GitHub @ deezombiedude622

III. CONTAINMENT, ERADICATION, RECOVERY, POST-INCIDENT ACTIVITIES

Strategy Considerations
- potential ding to $ & theft of resources
- need for evidence preservation
- service availability
- time & resources required, effectiveness, duration

Containment
isolating affected systems to ensure the incident ↛ escalate
ex., disconnecting malware-infected endpoint fm network

III. Containment, Eradication & Recovery

Eradication
process of removing threat fm org's environment (incls. identifying & eliminating root cause of incident)
ex., ① rebuilding malware-infected endpt fm a clean baseline OS image
② updating all EDR clients to detect & stop the known atk vector

(ref. ChatGPT)
w/out ERADICATION efforts:
* residual threats may still exist ⇒ ∃ risk of infection
* compromised data/sys. remains unavailable
  ↳ integrity still compromised, reputation tarnished
  ↳ ≡ non-compliance w/ regulatory requirements/legal obligations
* extended downtime
  ↳ systems may need to remain offline or undergo maintenance
  ⇒ disrupt business ops ⇒ ↑ costs: recovery efforts, potential legal consequences

Recovery
process of restoring & returning affected systems & devices back to their fully operational states
(incls. – verifying ↛ threats remain
– verifying sys. integrity)
ex., ① returning clean endpt back to network & ready for work
② resumption of work as pre-incident

Evidence Gathering
① use predefined templates to collect data (ex., hostname, IP addr., MAC addr., etc.)
② keep incident response/mgmt sys. isolated fm affected network & systems
③ reconcile evidences & notes w/ other incident responders
④ identify missteps early, gather other supporting evidences
⑤ identify atking hosts
↳ look for incoming connections (ex., fm login events, firewalls)
- EID 4624 : successful login
- EID 4625 : Failed login attempt
- EID 4672 : Special privileges assigned
- EID 4648 : Login using explicit credential

↳ research atking hosts' IP addrs. fm threat intel svc/search engines
↳ use incident dlos of known "bad" IP addr.
↳ monitor possible other communication channels

Activities
① undoing threat actors' actions (as much as possible)
② restoring to known good state (baseline) – rebuild endpts, computers, appliances affected
– review config. & restore to known "snapshot"
③ removing threat actors' presence & backdoors
– sus/unexpected processes that may provide access as backdoor
– disconnect access to C2 servers
④ perform security testing – vuln. assessment, pen tests; playback atk & ensure ↛ reoccurrence
⑤ deal w/ unauthorized transactions (during incident window w/ before & after range tolerance)
⑥ revoke & renew access credentials

IV. Post-Incident Activity
* often most underrated activity in lifecycle
  ↳ fallacies – incident closed ⇒ ↛ further activities required
  – incident response ends after report approved & communicated
  – identifying lessons should be done by other teams
* how to get adequate investment & funding for cyber incident response & forensics capability? → DATA
  ↳ # handled incidents per year
  ↳ time dimension per incident
  ↳ subjective assessment of each incident

Evidence Retention
How long various types of data should be retained?
① General & specific data retention policy → How to dispose & wipe expired data?
② Safekeeping – secure data collected & filed for potential & future litigation
– access rights & confidentiality
– must survive thru leadership & staff changes
③ Cost – what happens to existing "seized" hardware & other assets?
– budget cost until disposal

ISAC: Information Sharing & Analysis Center
TLP: Traffic Light Protocol

Incident Response Coordination R'ships

Team-to-Team
exist whenever technical responders in diff. orgs collaborate w/ their peers during any phase of incident handling lifecycle

Team-to-Coordinating Team
exist btwn an organizational incident response team & a separate org that acts as a central pt for coordinated incident response & mgmt (ex., ISAC, supervisory/regulatory body)

Coordinating Team to Coordinating Team
r'ships btwn multiple coordinating teams (ex., US-CERT, ISACs) to share info relating to cross-cutting incidents which may affect multiple communities

TLP

TLP:RED Not for Disclosure
* info ∅ dissemination to 3rd parties unless sender permits
* only participating groups can have access to it

TLP:AMBER Limited Disclosure
* info can be shared w/ participants of an org & some members of a community
* additional restrictions can be made

TLP:GREEN Community-Wide Disclosure
* info can share w/ everyone of a particular community
* but ∅ publish publicly on internet

TLP:WHITE Unlimited Disclosure
* info can be shared publicly w/ everyone
* subject to copyright laws

Info. Sharing Techniques
* any incident related info must be classified
  - ↳ internal only — use your org info classification
  - ↳ external — use TLP classification
* monitor trustworthiness & track record of recipients