INCIDENT COMMANDER JOB AID

Incident Commander (IC) identifies cyber incident response S.M.A.R.T objectives. The objectives will further be separated into Managerial and Operational and assigned accordingly. IC then communicates to response team and assigns objectives to key personnel. Objectives will be based on response to gathered information using the pattern below.

EVALUATE

What is the current situation, what is going on, what impact is the incident having on normal operations? This step will allow Incident Commanders to make good decisions later.

* Identify the Problem
	+ Identify symptoms and have experts provide information.
	+ Gather as much information and as quickly as you can remember incident is still going on.

Identify what the incident is affecting and how it is affecting what is normal.

* Identify the impact or sizes of the issue whether it is static or escalating.
	+ Get all the facts the current impact, future impact and probability of things that could happen.

STABILIZE

Next step is to stabilize the incident. We need to determine what we can do to fix it, and then execute those actions.

* Identify possible actions
	+ Identify any actions you can take to alleviate the issue. Ask your experts what they want to do.
	+ Identify the risks associated with each of those actions.
* Decide.
	+ Decide which action to take based on the information you have available.
	+ Making the "wrong" decision is better than making no decision. If you have nothing but bad options, pick one and proceed.
* Gain consensus. - Ask "Are there any strong objections?"
	+ Gather support for the plan (See "Polling During a Decision" below).
	+ Listen for objections.
	+ Be prepared to adjust your plan if new information is presented.

UPDATE

While remediation steps are being carried out, it's important to provide status updates, not just to responders, but other stakeholders within the organization.

* Provide regular updates.
	+ Maintain a cadence and provide regular updates to everyone that is part of the incident response.
	+ What's happening, what are we doing about it, etc.
	+ Keep updates short and factual.

VERIFY

Once remediation actions have been performed, we need to verify that they have been successful or not and proceed with a backup plan if not.

1. Follow-up on task completion.
	* Ask for the status of task completion from the tasks you assigned out.
	* If responders need more time, give them more time.
	* If problems persist, begin again from the size-up step.

Throughout the ICS/SCADA Cyber Incident the company leadership will exert a lot of pressure to return IT services to production.

At the same time, internal and external legal counsel will want to know how the attack happened and if any data was stolen. Knowing how it happened is essential to remediation and understanding if data exfiltration occurred informs legal reporting and decision-making.

These goals often conflict with a speedy recovery. The incident commander must direct an expedited collection of evidence to investigate. This investigation assists in securing the environment, determining if data was stolen, and freeing storage for the recovery effort.

Also in conflict with a speedy recovery is the security of the recovery effort. Failing to properly secure the environment before rebuilding could result in re-compromise.

If the attacker’s access is not severed, they often re-encrypt servers, eavesdrop on meetings, and send messages to employees and customers to disrupt and harass the victim. Containing the network and evicting the attacker are essential for a secure recovery.

Attached:

Incident Commander P

