Threat Intelligence | Insider Threat Detection | User Behavior Analytics | Cyber Threat Management | Data Security Intelligence | Cloud Security Intelligence Application Security Intelligence | Anomaly & Pattern Detection | Security Information Event Management | Digital Forensics | Data Recovery | Malware Investigation | Packet Analytics | Packet Forensics | security operations and analytics platform architecture (SOAPA)

Cyber Security Lifecycle

ROHIT SADGUNE 18TH SEPTEMBER 2017 LEAVE A COMMENT 0 16

Cyber Security Lifecycle

Project Name: Cyber Security Lifecycle

evaluated for any loopholes and is improved and worked upon.

Author: Rohit D Sadgune / Amruta Sadgune

FAQ:-

1. What is cyber security Lifecycle?
2. What are the different phases of cyber security Lifecycle?
3. What are the significance of protection in cyber security?
4. What is the importance of identification of cyber threat?

IDENTIFY KEY ASSETS

The most important step in the cyber security Lifecycle is to identify what is to be protected.

Identification of network, protocols, topography, assets and servers needs to be understood in order to have their information on hand before any risk occurs. A detailed drilled down information from operating system, applications, network drives, host name, IP addresses and tools is expected to be with the organization. Few question which can be asked to various teams in order to collect information can be through discussion, interviews and forums like –

- What type of information is to be protected?
- At what location is the information?
- Which information is crucial for the organization?
- What is the Operating environment and system considered for customer?
- How many routers, servers, firewalls do the system has?

Identification process may involve the below points.

Asset Management – Involves a process of operating, maintain, deploying and acquisition through disposal.

Business Environment – Environment for which protection is needed.

Governance – Establishment of policies and monitoring them for proper implementations.

Risk Assessment – To evaluate potential risk involved in an activity.

Risk Management Strategy – Approach for identify, manage and assessing risk.

management software's

PROTECT DATA

After identification of the network securities and vulnerabilities now it's the time to protect your system. This phase in the cyber security Lifecycle is also referred to as 'MITIGATE' phase as this eases the risk identified. The system here should be brought in accordance to the company policies and rules. Awareness about the different techniques available in industry should be developed among the team. This can be achieved through a series of trainings.

Access control – Understanding the various levels of access and grants.

Data Security – Providing the security for the data to be protected.

Information Protection and procedures– Information regarding processing storage and transmission of sensitive information.

Maintenance – Regular checks for preserving a specific condition.

Protective Technology – Technologies protecting your system environment.

Technologies to Protect Information

Identity and Access Management Solution, DLP Solutions, SIV (Signature Integrity Verifies), Intrusion Prevention Systems, Endpoint Solutions, Advance Persistent Threat Detection. System Patch Management Solutions

DETECT THREATS

No matter what level of protection a system may have, with the increasing threat today it may get compromised at any level. In detection phase the system may identify attack signatures and identify the level of activities carried out in the affected system. Security tolls should be able to identify normal and malicious activities. This can be considered similarly like the fire alarm in our offices or homes. It detects the fire in few seconds and throws an alarms to an environment. IDS (Intrusion Detection System) should be able to suspect the intrusion once it has happened. It should keep a close look on the attacks which are originated from within the system. Following factors can be considered for the same.

- **Anomalies and events**: – Identifying anomalies at perimeter level is primary job of all boundry level solution if that fails the entire network is playground for attacker.

can add anomalies into their threat library.

Technologies to Detect Threat Information

Intrusion Detection System, Threat Intelligence Feed, Layered Defense System, User Behavior Analytics Solution, SIEM, Threat Hunting Tools, Vulnerability Assessment,

RESPOND ATTACKS

Timely action is the key behind protecting the system for attacks. Considering our example of fire alarm if the necessary actions are not taken when the fire has occurred would result in a huge loss of resources. Similarly, if timely actions is not taken against the attacks would result in greater loss of information hampering the entire business and environment. Policies against these cyber attacks should be available prior so that timely action can be possible. Prioritization of different types of risk levels and actions against them needs to be identified clearly.

A Computer Security Incident Response Team (CSIRT) should be able to co- ordinate and manage all the activities from detection to documentation of the occurrence. Concisely, the below points can be considered.

- **Incident Respond Planning**: – Incident management is a process of reporting the events of an organization to identify, analyze, and correct risk to prevent a subsequent re-occurrence.
- **Incident Communications**: – Communication is Key for any incident response phase. This includes incident response team resource, management and the general employee base. Sharing information with Computer Security Incident Response Team (CSIRT) about facts encircle the incident at the appropriate level, Incident time and reminding them of their duties to preserve the confidentiality of any related information can spread hearsay. It will also help to for predictive intelligence and minimize the risk of information being exfiltrated from organization.
- **Cyber Incident Analysis**: – In incident analysis analyst must start with endpoint system analysis, the attacker may have left with some backdoor or attack vector for more damage. One should perform behavior analysis on all users, entities of organizational assets and try to find anomalies form that. If you find no satisfactory results then security analyst can involve threat hunting team to perform deep dive analysis on logs and correlate different data source.
- **Incident Mitigation**: – Incident Mitigation is actual process of limiting attack surface for attacker. Applying on situational controls based on all indicators of compromises. Enforcing new policies to security solutions.

Indicator of Attack vs Indicator of Compromises
1st April 2018
In "Cyber Threat"

Cyber Security Control
3rd March 2016
In "Cyber Threat"

Power of Security Operation Center
25th December 2017
In "Cyber Threat"

Author: Rohit Sadgune

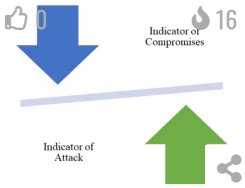
Core Working Areas :- Threat Intelligence, Digital Forensics, Incident Response, Fraud Investigation, Web Application Security Technical Certifications :- Computer Hacking Forensics Investigator | Certified Ethical Hacker | Certified Cyber crime investigator | Certified Professional Hacker | Certified Professional Forensics Analyst | Redhat certified Engineer | Cisco Certified Network Associates | Certified Firewall Solutions | Certified Network Monitoring Solution | Certified Proxy Solutions

WEBSITE

TAGGED CYBER INCIDENT ANALYSIS, CYBER SECURITY LIFECYCLE, CYBER THREAT INFORMATION, INCIDENT RSPONSE PALN

RELATED ARTICLES

Cyber Security Control



Indicator of Attack vs Indicator of Compromises

Computer and Network Log Analytics

Principal Components of Security Information Event Management

← Previous
Types of System Software

Next →
Power of Security Operation Center

step look by CSIRT so that this information will be very handy for future cyber incidents.

Technologies to responds cyber security incidents

Security Information Event Management, Incident Ticketing System, Threat Intelligence Feed, Digital Forensics Solutions

INCIDENT RECOVER

Incident recovery is nothing but putting entire compromised posture of company back to production environment. We can call this as the last stage in the cyber security Lifecycle. This helps us to recover and protect a business from disaster. Documentations also needs to be considered in order to understand the loopholes and improvement areas.

Recovery Planning- It's a long term process which goes through continuous stages of improvement. Based on the earlier lessons learned the weakness of organization can be encountered and thus can be worked upon. The entire team working together should have a thorough understanding of the organizations technologies, processes, interacting teams, protocols, dependency maps and motive behind each execution plan.

How to report cyber Incident

- How did this Incident happen?
- Did the intruder access sensitive data?
- If so, how much sensitive information were raided?
- Who are the attackers
- When did the Computer Security Incident Response Team find out?
- Who was the vulnerability internally?

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

CAPTCHA Code *

Notify me of follow-up comments by email.

Notify me of new posts by email.

POST COMMENT

INDICATOR OF ATTACKS | INDICATOR OF COMPROMISE

FOLLOW US

Facebook

LinkedIN

Twitter

Google+

BLOG STATS BY WEEK

49,012 Hits

CYBER THREAT CATEGORIES

TOP CYBER SECURITY ARTICLES

THREAT HUNTING SCENARIOS