(10th December 2025) - JAGUAR COHORT
Made by Chris Cownden
I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

9th Lab Recap Guide: Security+

Recording is here

Timestamps

00:00 Client Onboarding Process Explained

23:03 SEC Plus Business Impact Analysis

31:47 OSSEC: File Integrity Monitoring Tool

53:41 Configuration Baseline for Security

01:03:54 "Two-Factor Authentication Tools"

01:25:29 "Secure Development Lifecycle Overview"

01:32:36 GitHub for Linux Secrets

01:49:57 Middleware Facilitates Backend Requests

01:53:58 Practical Security for Professionals

Resources

- Exam Compass
- GitHub
- Jon's Security Architecture Handbook
- Jon's Secure By Design PPT
- Jon's Security Architecture Github
- OSSEC - Open Source IDS (Intrusion Detection System)
- Here are all the resources mentioned in the recording:
- Burp Suite - Web application security scanner and proxy
- OWASP Top 10 - Key web application vulnerabilities list to memorize
- MX Toolbox - Online tool to check DNS records, SPF, DKIM, DMARC etc.
- CVSS Calculator - Tool for grading/assessing the severity of vulnerabilities
- Contact Jon on WhatsApp = +447818426065
- Contact Optima-IT for CV Review and Career Support = studentsupport@optima-it.co.uk

(10th December 2025) - JAGUAR COHORT
Made by Chris Cownden
I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

Other Recordings To Date

Date	Order	Recordings	Lab Recap Guides
10th December	Lab 9	RECORDING	THIS ONE
3rd December	Lab 8	RECORDING	RECAP GUIDE
26th November 2025	Lab 7	RECORDING	RECAP GUIDE
19th November 2025	NO SESSION AS JON WAS ABSENT		
12th November 2025	Lab 6	RECORDING	RECAP GUIDE
5th November 2025	Lab 5	RECORDING	RECAP GUIDE
2nd November 2025	3rd Sunday	RECORDING	
29th October 2025	Lab 4	RECORDING	RECAP GUIDE
22nd October 2025	Lab 3	RECORDING	RECAP GUIDE
19th October 2025	2nd Sunday	RECORDING	
15th October 2025	Lab 2	RECORDING	RECAP GUIDE
8th October 2025	Lab 1	RECORDING	RECAP GUIDE
5th October 2025	1st Sunday	RECORDING	

Core Concepts

Security Architecture

- Configuration Baseline: Default secure settings for systems.
- Vulnerability Types: Software/version, configuration (e.g., default passwords), code-based (e.g., hard-coded passwords).

- Isolation/Sandboxing: Restricting device communication for security (air-gapping, guest networks).
- Full Disk Encryption (FDE): Encrypts all data at rest.
- Patch Management: Continuous process—identify, test, deploy, and (if needed) roll back.
- EDR: Active agent on endpoints, detects/responds to threats.

File & System Security

- File Integrity Monitoring (FIM): Hash-based integrity check, e.g., OSSEC—detects file tampering.
- NTFS/EFS: NTFS is Windows' modern file system; EFS adds built-in encryption.
- Expect questions on how to protect data at rest, integrity, and what processes/tools (and commands) should be in place.

API Security & GitHub Dangers

- **API Keys:** Credentials for accessing backend services—should *never* be public (e.g., in code/environment files).
- **.env Files:** Used by devs to store secrets/configs—should be protected.
- **GitHub Security:** Secrets in public repos = critical vulnerability (know how attackers search for them!).

CVSS Framework

- CVSS (Common Vulnerability Scoring System): Framework to rate vulnerability risk/severity—be able to determine criticality based on access, complexity, privileges needed, scope, confidentiality, integrity, and availability impact.

Digital Signature Algorithms

- ECDSA (Elliptic Curve Digital Signature Algorithm): Efficient, small-key digital signatures (great for IoT/low-power).
- ECC/DSA: ECC is the math, ECDSA is the security implementation.

Practical Security Controls

- Port Security: Physical (USB/SATA) versus network (802.1X) – how to prevent attack vectors.
- Least Privilege: Only give users the permissions they need—"minimum permissions to do your job."

- Segmentation: Network segmentation for critical infra (ICS, SCADA)—prevents lateral movement.

Jon's Github Workshop

Starts at [1.29.03 to 2:06.09]

1. Get a GitHub Account

- Go to GitHub.com.
- Click **Sign Up** if you don't already have an account.
- You can sign up using **Google**, **Apple**, or your **email**.
- Choose a username and set a strong password (at least 15 characters).
- Complete any verification steps (including enabling two-factor authentication if prompted).

2. Find John's Repository

- Once you're logged in, use the GitHub search bar at the top.
- https://github.com/heaps1345/security-architecture

3. Open the Repository

- Click on the repository name "**Security Architecture"** to open its main page.
- You'll see a list of files, a README, etc.

4. Locate and Click the 'Fork' Button

- Look in the top-right area of the repository page: there's a **Fork** button.
- Click **Fork**.

5. Configure Your Fork

- After clicking **Fork**, you'll be prompted to:
  - Choose an owner: Select your own GitHub username/account.
  - Name your repository: By default, it will copy the original name, but you can give it a custom name (e.g., "security-architecture-YOURNAME" if you wish).
  - Description (optional): Add a short note like "Working through secure architecture, John's repo."
- Click **Create Fork**.

6. Your Personal Copy is Ready!

- In a few seconds, GitHub creates your own copy ("fork") of John's repo.
- You'll be redirected to your new fork, where you can see your username in the URL: `github.com/YOURUSERNAME/security-architecture`
- You can now make changes, review code, and try security exercises independently without affecting John's original version.

7. What Next?

- Start exploring or editing files (such as the `.env` file mentioned in the lesson).
- Document security issues, practice fixes, and learn version control as you go.

Terminology

OWASP Top 10: List of critical web application security risks.
Metasploit: Popular penetration testing framework for exploiting vulnerabilities.
Burp Suite: Tool used for web vulnerability scanning and testing.
OTA: Over-the-air, method of wirelessly updating devices.
EFS: Encrypting File System, Windows file-level encryption feature.
HSM: Hardware Security Module, device for cryptographic and key management functions.
TPM: Trusted Platform Module, hardware chip for cryptographic operations.
PUP: Potentially Unwanted Program, software not explicitly classified as malware.
FRR: False Rejection Rate, metric for biometric systems rejecting authorized users.
FAR: False Acceptance Rate, metric for biometric systems accepting unauthorized users.
SCAP: Security Content Automation Protocol, standard for automated vulnerability scanning.
BIA: Business Impact Analysis, process identifying critical business functions.
BCP: Business Continuity Plan, strategy for continuing operations during disruptions.
IoT: Internet of Things, interconnected smart devices with limited computational resources.
ECC/ECDSA: Elliptic Curve Cryptography/Digital Signature Algorithm, efficient cryptographic methods.
AV: Antivirus, software for preventing, detecting, and removing malware.
ARO: Annual Rate of Occurrence, risk assessment metric estimating yearly threat frequency.
ACL: Access Control List, rule-based mechanism for file/directory access.
FIM: File Integrity Monitoring, tool for detecting unauthorized file changes.
SPF: Sender Policy Framework, DNS record authorizing mail servers for a domain.
DKIM: DomainKeys Identified Mail, email authentication using digital signatures.
DMARC: Domain-based Message Authentication, Reporting & Conformance, email validation system.
GitHub: Online repository for collaborative code development and version control.
Patch Management: Process of identifying, testing, and deploying code fixes.
EDR: Endpoint Detection and Response, software monitoring endpoints for threats.

API Key: Unique identifier for authenticating API requests.
CVSS: Common Vulnerability Scoring System, industry standard for rating vulnerability severity.

Acronyms

OTA = Over The Air
EFS = Encrypting File System
NTFS = New Technology File System
SFC = System File Checker
HSM = Hardware Security Module
TPM = Trusted Platform Module
PUP = Potentially Unwanted Program
FRR = False Rejection Rate
FAR = False Acceptance Rate
CER = Crossover Error Rate
CRC = Cyclic Redundancy Check
SAML = Security Assertion Markup Language
SCAP = Security Content Automation Protocol
OVAL = Open Vulnerability and Assessment Language
SASE = Secure Access Service Edge
BCP = Business Continuity Plan
BIA = Business Impact Analysis
SLE = Single Loss Expectancy
BPA = Business Process Automation
IDS = Intrusion Detection System
IDP/IPS = Intrusion Detection/Prevention System (spoken about as IPS/IDS, implied, commonly paired in Security+)
AV = Antivirus
WAF = Web Application Firewall
ALE = Annual Loss Expectancy
ARO = Annual Rate of Occurrence
ACL = Access Control List (spoken as file access control list)
FIM = File Integrity Monitoring
SPF = Sender Policy Framework
DKIM = DomainKeys Identified Mail
DMARC = Domain-based Message Authentication, Reporting & Conformance
EDR = Endpoint Detection and Response
FDE = Full Disk Encryption
KEK/KEK = Key Encryption Key
OPAL = Standard for Self-Encrypting Drives
API = Application Programming Interface
JWT = JSON Web Token

(10th December 2025) - JAGUAR COHORT

Made by Chris Cownden

I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

2FA = Two-Factor Authentication

GUI = Graphical User Interface (implied with discussion of "front-end")

Analogies

Secure By Design

Think of "secure by design" like building a house with security in mind from the very first blueprint.

Instead of adding locks, alarms, or sturdy doors after the house is finished, you plan for them at every step by choosing strong materials, positioning windows so they're hard to reach, and designing entryways that limit unwanted access. You're not just sticking on a padlock as an afterthought; you're making sure safety is part of the structure itself.

In cybersecurity, "secure by design" means baking in protection from the start so your network, software or system is ready for intruders from day one, not scrambling to patch up gaps after trouble strikes.

API keys

An API key is like a visitor badge you get when entering a secure building:

- The badge proves you're allowed inside (authentication).
- It lets you access only the rooms you're approved for (authorization).
- If the badge is lost or misused, security can deactivate it and issue a new one.
- So an API key is essentially your digital access badge that tells a system, "I'm allowed to be here, and here's what I can do."

Questions

What does OTA stand for and what does it mean?

- **Answer:** OTA means "Over The Air." It refers to wireless updates sent to devices via cellular, Wi-Fi, etc.

(10th December 2025) - JAGUAR COHORT

Made by Chris Cownden

I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

Which acronym refers to a piece of hardware/software/firmware for cryptographic key management?

- **Answer:** HSM (Hardware Security Module) is the correct answer.

What does EFS stand for?

- **Answer:** Encrypting File System. It's a Windows feature to encrypt files at the file level.

What is a PUP?

- **Answer:** Potentially Unwanted Program—not classified as malware, but often installed during downloads and may be unwanted or affect security/performance.

What is the measure of likelihood that a biometric security system will incorrectly reject an authorized user?

- **Answer:** False Rejection Rate (FRR).

Which protocol enables automation of vulnerability scanning and compliance checking?

- **Answer:** SCAP (Security Content Automation Protocol).

Which acronym refers to a plan for keeping operations running during/after a disruptive event?

- **Answer:** BCP (Business Continuity Plan).

Which digital signature algorithm is most efficient (small key size, low computational requirement)?

- **Answer:** ECDSA (Elliptic Curve Digital Signature Algorithm).

(10th December 2025) - JAGUAR COHORT

Made by Chris Cownden

I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

Which type of software prevents, detects, and removes malware?

- **Answer:** AV (Antivirus).

What is an annual rate of occurrence?

- **Answer:** It's an estimate of how often a threat will successfully exploit a vulnerability per year.

Which mechanism is rule-based access control for files/directories?

- **Answer:** File Access Control List (ACL).

What is File Integrity Monitoring (FIM)?

- **Answer:** It uses hashes to monitor files for unauthorized changes; alerts security teams to potential tampering.

Which DNS record allows domain owners to specify authorized mail servers?

- **Answer:** SPF (Sender Policy Framework).

What's the purpose of security configuration baselines?

- **Answer:** It's the minimum configuration for network appliances/servers ensuring they're secure and not vulnerable by default.

What are examples of vulnerabilities?

- **Answer:** Software/version vulnerabilities, code-based vulnerabilities (such as hardcoded passwords), configuration vulnerabilities (like default credentials).

What is isolation in endpoint security?

- **Answer:** Separating endpoints (devices) or networks (like guest networks) to reduce attack surface—e.g., air-gapping, sandboxing.

(10th December 2025) - JAGUAR COHORT

Made by Chris Cownden

I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

What is FDE?

- **Answer:** Full Disk Encryption—encrypts all data on a disk, protecting data at rest.

What is a self-encrypting drive?

- **Answer:** A disk drive whose hardware controller encrypts data automatically.

What is a 'KEK'?

- **Answer:** Key Encryption Key—used as a private key to encrypt the bulk data encryption key (DEK).

What is Opal in device encryption?

- **Answer:** Opal is a Trusted Computing Group standard for self-encrypting drives.

What is a patch and what's patch management?

- **Answer:** A patch is a code update fixing bugs or vulnerabilities. Patch management is the process of identifying, testing, deploying, and reverting patches.

What is EDR?

- **Answer:** Endpoint Detection and Response—software agent monitoring endpoints for early detection and response to threats.

Could a malicious USB battery charger exploit a mobile device?

- **Answer:** Yes, but often requires user consent; zero-click attacks are rare.

What can be done to prevent malicious USB/device attacks?

- **Answer:** Disable or monitor USB ports, enforce port security, centrally manage configuration.

(10th December 2025) - JAGUAR COHORT

Made by Chris Cownden

I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

What is the purpose of User and Entity Behavior Analytics (UEBA)?

- **Answer:** UEBA monitors/analyzes behavior to detect threats based on deviations from normal activity.

What control best protects ICS/SCADA in industrial systems?

- **Answer:** Network segmentation.

What's the key benefit of web filtering in security operations?

- **Answer:** Preventing malware infections and phishing from malicious websites.

What does the Principle of Least Privilege enforce?

- **Answer:** Grants users minimum permissions necessary to perform their tasks.

What is an environment file (.env)?

- **Answer:** A config file containing secrets like API keys, database credentials, etc.—should not be publicly accessible.

What is an API key?

- **Answer:** A unique identifier used to authenticate requests in APIs (Application Programming Interfaces).

What risks exist if secrets (API keys/passwords, etc.) are exposed in a codebase or GitHub?

- **Answer:** If exposed, attackers can access or compromise services (critical security issue).

How do we rate vulnerability severity (e.g., API key exposure)?

- **Answer:** Using CVSS: Internet-accessible, low complexity, no privileges, high confidentiality/integrity impact. ***Result: Critical.***

(10th December 2025) - JAGUAR COHORT

Made by Chris Cownden

I’m creating recap guides as revision notes for future use. Please use this document as you see fit.