#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **AIR-W02**

Dissecting The Ransomware Kill Chain: Why Companies Need It

Kurtis Minder

CEO, GroupSense

Bryce Webster-Jacobsen

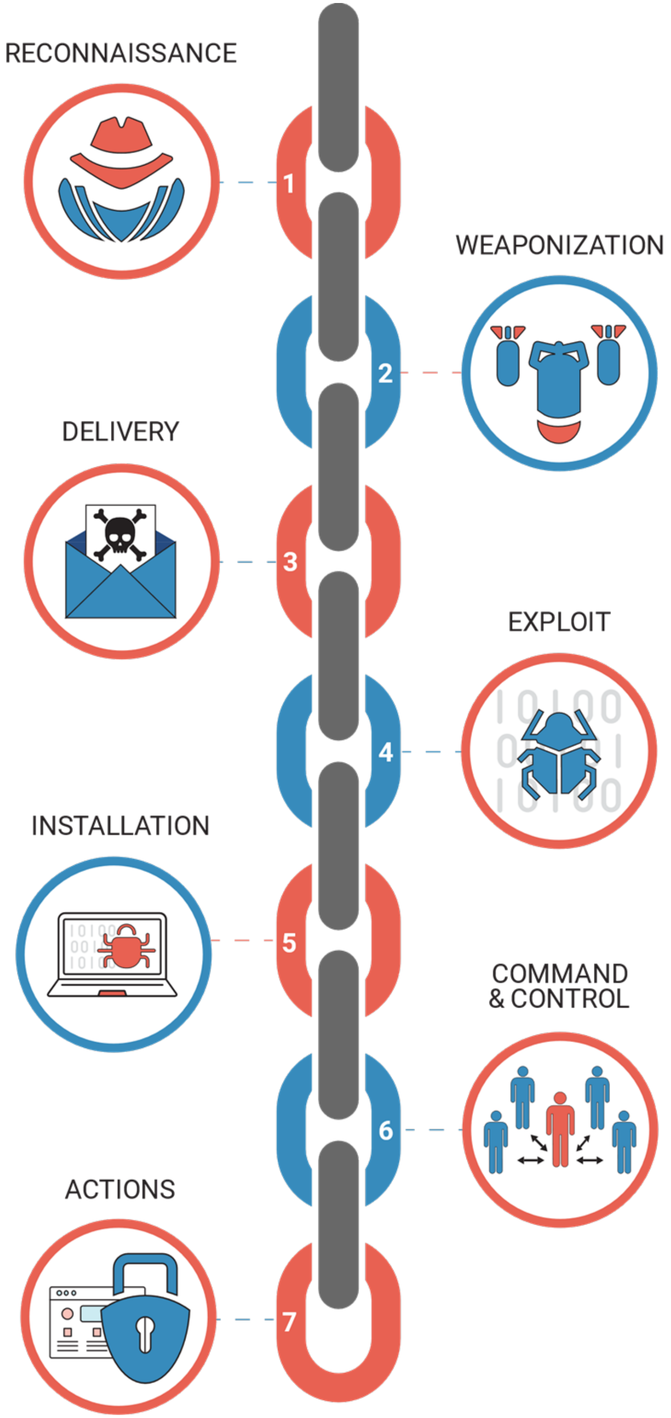
Director of Intelligence Operations,
GroupSense

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

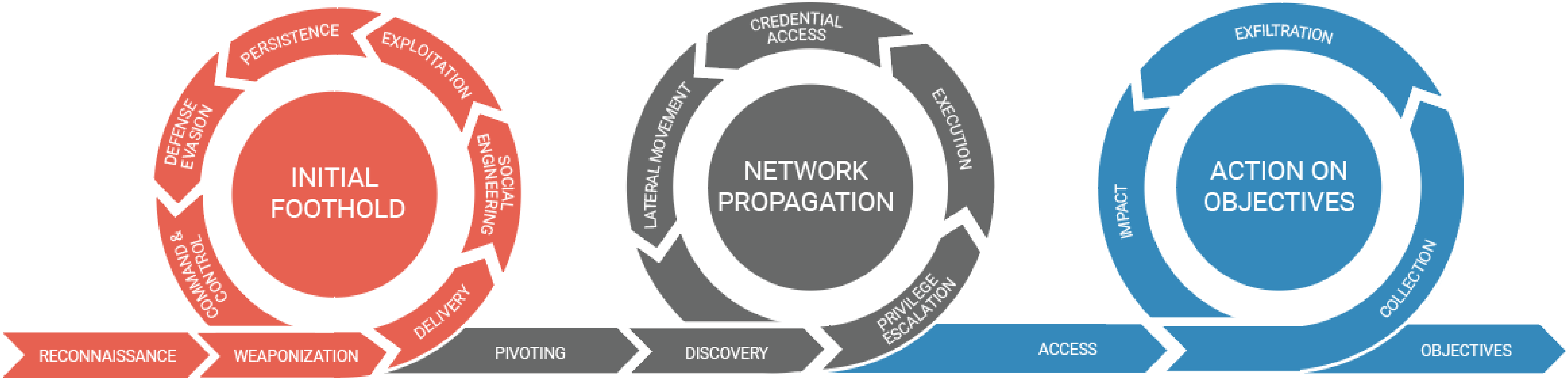
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Pandemic + Extortion = The Perfect Storm for Ransomware Operators



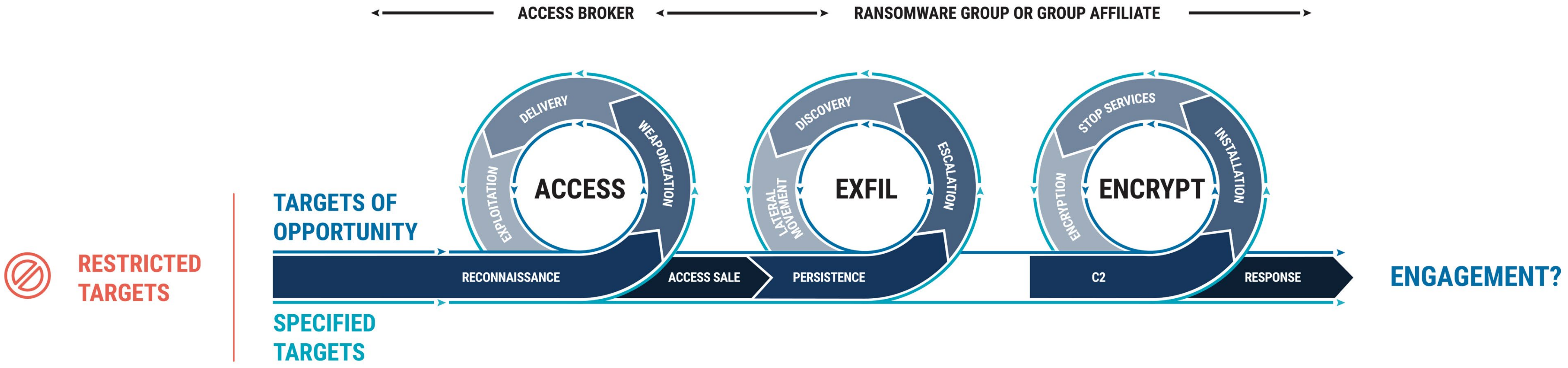
The Lockheed Martin Kill Chain

The Unified Kill Chain by Paul Pols



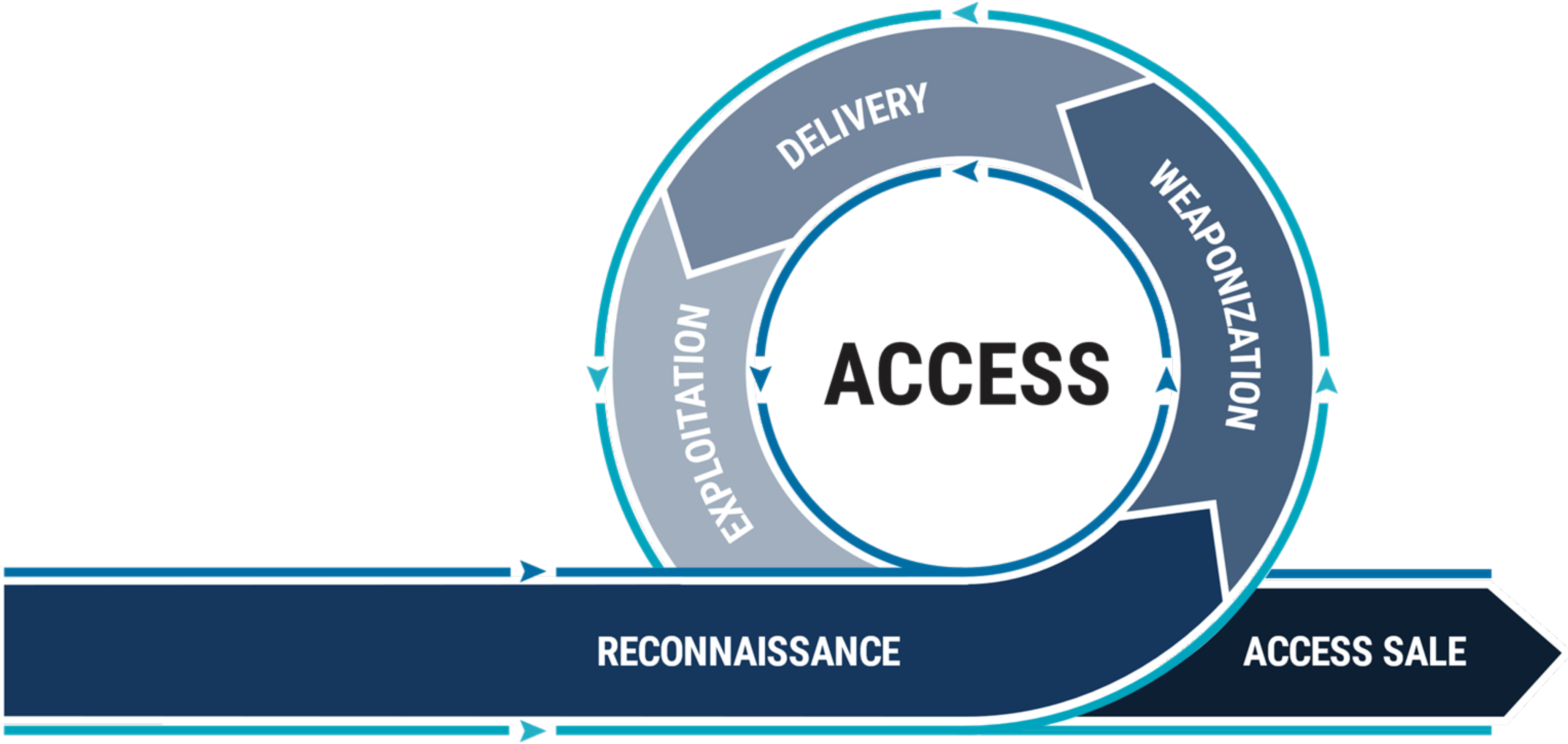
We need to evolve to combat ransomware

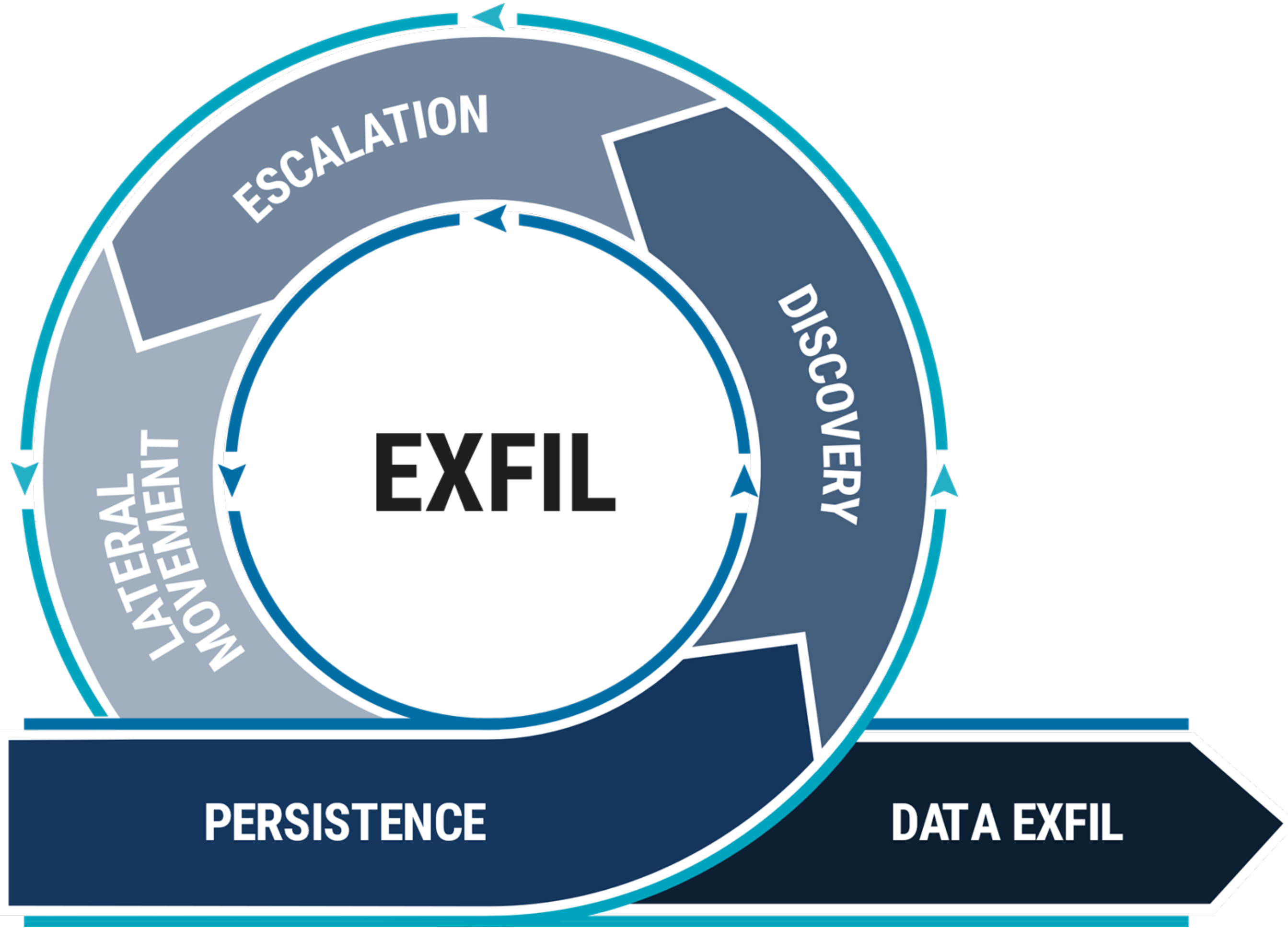
The Ransomware Kill Chain

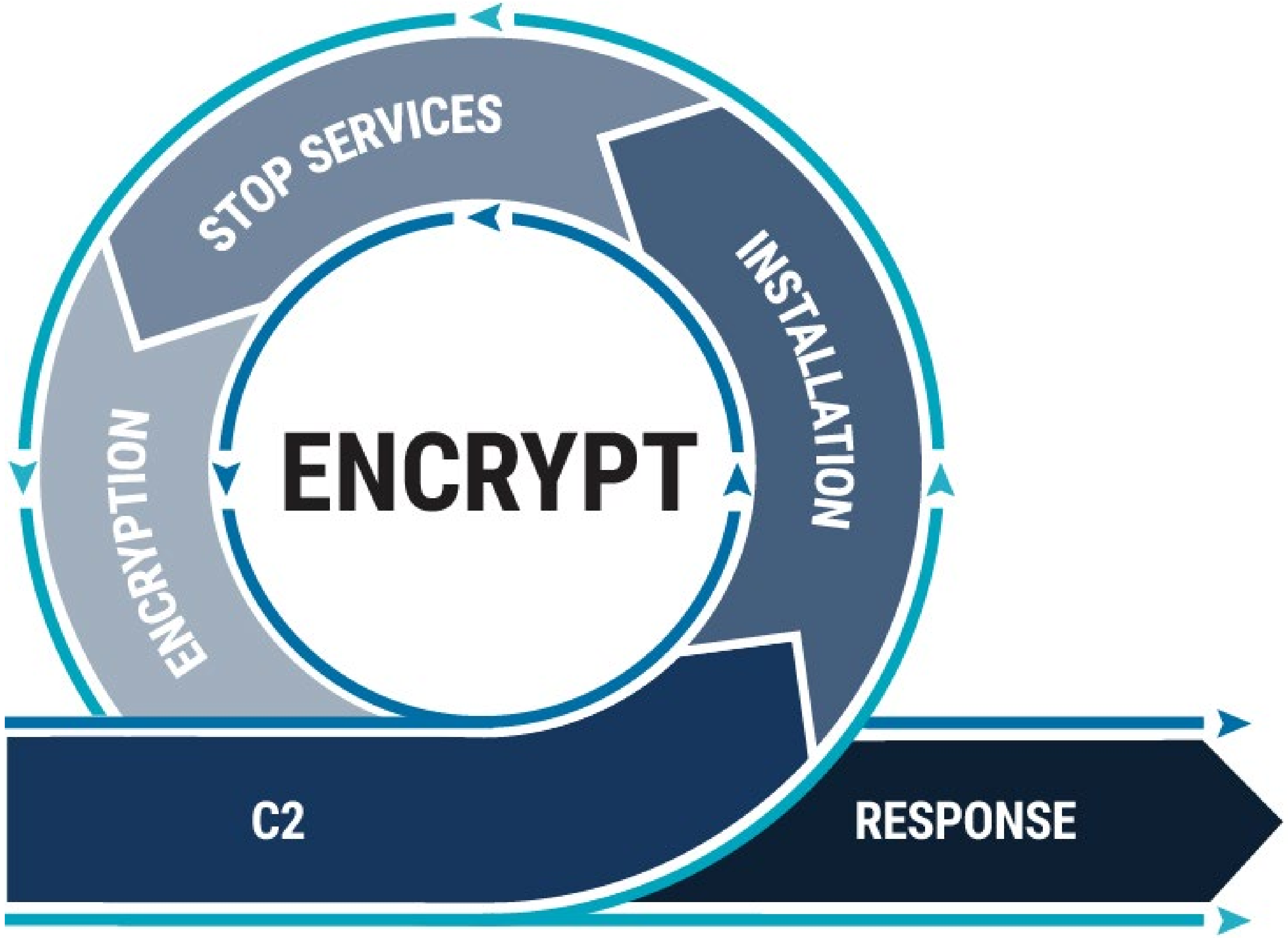


Types of Targets

- Restricted Targets
- Targets of Opportunity
- Specified Targets


DELIVERY
WEAPONIZATION
ACCESS
EXPLOITATION
RECONNAISSANCE
ACCESS SALE


ESCALATION
DISCOVERY
LATERAL MOVEMENT
EXFIL
PERSISTENCE
DATA EXFIL


STOP SERVICES
INSTALLATION
ENCRYPT
ENCRYPTION
C2
RESPONSE

Beyond the Ransomware Kill Chain

Lessons Learned in the Trenches

Do Not Panic

You have options. This is recoverable. Revert to your plan and execute.

Do Not Engage

Don't let anyone go to the site / respond. It can start a timer. Tone, language, style, and content can significantly impact odds and costs negatively.

Don't Shut Down

Don't shut down machines, this can cause file corruption, and hinders the incident response process.

Do Not Bury Your Head

Having backups and restoring doesn't mean this is over. There are many other things to consider.

Engage Legal Counsel

It is likely you are subject to breach disclosure laws - bring legal help to determine your obligations.

Consider Sanctions

Your country may have rules about which entities you can transact with. Responders can help you avoid penalties.

Engage PR Support

You will have to notify impacted constituents. Do this carefully and with professional guidance.

Engage IR

Bring in incident response assistance to understand the scope of the attack and to ensure the threat actors no longer have access.

Bring in a Professional Responder

Bring in a professional that has firsthand experience with the entire ransomware process.

Notify Law Enforcement

It is best practice to make local law enforcement aware of the situation.

Monitor

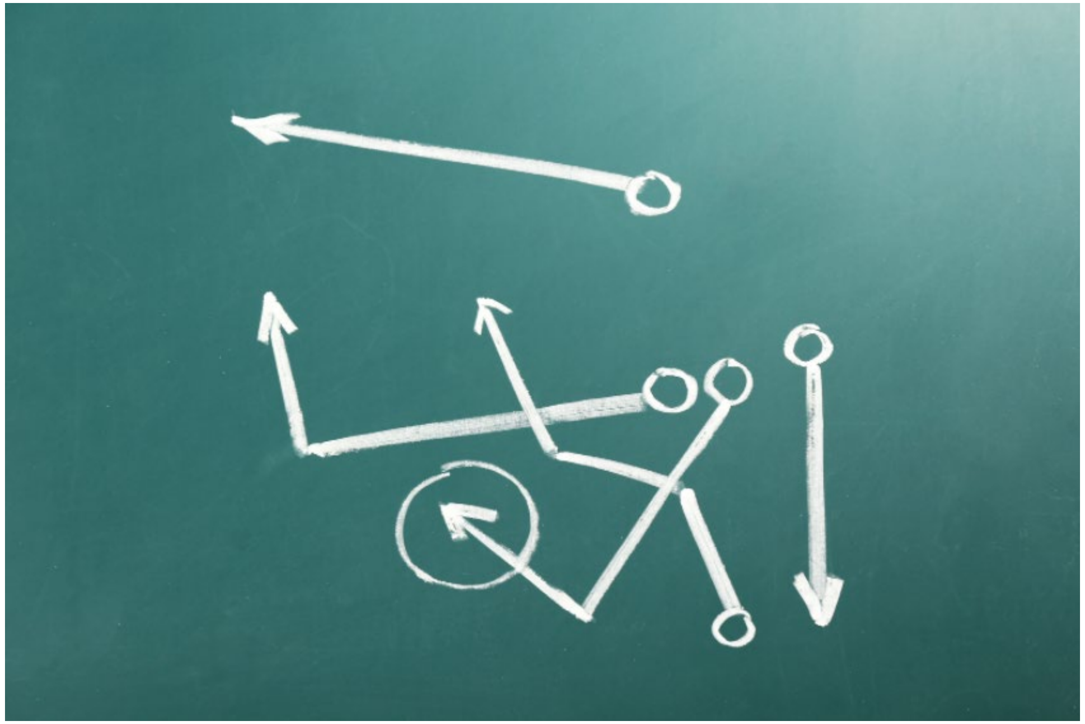
It is likely the threat actor took a significant amount of data. Monitor just in case it surfaces elsewhere.

Contact Insurance

Your insurer may have requirements dictating how the response is carried out. Engage them early.

Importance of Having a Ransomware Playbook

The objective of a ransomware playbook is to ensure the availability and integrity of digital information stored on all assets by detecting and disrupting threats that would attempt to hold the organization’s data hostage.



Ransomware Playbook Infrastructure

- Your ransomware playbook should include:
  - List of Key Stakeholders and Responsibilities
  - Detection, Assessment, and Containment Plans and Checklists
  - Communications Plan and Checklist – Which Should Include Incident Communications Statements
  - Response Plans
  - Incident Priority and Impact Classification
  - Payment Decision Making Process and Extortion Payment Approvals
  - Ransomware Event Cost Sheet

Apply What You Have Learned Today

- Next week you should:
  - Review your organization’s incident response plans and determine ransomware preparedness.
- In the first three months following this presentation you should:
  - Assess your organization’s digital footprint and determine the amount of exposure.
- Within six months you should:
  - Have a ransomware playbook

RSAConference2022

Thank You

Kurtis Minder

CEO, GroupSense

Bryce Webster-Jacobsen

Director of Intelligence Operations