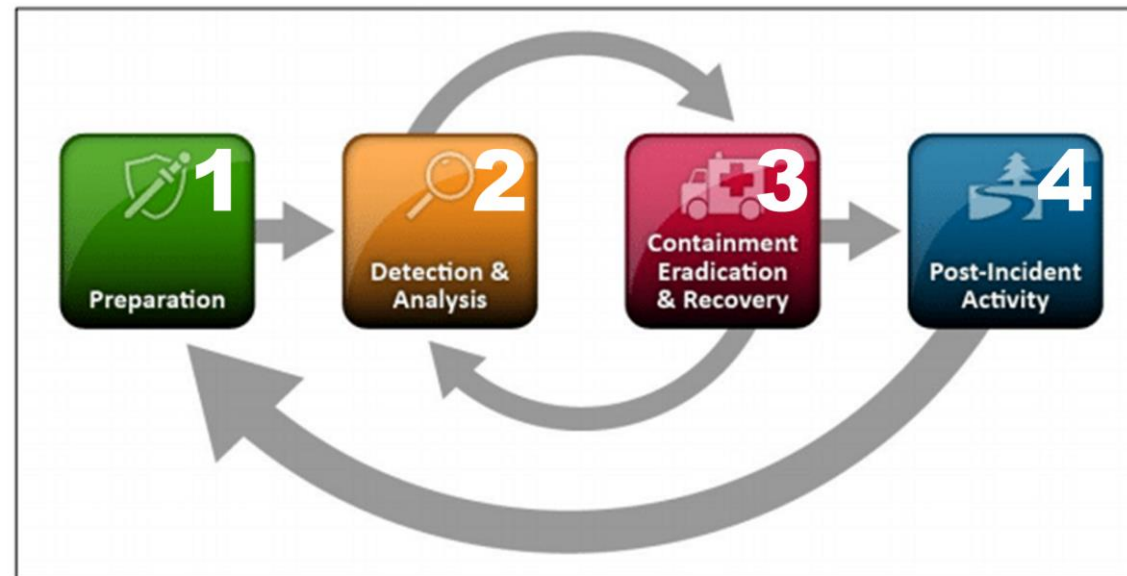


The Need for Out of Band Collaboration

30 SEPTEMBER 2022

Incident Response Plans Typically Share a Gap

- At each step in any incident response framework, the underlying assumption is responders and mission critical functions can maintain communications



The NIST Incident Response Lifecycle

- The gap is communications must be outside normal channels

The Need for Out of Band Communication is Clear

- The best incident response and business continuity plans will struggle to be effective if communications are unavailable.
- Even if normal communications channels are available, they should not be trusted as a malicious attacker could be on the inside (and verifying they are not is time consuming).



"Organizations should develop an **out-of-band communication plan for incident responders** that is usable for *multiple days* while an investigation occurs."












Privacy Apps Are Not Adequate Substitutes

- Security is more than just end-to-end encryption of communications
- Enterprises require user management, policy enforcement, and need the ability to retain appropriate business records
- Privacy applications create liabilities for organizations



Requirements for Out of Band Communication

1	It must stand alone	 A duplicate of current toolset  Rely on on-premise component(s)  Be dependent on network
2	It must be more secure	 End-to-end encryption  Protect against insider threats  Protect against 3rd-party breaches
3	It cannot sacrifice controls	 Maintain user policy controls  Retained records requirements  Reintroduce on-premise dependency

The COVID-19 Pandemic Changed Us

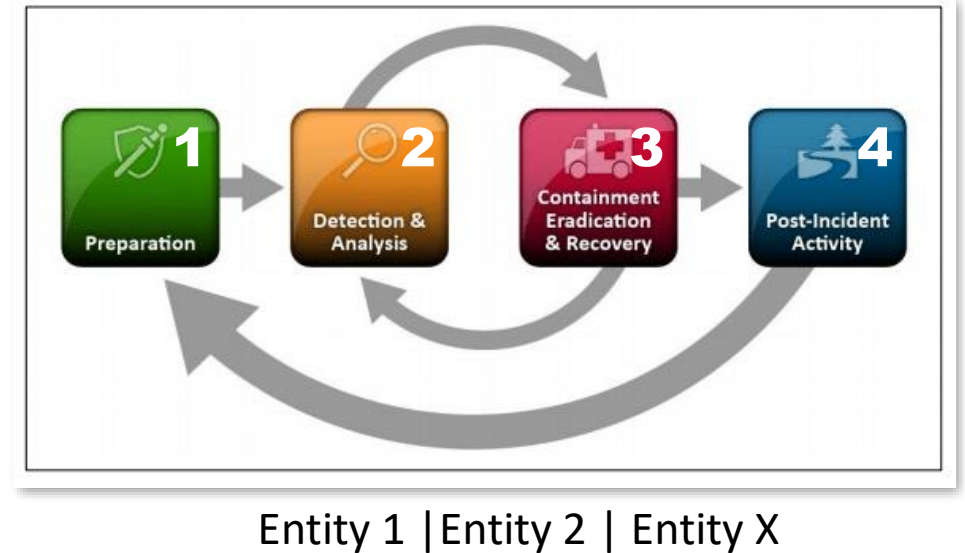
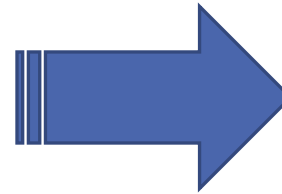
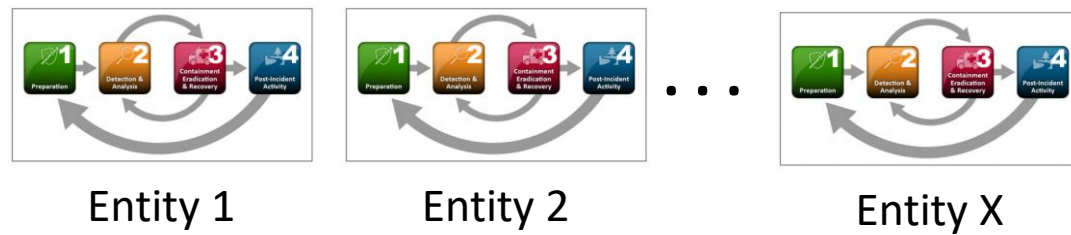
- It drastically changed the balance of maintaining an effective information security posture
- More vulnerable apart than together
- Focus shifted to the attack surfaces we all relied upon during the pandemic to work effectively
- Frequency of the attacks seems to be accelerating (and focused less on disruption and more on what information can be accessed/exfiltrated)
- Some attacks even took shape that the best security tools could not avert a compromise

Security Incident Response May Not Drastically Changed

- The tools we use improved incrementally
- Security incident response processes may have been streamlined to eliminate steps and reduce time to respond
- For the most part, staffing levels remained flat

The issue we collectively face is that the people wanting to exfiltrate data out of organizations are attacking the technology foundations we depend upon, and we do not have the resources to respond and readily thwart their efforts without working together more.

The Next Step is Collective Out of Band *Collaboration*



- Communicate on common issues which impact us all
- Tiered real time communications (CISO-CISO, SOC-SOC, Analyst-Analyst)
- Anonymity is possible (if needed)
- Stronger together by bringing to bear the best resources across multiple disparate organizations

THANK YOU
