Github @ deezombiedude612

II. PREPARING FOR INCIDENTS

Event vs Incident

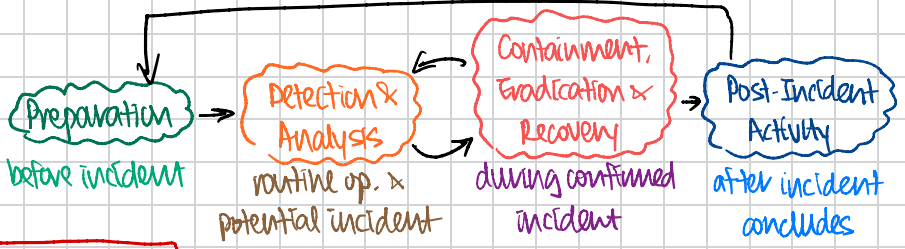
Event
- any observable occurrence in a network \ system
- * ≠ always indicative of security breach
  - ↳ many events are routine & ≠ indicate security problem
- * monitoring & analysts
  - ↳ required by events to determine their significance
- ex.: ① employee flags sus. email
  ② security lapse occurs due to server outage
  ③ someone downloads software (authorized / not) to a company device

Incident ⊆ Event
- a type of event that actually harms \ represents real threat to CIA of data \ systems
- * indicates security breach \ threat
  - ↳ incidents are events that have a real (-)ve impact on security procedure
- * requires immediate response
  - ↳ incidents demand an immediate & structured response to mitigate dmg
- ex.: ① employee replies to email, divulging confidential info
  ② equipment w/ sensitive data stolen
  ③ pswd compromised thru brute force atk on sys.

Threat Alert Levels

- Green — everything is normal; ≠ significant new threat known
- Blue — used for testing only; same as GREEN
- Yellow — currently tracking significant new threat; impact currently unknown \ expected to be minor
- Orange — major disruption in connectivity imminent \ in progress
- Red — loss of connectivity across large part of internet

Cyber Incident Response Lifecycle



- Preparation — before incident
- Detection & Analysis — routine op. & potential incident
- Containment, Eradication & Recovery — during confirmed incident
- Post-Incident Activity — after incident concludes

Why Cyber Incident Response?

Ensuring Business Continuity
support quick resumption of normal ops. after incident (maintain integrity & availability of business process) ≠ detail steps

Rapid Containment
minimize impact of security breaches by quickly containing threats

Reduce Dmg & Costs
- * dmg potential to systems & data
- * financial losses associated w/ data breaches & sys. downtime

Legal & Regulatory Compliance
adherence to data protection laws & regulations; avoid legal penalties & fines

Learning & Improvement
provide insights fm incidents to:
- → improve security measures & protocols
- → enhance organizational preparedness for future threats

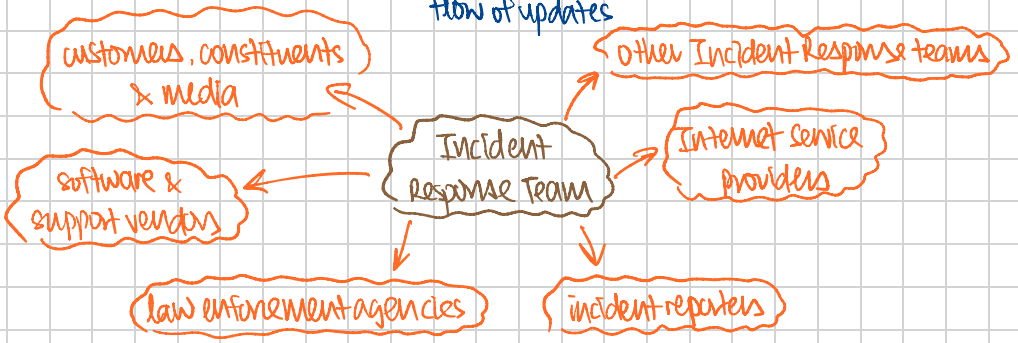
Maintaining Trust & Reputation
- * demo. commitment to security
  - ⇒ protect org's reputation
- * capability in handling incidents
  - ⇒ help maintain customer & stakeholder trust

Policy Preparation

- * prepare policy, std, guidelines, procedure

- Guideline: provides additional, recommended guidance
- Procedure: establishes proper steps to take (How do I do it?)
- Standard: assigns quantifiable measures (what is required?)
- Policy: identifies issue & scope (Why do I need to do this?)

- * identify key stakeholders
  - ↳ internal (w/in company, group level)
  - ↳ supply chain
  - ↳ regulators
  - ↳ law enforcements
  - ↳ w/in & cross-sectors
- * manage media interaction — designated spokesperson, timely updates, flow of updates



Cyber Security Incident Response Team (CSIRT)

- * tasked w/ organizing & providing assistance in responding to a computer security event \ incident
- * struct. is determined by requirements of parent org.
  - ↳ internal security team, coordinating CSIRT, centralized CSIRT, hybrid CSIRT, distributed CSIRT, CSIRT \ SOC hybrid, externalized CSIRT

Incident Responders during:

(1) Peaceful Times (Proactive Measures)

* continuous monitoring: regularly monitor systems & networks for unusual activities
* training & awareness: conduct cybersec training & awareness programs for employees
* updating & testing: regularly update security measures, conduct drills & simulations
* threat advisory: analyze, publish & distribute advisories

(2) Potential Intrusion (Active Monitoring & Preparation)

* alert verification: verify & assess alerts for potential security incidents
* initial assessment: determine scope & potential impact of suspected intrusion
* enhanced monitoring: surveillance of network traffic & sys. logs ↑
* preparatory measures: ready the team & tools for potential escalation to an incident

(3) Active Intrusion (Response & Mitigation)

* incident confirmation: confirm intrusion & its severity
* containment: take immediate actions to contain incident & prevent further dmg
* eradication: eliminate src of intrusion & secure vuln.
* recovery: restore systems to normal ops, ensuring no remnants of threat remain
* communication: maintain clear & regular communication w/ relevant stakeholders

Recommendations for Incident Response

Basically...

1. Create incident response policy
2. Develop procedures
3. Select incident response team model
4. Recruit
5. Determine services to offer

Establish formal incident response capability → Create incident response policy → Develop incident response plan based on policy → Develop incident response procedures → Establish policies & procedures for info. sharing → Provide info to appropriate org. / Select team model → Recruit ppl w/ appropriate skills for incident response team → Any extra participants needed for incident handling? → Determine services to offer

I. Preparation

Documentation
* Others
* network diagrams
* firewall & other (technical) security policies
* baselines
* storage (large cap, high speed)
* packet sniffers & protocol analyzers
* elevated credentials

Asset Lists
* List of critical & impt servers, network appliances, apps.
* cloud assets
* asset mgmt tools (servicenow, freshworks, CMDB)
* business & sys. owners

Tools
* Computers
  * laptops, desktops
  * forensic workstations
  * cloud instance
* Software
  * OS
  * digital forensics tools (ex., Axios, Encase)
  * special appliances (forensic workstation, drive cloners, write blocker)
  * storage (large cap., high-speed)
  * packet sniffers & protocol analyzers
  * note-taking tools (notebooks, cams, audio recorders, forms, evidence bags & tags, camcorders)
* encryption software (encrypted SIP, PGP)

Facility
* designated war/incident room
* secure storage facility

Communication
* mobile phones (iOS, Android)
* incident tracking & reporting sys. (ex., MISP, TheHive)
* reserved conference bridge / virtual collab app
* IM/communication for potential & confirmed incidents
* up-to-date contact info

Signs of Potential Incident (Detection)

SIEM: security incident & event mgmt

* user reports
* proactive monitoring (SOC, NOC, Cyber Fusion Center)
* threat actors (APT Groups, Ransomware Gangs, Hacktivist)
* Dark-web marketplace

II. Detection & Analysis

Analysis

- Profile networks, systems & apps
  - * define baseline of network traffic across diff. time periods
  - * take snapshots of app load across diff. time & traffic load
  - * consider various metrics - transactions per second, CPU load, memory load, etc.
- understand normal behavior
  - * allow tolerance for set baseline
  - * regular measurements & adjustments
- define log collection & retention
- Automate correlation in SIEM
- Synchronize all clocks across all systems
  - for timeline analysis
  - NTP server closest to you
- Define high-risk apps & systems
- Isolated systems
  - * independent internet connectivity & secure msging systems
  - * GREEN (IR Network), YELLOW (IR Sys. connected to Intranet), BLUE (Intranet) separation
- Established communication channel to other CERT or ISACs

Prioritization
- refer to business impact matrix & incident classification in policy
- consider impact - fxal, info. impact, availability impact

Notification
- refer Incident Response Policy, Stds, Guidelines & Procedure for notifications
- consider custom msging, frequency & details to diff. audiences
- follow regulatory requirements
- consider various channels for notifications

Atk Vectors	Source of Indicators
Removable media \ USB ports	* OS Logs * Endpoint Detection & Response (EDR) * Data Loss Prevention (DLP)
Web traffic	* proxy * firewalls, web app. firewall (WAF) * intrusion detection system (IDS) * Extended Detection & Response (XDR) * network flows
Email	email security gateway, EDR, DLP, proxy
Impersonation	OS & app. logs, network devices
Improper Usage	* User Entity & Behavior Analytics (UEBA) * Security Info & Event Mgmt (SIEM) * integrity checks * OS * app & network logs
Theft \ Loss	asset mgmt, EDR, active directory
Disgruntled Employees	DLP, network logs, OS & app, UEBA
Supply chain	access ctrls, app & network logs
others	TBA