Incident and Vulnerability Handling

Session Goals

Schulung der wichtigsten Aspekte des Managements von Schwachstellen und Security Incidents.

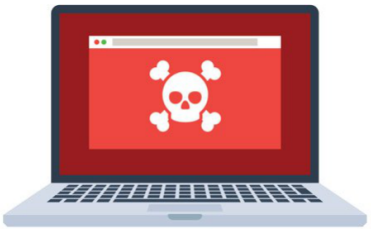
Incident Handling

Security incident

Ein Sicherheitsvorfall bezieht sich auf eine Situation, die auf eine mögliche Verletzung (Breach/Leak) der Systeme oder Daten einer Organisation oder auf das Versagen von Schutzmaßnahmen hindeutet.

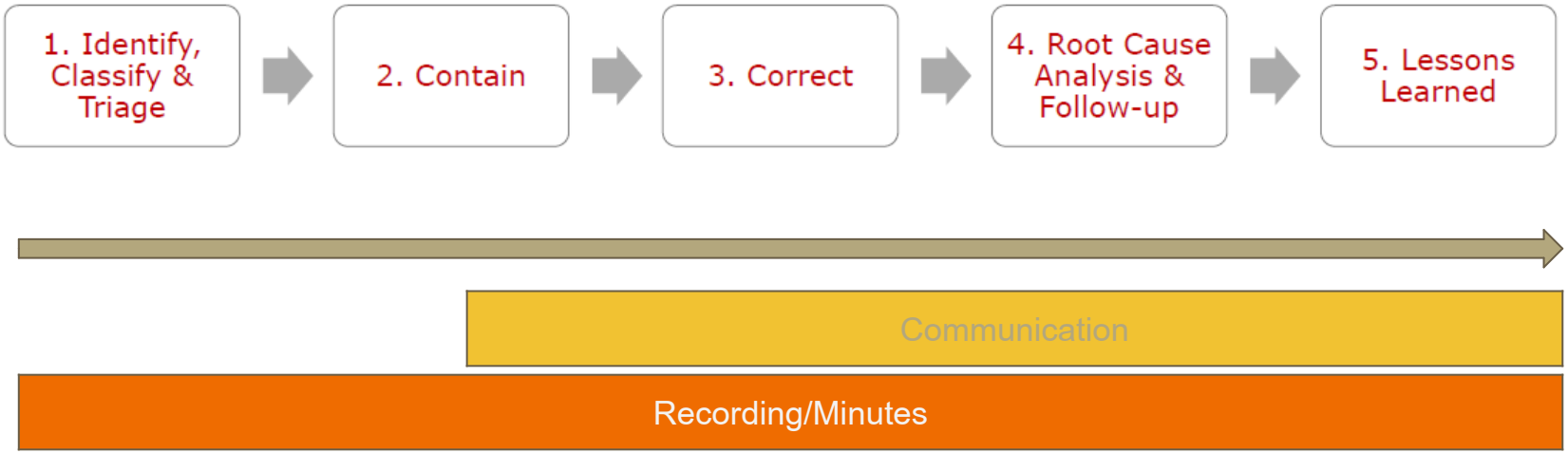
Im OT-Kontext wirkt sich ein Ereignis auf die System-Hardware oder -software aus, während ein Vorfall die Produktionstätigkeit unterbricht.

Der Schweregrad (Severity) und das Risiko für die Organisation unterscheiden Sicherheitsereignisse von unbedeutenden Vorfällen.



Security Incident Management Process

Das Management von Sicherheitsvorfällen im OT-Bereich konzentriert sich auf die unverzügliche Identifizierung und Analyse von Sicherheitsbedrohungen.



How Do Security Incident Management Plans Work?

Strategien für das Management von „Security Incidents“ umreißen in der Regel Maßnahmen zum Umgang von Bedrohungen und deren Risiken durch „Security Incidents“.

Sobald eine Bedrohung erkannt wird, wird der Plan aktiviert und die erforderlichen Teammitglieder werden zusammengestellt.

Die erste Maßnahme in den meisten dieser Pläne besteht darin, eine umfassende Untersuchung des Vorfalls einzuleiten, wobei der Schwerpunkt auf den Auswirkungen auf das System, die Daten oder die Benutzeraktivitäten liegt.

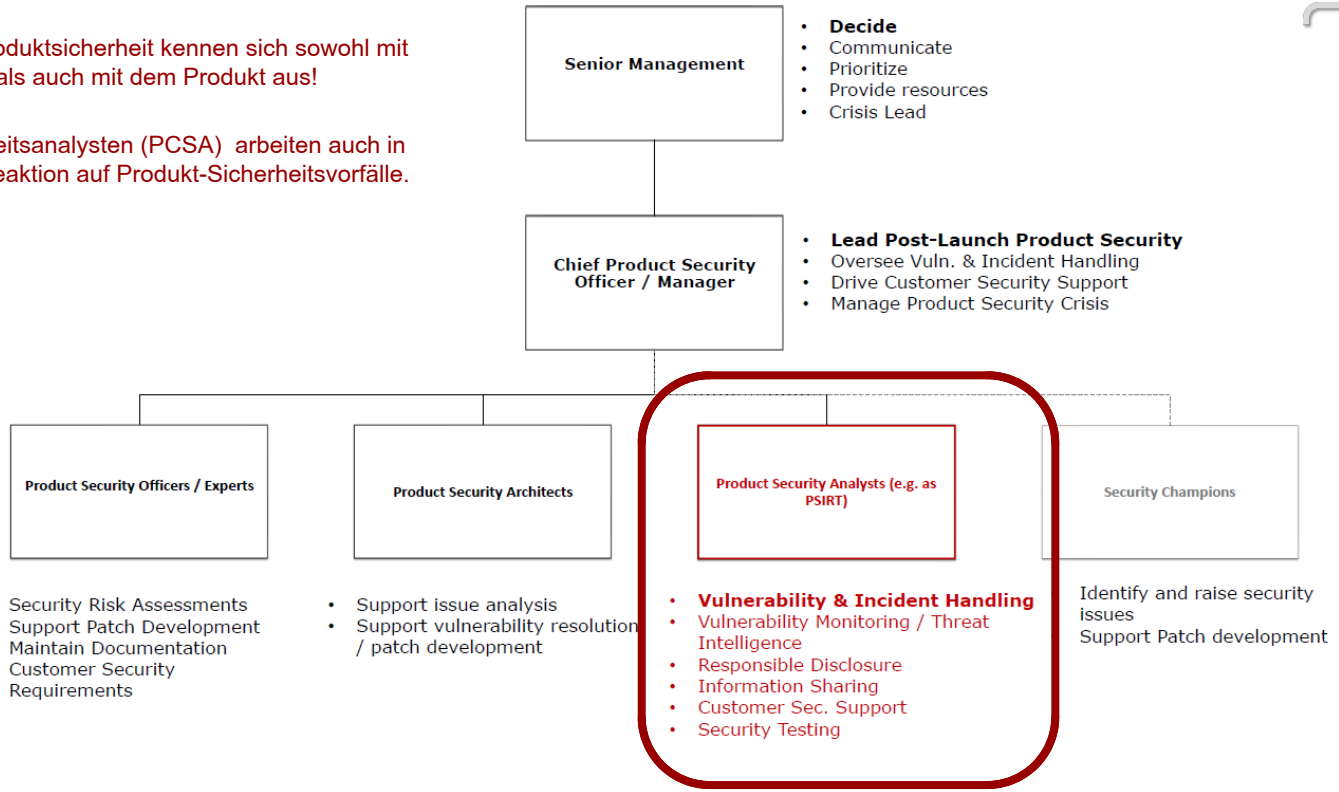
Wichtiger ist allerdings eine erste grobe Einschätzung der Lage um Sofortmassnahmen zu ergreifen, wie das Abschalten oder Segregieren von Systemen oder Netzen!

We are in the world of Product Security

An

Analysten für Produktsicherheit kennen sich sowohl mit Cybersicherheit als auch mit dem Produkt aus!

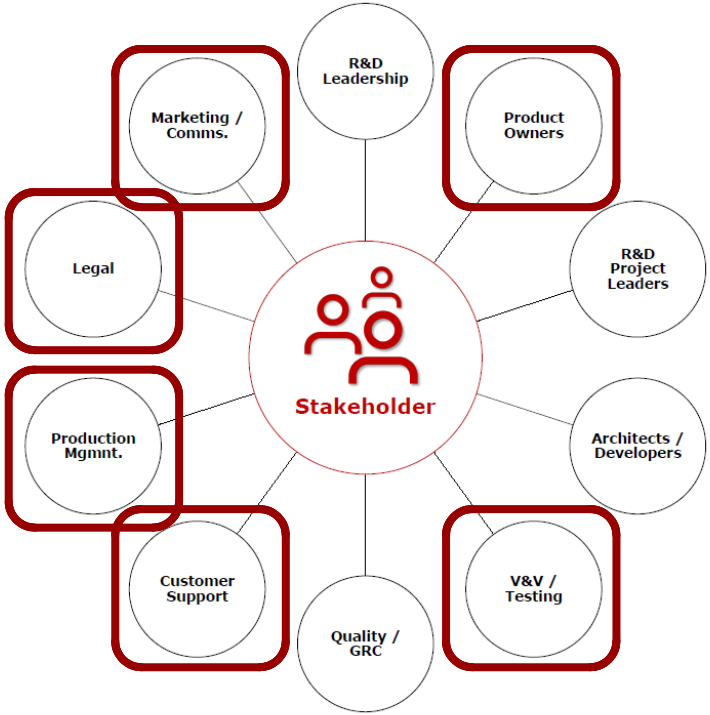
Produkt-Sicherheitsanalysten (PCSA) arbeiten auch in Teams für die Reaktion auf Produkt-Sicherheitsvorfälle.



The Product Security Analyst!

- Vulnerability & Incident Handling
  - Vulnerability Handling & Threat Intelligence
  - Responsible Disclosure Notification
  - Information Sharing
  - Customer Security Support
  - Security Testing

The IR Stakeholder Challenge



Typisch für die Sicherheit in der Produktentwicklung Umgebung.

Tools

Werkzeuge können Dokumentvorlagen sein, aber auch Analysewerkzeuge.

Forensische Werkzeuge und Wissen kommen zum Einsatz.

Schwerpunkt heute: Abläufe und Dokumentation

CIRP - Cyber security Incident Response Protocol

Als wesentliches Werkzeug kann die Vorlage eines solchen Protokolls gesehen werden.

Es kann als beliebiges Dokument oder als Bestandteil eines Ticket-Systems geführt werden.

Es unterliegt besonderen Vertraulichkeitsansprüchen.

Es führt durch den Fall.

Die Aufgabe

Üben sie Incident Response in dem Sie das Protokoll korrekt ausfüllen und den Vorfall zum Abschluss führen.

Verteilen Sie innerhalb der Gruppe entsprechend die Ihrer Ansicht nach erforderlichen Rollen. Mehrfach-Zuteilungen sind zulässig.

Benutzen Sie das zur Verfügung gestellte Material.

Wie arbeiten in Breakout Räumen.

Mehr Material

Wer Interesse hat, bekommt Zugriff auf unser github Repository und kann so auch die Entwicklung der Vorlagen verfolgen und künftig frei nutzen.

Ein Einbringen über das github Issue system ist willkommen.

Das Repository ist privat. Bei Interesse bitte eine E-Mail mit dem github-Konto an: chris.ditze-stephan@zentric.com und der Betreff sollte “[prodsec access] enthalten. (https://github.com/cidies/prodsec)

References

ISO/IEC 27035-2

Information technology — Security techniques — Information security incident management — Part 2:Guidelines to plan and prepare for incident response

ISO/IEC 30111

Information technology — Security techniques — Vulnerability handling processes

CVE

Common Vulnerability Enumeration
https://www.cve.org/

CWE

Common Weakness Enumeration
https://cwe.mitre.org/

CVSSv3

https://www.first.org/cvss/specification-document

The DFIR Report

https://thedfirreport.com/