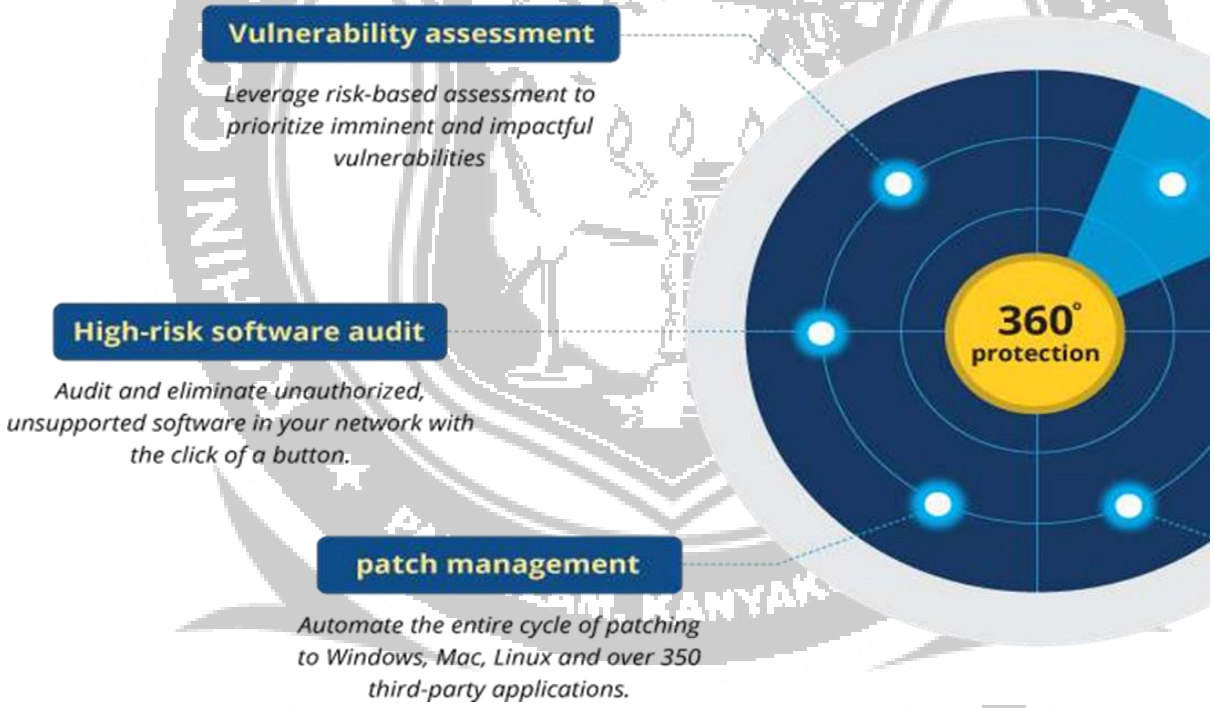
UNIT IV

TECHNICAL SECURITY

Vulnerability Management-Security Event Management-Forensic Investigations

VULNERABILITY MANAGEMENT

Vulnerability management is vital to endpoint security and is one of the most proactive approaches to need out security weaknesses before they lead to a breach.



Prioritize with comprehensive vulnerability assessment:

- Identify vulnerabilities along with their context, such as CVSS and severity scores,to ascertain priority, urgency, and impact.
- Gain Leverage are dedicated tab on publicly disclosed and zero-day vulnerabilities, and utilize work-arounds to mitigate them before the fixes arrive.
- Isolate and identify vulnerabilities in critical assets, namely databases and webservers, that hold critical data and perform crucial business operations.

- recommendations on high-profile vulnerabilities procured based on above riskfactors

SECURITY AND EVENT MANAGEMENT:

Security information and event management (**SIEM**) is a field within the field of computer security, where software products and services combine security information management (SIM)and security event management (SEM).

They provide real-time analysis of security alerts generated by applications and network hardware. Vendors sell SIEM as software, as appliances, or as managed services; these productsare also used to log security data and generate reports for compliance purposes

Components

Basic SIEM Infrastructure

The essential components of a SIEM are as follows:[30]

- A data collector forwards selected audit logs from a host (agent based or host basedlog streaming into index and aggregation point)[31][32]
- An ingest and indexing point aggregation point for parsing, correlation, anddata normalization[33]
- A search node that is used to for visualization, queries, reports, and alerts (analysistake place on a search node)

FORENSIC INVESTIGATIONS

Forensic investigation is **the act of utilizing science to establish facts or evidence which is tobe used for crime based trials or proceeding**. Many different fields of science can be appliedfor forensic investigations or forensic studies including biology, medicine, anthropology and even engineering.

- Physical Matching.
- Fingerprint Matching.
- Hair and fibre analysis.
- Ballistic Analysis.
- Blood Spatter Analysis.
- DNA Analysis.
- Forensic Pathology.
- Chemical Analysis

7 Steps of a Crime Scene Investigation

1. Identify Scene Dimensions. Locate the focal point of the scene. ...
2. Establish Security. Tape around the perimeter. ...
3. Create a Plan & Communicate. Determine the type of crime that occurred. ...
4. **Conduct** Primary Survey. ...
5. Document and Process Scene. ...
6. **Conduct** Secondary Survey. ...
7. Record and Preserve Evidence.

Three types of investigations to research and develop explanations, such as **descriptive investigation, comparative investigation, and experimental investigation**.

The **six phases of the forensic investigation process** areRequirement Analysis;
Data Retrieval;
Reliability;
Evidence Review
Evidence Representation
Repository of Data Explanation

The Requirement Analysis include methods of contrastive analysis, operational analysis, distributional analysis, immediate constituents analysis, componential analysis, transformational analysis, method of semantic differentiation.