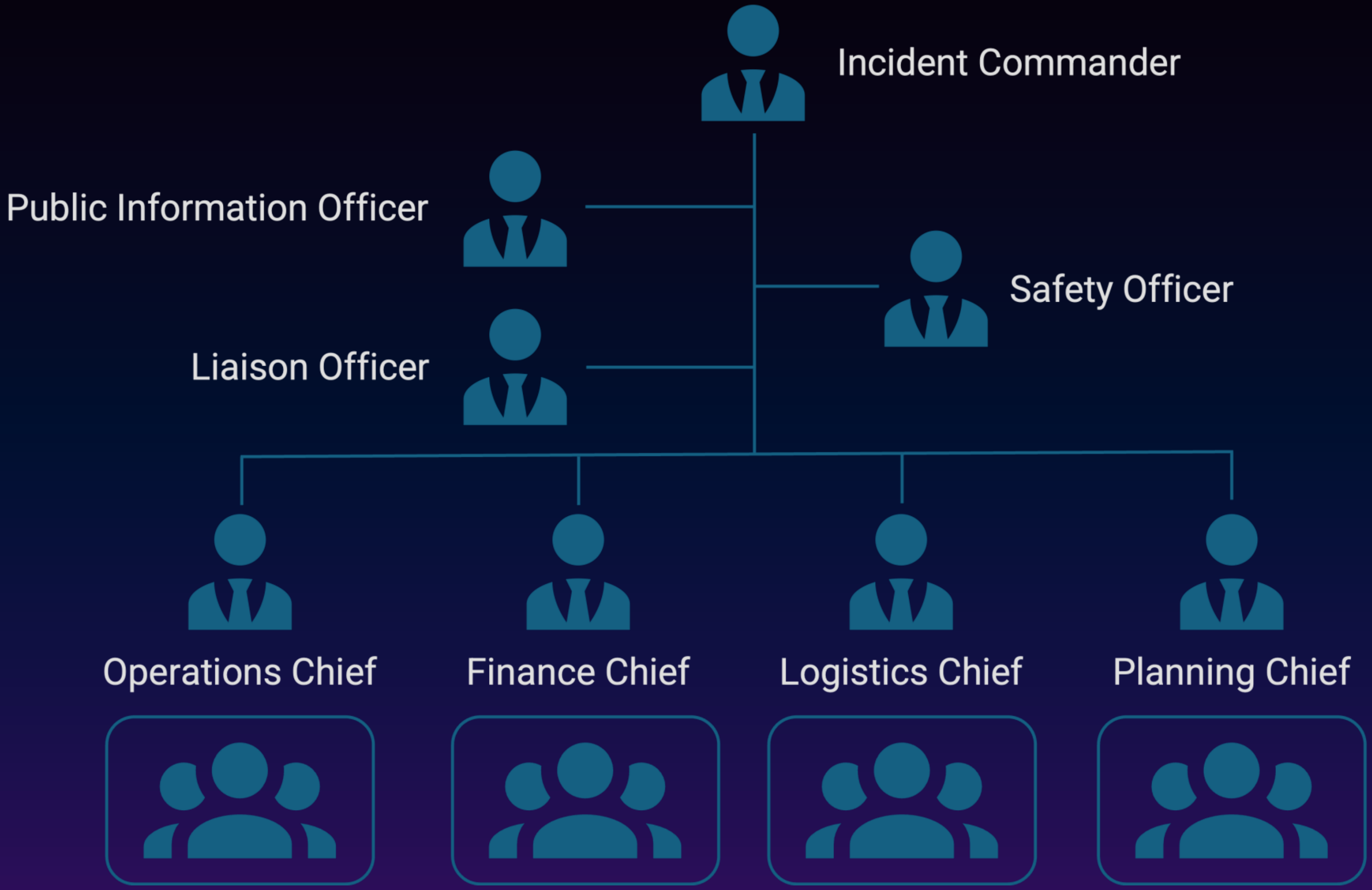
On-call IR Response

- EDR got it, close ticket

Adversary Escalation

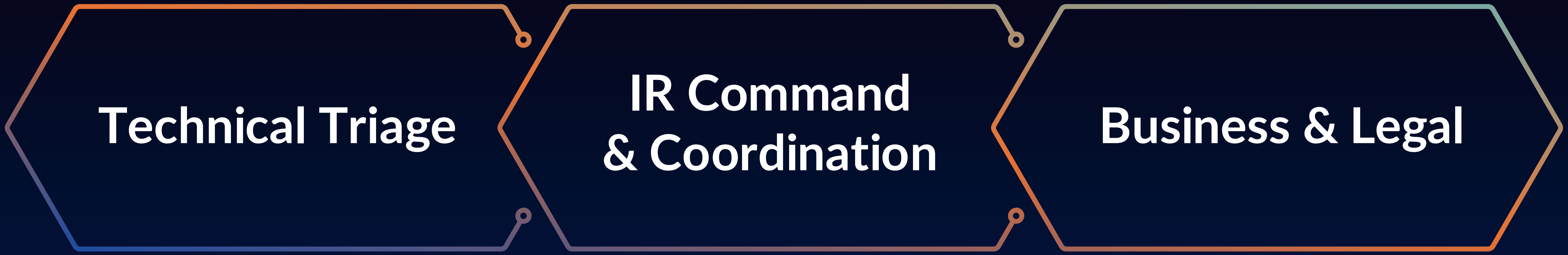
- Escalate privilege and pivot

Incident Command System



DFIR Workstreams

Who's Involved



Technical Triage

- *IT Operations*
- *IR MSSP*

IR Command & Coordination

- *Incident Lead*
- *Incident Responders*

Business & Legal

- *CISO / CIO*
- *Legal Counsel*
- *Insurer*
- *Regulator*

exterro inform VIRTUAL CON

Containment

Blunt Force

- Pull the plug
- Reboot
- Wipe
- Rebuild

Incomplete Information

- Improper isolation
- Isolation too much / too little
- Too few controls

exterro inform VIRTUAL CON

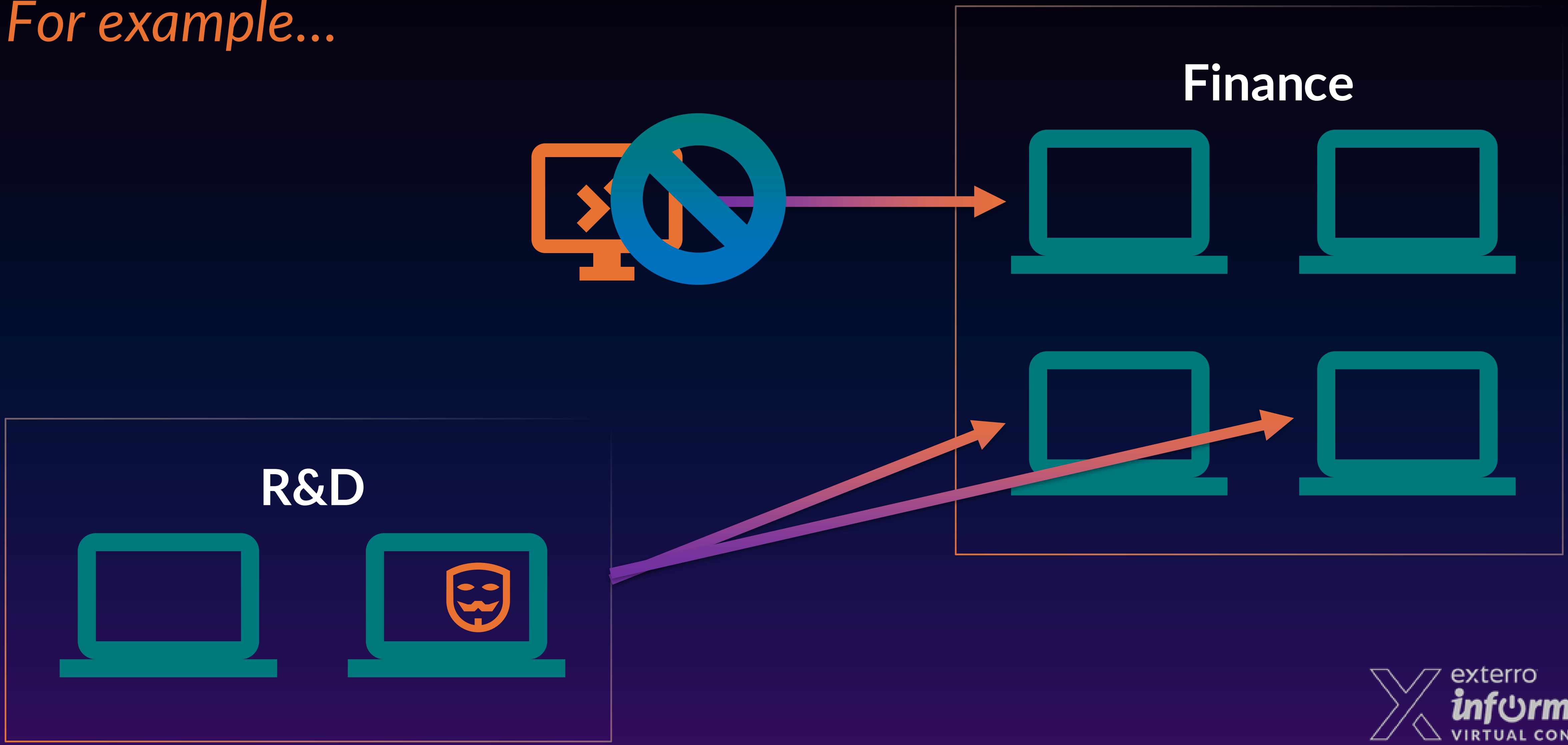
Containment

In the first hour

- Stabilisation, not eradication
- Quarantine VLAN, firewall East / West traffic
- Don’t tip your hand
- Make good choices
- Document, document, document

Containment

For example…

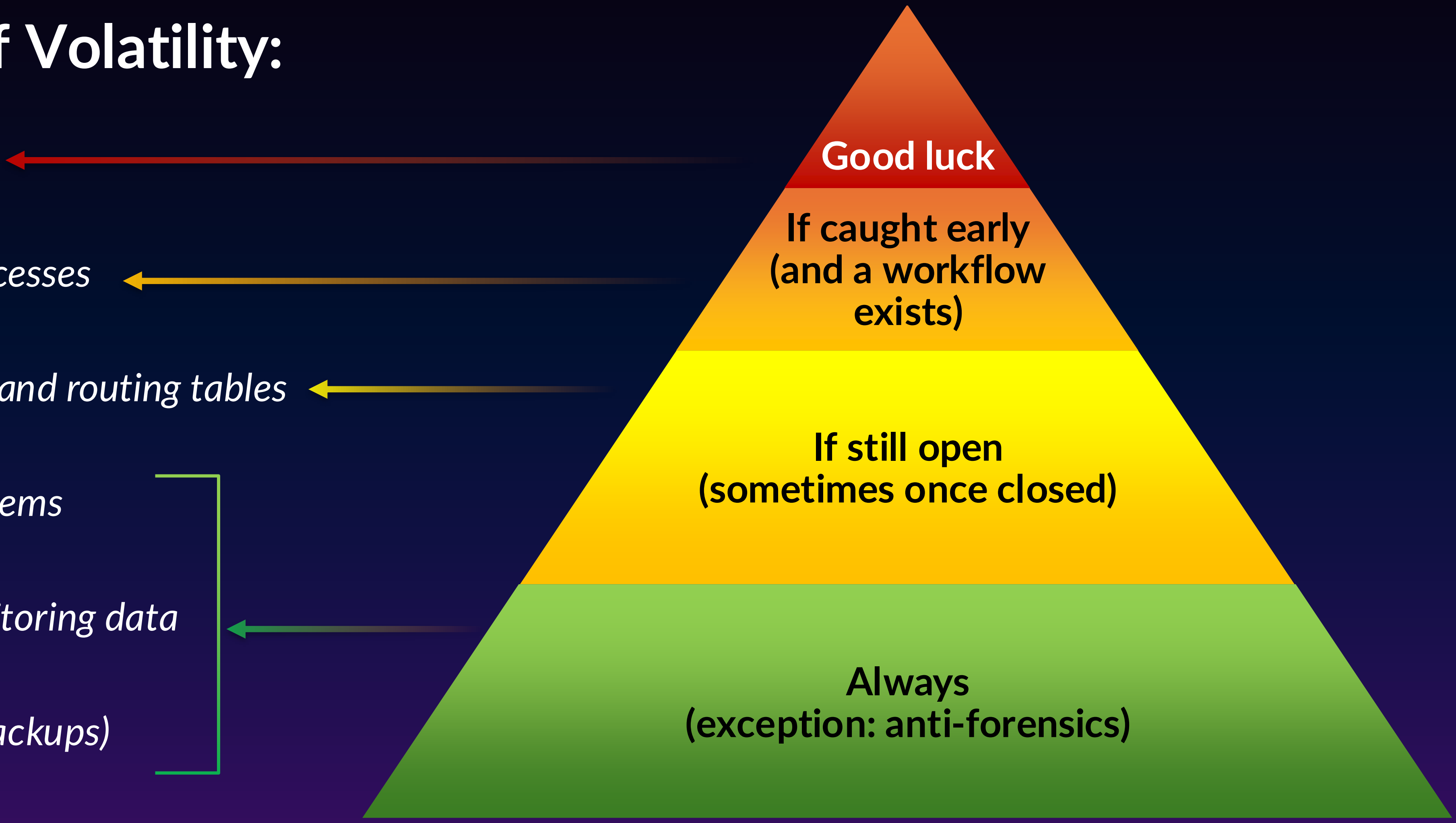


Preserve the Evidence

What to Capture

Standard Order of Volatility:

- *CPU registers, cache*
- *RAM and running processes*
- *Network connections and routing tables*
- *Disk data and file systems*
- *Logs and remote monitoring data*
- *Archival media (e.g. backups)*


Good luck
If caught early (and a workflow exists)
If still open (sometimes once closed)
Always (exception: anti-forensics)

Preserve the Evidence

What to Capture

Over-collection

- *”Get me everything”*
- *Full disk vs triage*

Wrong-collection

- *Forget memory*
- *No chain of custody*
- *Long-lived vs volatile*

Context Destruction

- *Premature eradication*
- *Reboot*
- *Pull the plug*

exterro inform VIRTUAL CON

Preserve the Evidence

What to Capture

Live state from relevant systems:

- *Memory, running processes, active network connections*
- *Logged-in users*
- *Scheduled tasks, persistence, evidence of execution*

High-value logs:

- *Anything likely to roll over, hard to capture, or not centralised*
- *Auth (success and failure), VPN, proxy, firewall, cloud audit logs*

Artefacts from high-risk systems:

- *KAPE, Velociraptor, etc.*

Document, document, document:

- *Actions taken (by blue and red)*
- *Timestamps*
- *Evidence collected*
- *Decisions made*

Common First-Hour Challenges

What Not to Do

- Shutting systems down as default
- Deleting / cleaning / remediating too early
- Patching or making mass changes
- Over-collecting, "get me everything"
- Lack of business context

exterro inform VIRTUAL CON

The First Hour Playbook

Ransomware

Priorities

- *Stop spread*
- *Protect backups*
- *Preserve enough evidence to ID strain and initial access*
- *Stabilise comms*

What goes wrong

- *Delayed response*
- *Scope isn't broad enough*
- *Backups unprotected / untested*

Other considerations

- *Don't expect perfection*
- *Capture and preserve what you can*
- *Expect leadership involvement early and often*

exterro inform VIRTUAL CON

The First Hour Playbook

Insider Threat

Priorities

- *Preserve evidence, with strong chain of custody*
- *Involve legal and HR early*
- *Minimise chances of tipping off the subject (except immediate harm)*
- *Scope access and activity patterns*

What goes wrong

- *Responders too visible / premature actions*
- *Subject becomes aware*

Other considerations

- *Chain of custody*
- *Document, document, document*
- *Work under privilege, involve legal and HR*

exterro inform VIRTUAL CON

DFIR Toolkit

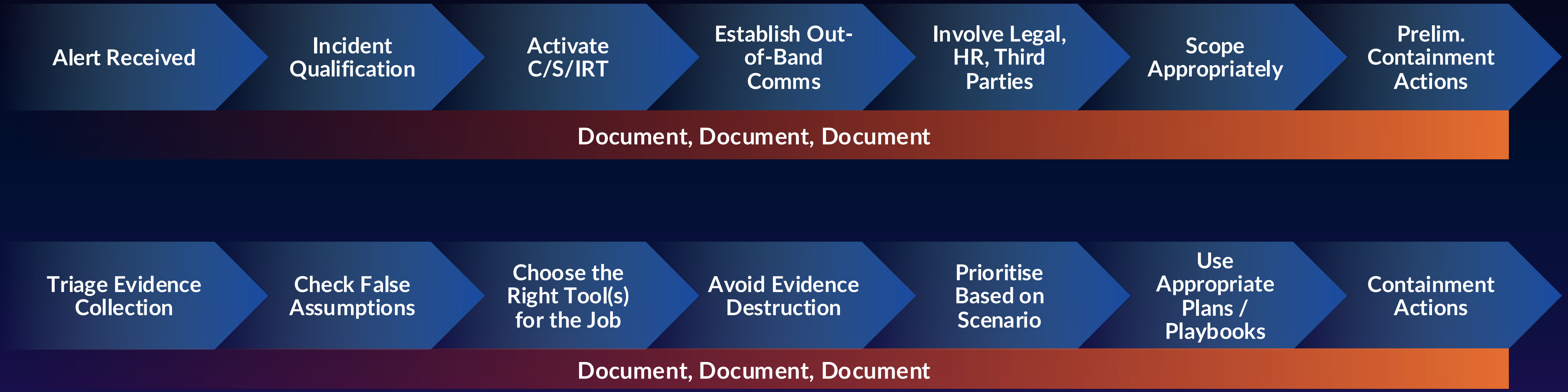
What question do you need answered?

- Which tool(s) can answer your question?
- Which tool(s) can prove your hypothesis?
- The tool is not the strategy; avoid tool-first behaviour
  - *Launching tools against an entire estate or subnet*
  - *Overwhelming data lakes*
  - *Push-button forensics*
  - *No detection? No problem*

- Tools must suit the scenario and workflow, not vice versa
- Confirm scope, capture, then contain

Takeaways

First Hour Narrative



Alert Received

Incident Qualification

Activate C/S/IRT

Establish Out-of-Band Comms

Involve Legal, HR, Third Parties

Scope Appropriately

Prelim. Containment Actions

Document, Document, Document

Triage Evidence Collection

Check False Assumptions

Choose the Right Tool(s) for the Job

Avoid Evidence Destruction

Prioritise Based on Scenario

Use Appropriate Plans / Playbooks

Containment Actions

Document, Document, Document

Q&A

EXTERRO INFORM

exterro inform VIRTUAL CON

Thank You for attending!

Contact Us : ashish.girish@exterro.com

Seth Enoka
Director & Principal Analyst
senoka@lykosdefence.com

exterro inform VIRTUAL CON