## Exam Cram Notes: Enhancing Security Capabilities

### 1. Overview

Enhancing security capabilities involves improving an organization's ability to detect, prevent, and respond to cyber threats. This includes **implementing advanced security tools, automation, continuous training, and adapting to emerging threats**.

---

## 2. Security Awareness & Training

✅ **Security Awareness Programs –** Educate employees on security best practices.
✅ **Phishing Simulations –** Test users' ability to recognize phishing attempts.
✅ **Insider Threat Awareness –** Train staff to detect and report suspicious behavior.
✅ **Role-Based Training –** Tailor security training based on job functions.

🔷 **Best Practices:**

- Conduct regular security training and simulated attacks.
- Make security a **shared responsibility** across the organization.
- Encourage employees to report security incidents **without fear**.

---

## 3. Automation & Orchestration

✅ **Security Orchestration, Automation, and Response (SOAR) –** Automates security processes to reduce response time.
✅ **Security Information and Event Management (SIEM) –** Collects and analyzes security logs for real-time threat detection.
✅ **Automated Threat Intelligence Feeds** – Ingests real-time threat intelligence data.
✅ **Automated Patch Management –** Deploys security updates to reduce vulnerabilities.

🔷 **Tools:** Splunk SOAR, IBM QRadar, Microsoft Sentinel, Palo Alto Cortex XSOAR

---

## 4. Advanced Threat Detection & AI/ML Security

✅ **Artificial Intelligence (AI) for Security –** Uses machine learning to detect anomalies.
✅ **User and Entity Behavior Analytics (UEBA)** – Identifies unusual user activity that may indicate an attack.
✅ **Threat Hunting –** Uses proactive search techniques to detect hidden threats.
✅ **Deep Packet Inspection (DPI) –** Examines network traffic at a granular level for suspicious patterns.

🔷 **Tools:** Darktrace, Vectra AI, CrowdStrike Falcon

---

## 5. Zero Trust Security Model

✅ **Principle of Least Privilege (PoLP) –** Users and systems get only the access they **absolutely need**.
✅ **Micro-Segmentation –** Divides the network into secure zones to limit attack spread.
✅ **Continuous Authentication & Verification –** Regularly checks users' identity during sessions.
✅ **Adaptive Access Control** – Grants access based on user behavior and device risk.

🔷 **Best Practices:**

- **"Never trust, always verify."**
- **Monitor all network traffic** to detect insider threats.
- **Implement Multi-Factor Authentication (MFA)** for critical systems.

---

## 6. Advanced Endpoint Protection

✅ **Next-Gen Antivirus (NGAV) –** Uses AI to detect unknown malware.
✅ **Endpoint Detection & Response (EDR) –** Provides real-time visibility into endpoint threats.
✅ **Application Whitelisting –** Allows only approved applications to run.
✅ **Isolation & Sandboxing –** Runs suspicious files in a controlled environment.

🔷 **Tools:** CrowdStrike Falcon, Microsoft Defender ATP, Carbon Black

---

## 7. Security Testing & Red Teaming

✅ **Penetration Testing (Red Teaming) –** Simulates real-world attacks to find security gaps.
✅ **Vulnerability Scanning (Blue Teaming)** – Identifies and patches system weaknesses.
✅ **Purple Teaming –** Collaborates between red and blue teams to enhance defense strategies.
✅ **Bug Bounty Programs –** Engages ethical hackers to find vulnerabilities.

🔷 **Tools:** Metasploit, Burp Suite, Nessus, OpenVAS

---

## 8. Cloud Security Enhancements

✅ **Cloud Access Security Broker (CASB) –** Monitors and secures cloud applications.
✅ **Cloud Security Posture Management (CSPM) –** Detects misconfigurations in cloud environments.

✅ **Secure DevOps (DevSecOps)** – Integrates security into the software development lifecycle.
✅ **Container Security –** Secures Docker, Kubernetes, and other containerized environments.

🔷 **Tools:** AWS Security Hub, Microsoft Defender for Cloud, Prisma Cloud

---

## 9. Identity & Access Management (IAM) Enhancements

✅ **Identity Federation –** Uses Single Sign-On (SSO) for seamless access.
✅ **Privileged Access Management (PAM) –** Monitors high-risk privileged accounts.
✅ **Biometric Authentication –** Uses fingerprints, retina scans, or facial recognition.
✅ **Behavioral Biometrics –** Analyzes typing speed, mouse movements, and login patterns.

🔷 **Tools:** Okta, CyberArk, Azure AD, Google Workspace IAM

---

## 10. Incident Response & Forensics Improvements

✅ **Incident Response Playbooks –** Predefined workflows for security incidents.
✅ **Digital Forensics & Investigation Tools –** Helps analyze attack sources and impact.
✅ **Threat Intelligence Platforms –** Provides real-time threat context.
✅ **Security Drills & Tabletop Exercises –** Prepares teams for cyber incidents.

🔷 **Tools:** Autopsy, FTK Imager, TheHive, MISP

---

## 11. Key Exam Takeaways

✅ **Train employees continuously** to recognize and prevent security threats.
✅ **Implement AI-driven security solutions** for proactive threat detection.
✅ **Adopt a Zero Trust approach** to minimize unauthorized access risks.
✅ **Leverage automation and orchestration** to improve response time.
✅ **Regularly conduct security tests (red/blue teaming, pentests).**
✅ **Enhance cloud security** with CASB and secure DevOps practices.
✅ **Strengthen identity and access controls** using IAM and MFA.
✅ **Improve incident response capabilities** with playbooks and forensics tools.