AIRGAP

Incident Response Lifecycle for Ransomware Readiness

NIST (SP 600-61 r2) Computer Security Incident Handling Guide

Effective Incident Response (IR) plans do not flow in a straight line with a clear beginning and ending point. Instead, IR veterans think and design effective IR playbooks in lifecycles. Each iteration of the playbooks improved upon and more customized as a result of the lessons learned from managing past incidents.

Use Ransomware Kill Switch™ Instantly in Current Attacks

During ransomware attacks, time is of the essence for the IR team. Airgap Ransomware Kill Switch™ is tailor-made for post exfiltration phase and provide the most time every IR need for ransomware mitigation even in the current attack cycle. The product can be deployed within an hour one VLAN at a time to prevent / block all unnecessary & unauthorized communications. So, you don't have to wait for 2 weeks to reopen the business operation. With the clear device inventory and protocol policy enforcement, the Ransomware Kill Switch™ can neutralize the attack or prevent it from getting worse.

During ransomware attacks, **time is of the essence** for the IR team.

Use Ransomware Kill Switch™ Adaptively in Future Attacks

When detection and prevention failed, the most critical action for all IRs is how to avoid the incidents from happening again. The lessons learned can be converted into an adaptive policy mapping in Ransomware Kill Switch policy bucket configuration and Endpoint security automation using 3rd-party threat intelligence or zero trust assessment (ZTA) risk score.

Incident response playbooks provide organization's step-by-step frameworks for preparing, identifying and containing cyber security threats such as Ransomware.

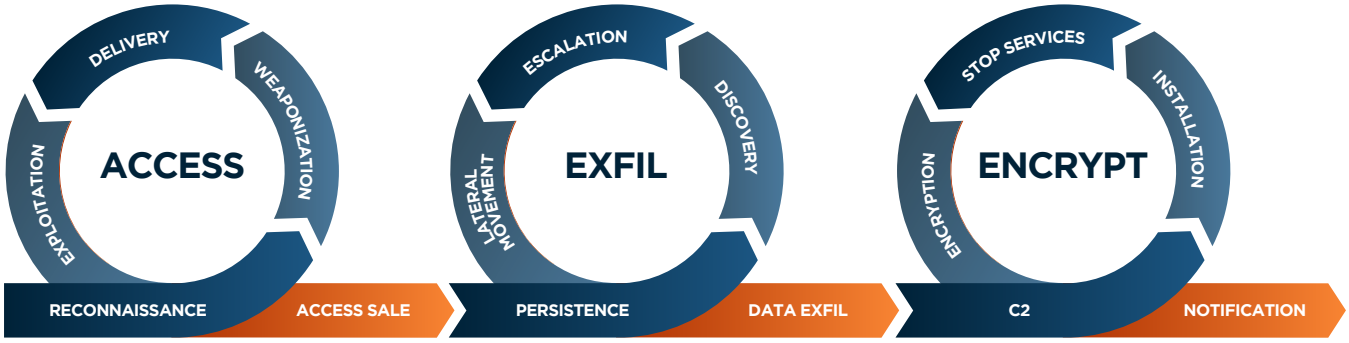

Figure: Kill Chain Lifecycle

The two main drivers to design IR playbooks in iterative lifecycles are that attackers are adaptive and will quickly improve their attack tactics and ransomware based on previous successful and failed attacks. Secondly, changes within an organization such as onboarding new applications, services and organizational teams will drive the need to adapt IR playbooks to account for the internal changes.

Attackers are **adaptive** and will quickly improve their **attack tactics and ransomware**

The following table describes the NIST Computer Security Incident Handling Guide framework. Aligned to each step will be Airgap's offerings to help Incident Response teams prepare, respond and continuously improve their incident response playbooks to minimize the impact of ransomware to business operations.

Step	Airgap Incident Response Lifecycle
Preparation	Preparation is key to implementing a rapid incident response to become Ransomware ready. The goal to aim for in this phase is to prepare step-by-step frameworks for IR teams to quickly implement in response to a ransomware attack. Incorporating Airgap's Ransomware Kill Switch™ as a tool to implement IR playbooks will enable customers to isolate and contain ransomware infections within minutes, not days or weeks, minimizing the impact of ransomware to business operations. In this step Airgap can help with the preparations: ▪ Compile a list of all assets through device discovery in your networks to make visible the location and classification of assets, including but not limited to: servers, networks, applications, and critical endpoints (like C-level laptops). ▪ Rank the risk of the assets with Airgap's policy monitoring. Host communications and host events are monitored to assess the risk of an endpoint ▪ Perform Zero Trust network segmentation and isolation for IT/OT/IOT devices and remove the interdependency from applications and networks.

Step	Airgap Incident Response Lifecycle
Detection & Analysis	At this phase in the process, a cyber security incident has been identified in your environment. Airgap integrates with leading Endpoint Detection and Remediation (EDR) solutions to assess risks of compromise inside the network or remote endpoints so IT admins can react quickly when an EDR system has detected suspicious network and host activity that may be indicative of a breach within the network.
Containment, Eradication & Recovery	Containment is aimed to minimize the impact to business operations. Airgap's Ransomware Kill Switch™ has been purposefully designed as a means for security administrators to quickly isolate infected hosts, endpoints and isolate non-infected hosts, devices and servers to resume business operations. Airgap's Ransomware Kill Switch™ isolates hosts at multiple levels, at the network and at the host level. Host isolation locks down access to non-infected hosts to enable only the critical applications to continue to be accessed by non-infected hosts. The impact to the user experience is minimal if even noticed as critical business operations continue to operate.
Post-incident activity	Just because business services become "operational" again, this doesn't mean the incident response process ends. Post-incident activities should have you adapting IR playbooks in preparation for future incidents and discovering gaps which will likely prevent fewer incidents. It's a never-ending cycle of improvement, and there are a few different ways to think about the various stages, depending on what school of thought you subscribe to. No IR process can account for every possible ransomware scenario. Some scenarios can't even be defended against until they've occurred. As the ransomware threat landscape is also ever-adapting so should your incident response processes will naturally need the occasional update. ▪ Airgap data and analytics can be used in the preparation phase for the next incident. Some lessons learned that can be beneficial for updating IR playbooks include but are not limited to: ▪ Gaining insights into the effectiveness of host firewall lockdown policies. Were there communications ports that need to add to enable new services or are there application communication ports that can be removed due to the non-use of those applications. ▪ Improve Airgap's Zero Trust Isolation™ for enterprise networks to improve the containment of infected hosts.

About Airgap

Airgap provides an agentless Anti-Ransomware platform to stop the spread of malware in the enterprise network. Our industry's first Ransomware Kill Switch™ locks down your most critical network assets at the first indication of compromise with complete control and policy enforcement over the device-to-device and device-to-application communication.

airgap.io

AIRGAP