Incident Containment

Blue Team Level 1 Certification (Standard) > IR4) Containment, Eradication, and Recovery Phas... IN PROGRESS

Depending on the type of incident, there are several responses we can take to contain the incident, preventing it from spreading to additional systems and potentially causing more damage. This lesson will cover actions that can be taken, along with any negative consequences that could occur. By definition, Incident containment is a function that assists to limit and prevent further damage from happening along with ensuring that there is no destruction of forensic evidence that may be needed for legal actions against the attackers later.

WHAT IS CONTAINMENT?

Usually, organizations think that containment is a process step that we need to follow during Incident Response. But in our opinion, Incident containment should be a Strategy. Once a containment strategy is defined, the respective tools & technologies can be selected to participate in the fulfillment of the strategy. Process pieces will eventually follow. Containment strategies can be defined based on the focus area in the IT Infrastructure. It can be at the perimeter, extended perimeter, internal tier, or at the end point, or it can also be a combination of any of the above. Mostly, the strategy is dependent on understanding your IT infrastructure and making the best use of the infrastructure. That is why it is not the same for every organization and rightly so. We would like to list down a few examples of such containment strategies below.

SHORT TERM CONTAINMENT

Typically short term containment is break-fix or quick heal. The objective of the short term containment is to prevent the asset or the user from causing further damage to the organization. It is akin to a Quarantine mechanism in AV software, where it is not removed, however its potential to create further damage has been quelled. Everyone reading this post would definitely have implemented short term containments in their CSIRT life. Remember "pull the plug", "block the mac", "disable the user" etc. However, it is important to note that this does not fix the real reason an incident happens. It also does not stop an incident from recurring on a different asset in the organization. This is where long term containment comes into play.

LONG TERM CONTAINMENT

Long term containment is an enterprise-wide fix that is a step short of complete remediation of an incident root cause or attack vector. The objective of the Long term containment is to stop other users or assets in the organization from getting impacted by the same incident. Input to long term containment comes from the Incident Handling phase where the appropriate investigations have been done and the possible attack vectors or infection methods have been identified. Till full-fledged enterprise-wide re-mediation efforts are carried out, steps like putting a WAF behavioral policy, a custom SNORT signature to block the attack pattern, a HIPS policy for system lockdown, etc. can be considered as long term containment strategies.

CONTAINMENT MEASURES

Perimeter Containment

- Block inbound traffic and outbound traffic.
- IDS/IPS Filters.
- Web Application Firewall policies.
- Null route DNS.

Network Containment

- Switch-based VLAN isolation.
- Router-based segment isolation.
- Port blocking.
- IP or MAC Address blocking.
- Access Control Lists (ACLs).

Endpoint Containment

- Disconnecting the infected system from any network connections (turning WiFi off, pulling ethernet cable).
- Powering off the infected system.
- Blocking rules in the Desktop firewall.
- Host intrusion prevention system (HIPS) actions.

HAS IT BEEN EFFECTIVE?

Now that you have a validated Incident Containment strategy, the next step is to ensure that your strategy was effective against the Attack Vector. This is where monitoring of the Attack Vector, Targeted Victims, Outbound Traffic from the victims, etc. become important measures of effectiveness. This can be a simple monitoring rule in SIEM products with a forward-looking time frame, or it could be a completely monitored network segmentation.

< Previous Topic   Mark Complete ✓   Next Topic >

Back to Lesson