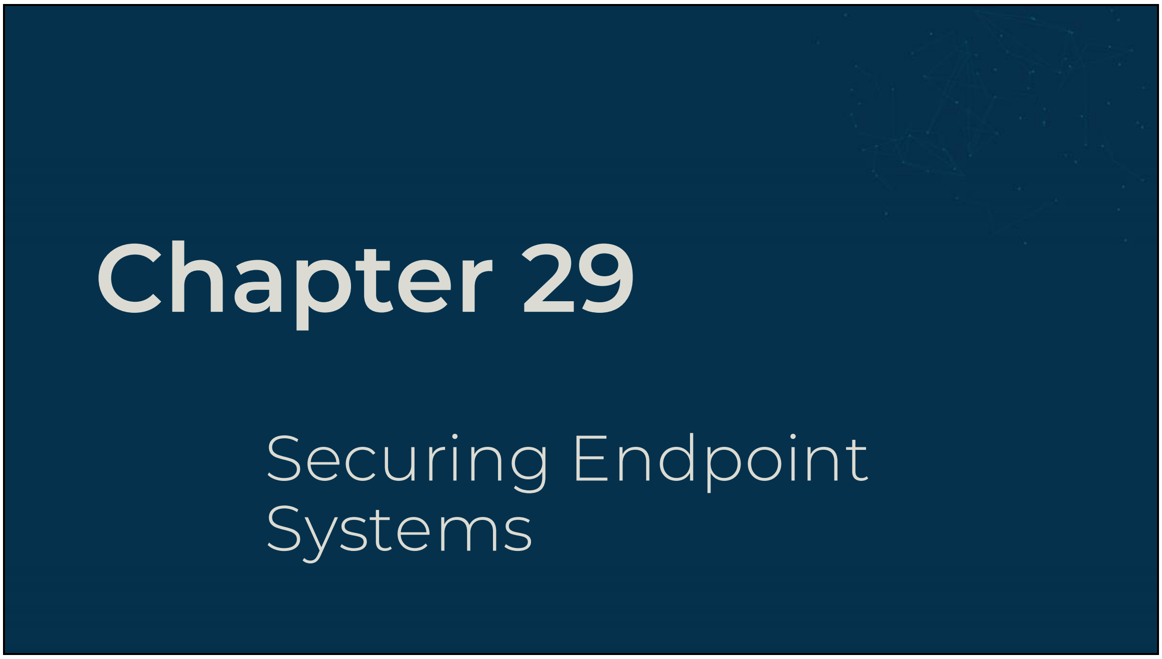


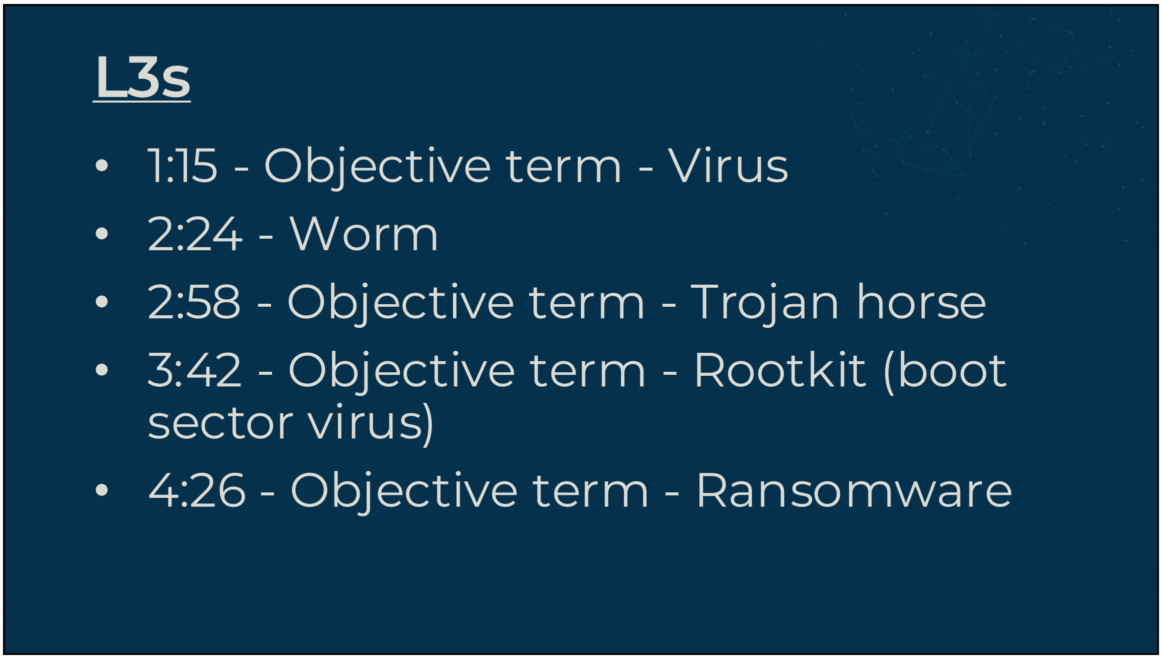
Chapter 29

Securing Endpoint Systems

Episode 29.01

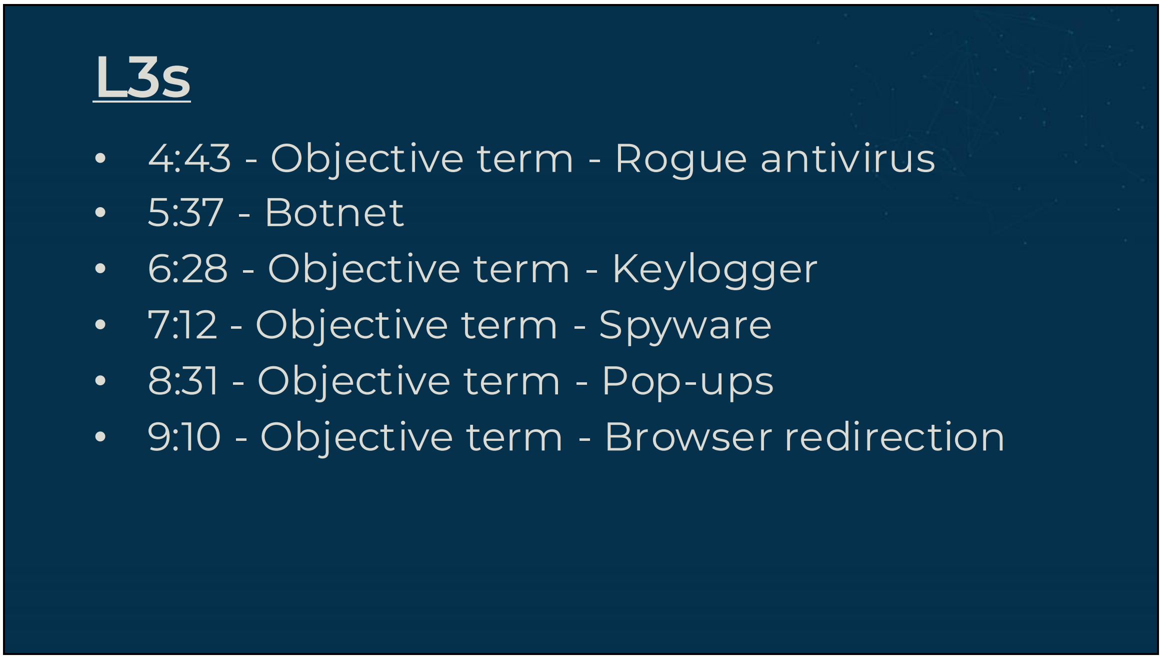
Episode title: **Malware**

Objective: 2.4 Summarize types of malware and tools / methods for detection, removal, and prevention



L3s

- 1:15 - Objective term - Virus
- 2:24 - Worm
- 2:58 - Objective term - Trojan horse
- 3:42 - Objective term - Rootkit (boot sector virus)
- 4:26 - Objective term - Ransomware



L3s

- 4:43 - Objective term - Rogue antivirus
- 5:37 - Botnet
- 6:28 - Objective term - Keylogger
- 7:12 - Objective term - Spyware
- 8:31 - Objective term - Pop-ups
- 9:10 - Objective term - Browser redirection

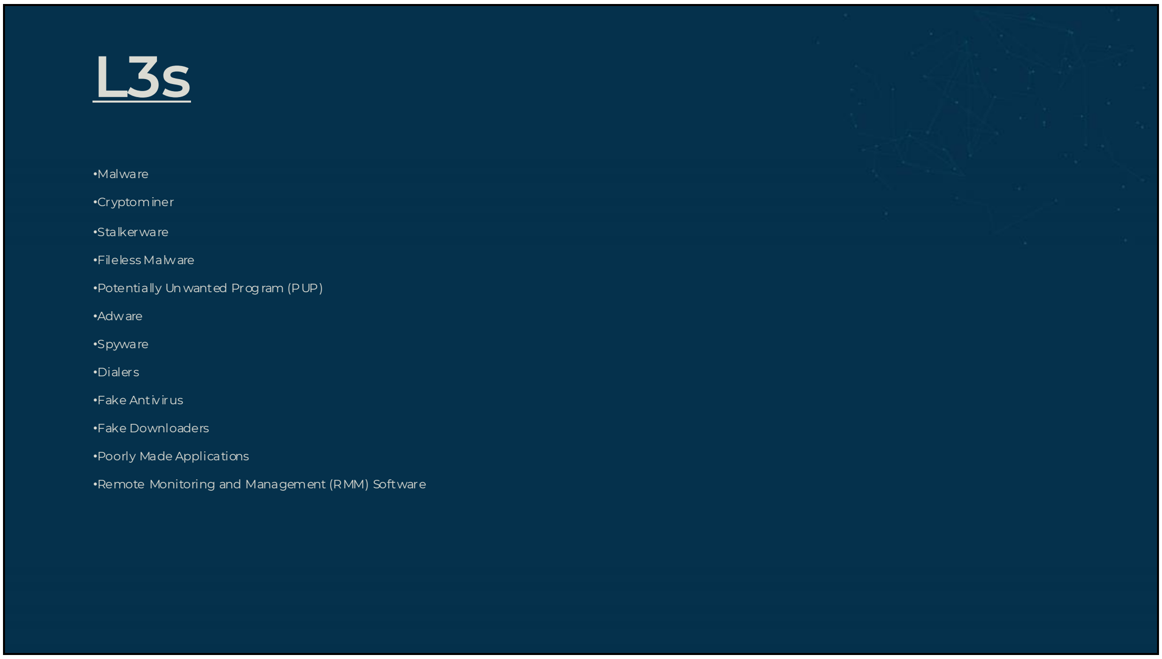
L3s

- 9:45 - Objective term - Security/desktop alerts
- 10:06 - Objective term - OS update failure
- 10:27 - Spam
- 11:17 - Hijacked e-mail
- 11:35 - Automated replies
- 12:01 - Objective term - Invalid certificates
- 13:12 - Objective term- Network LAN tap
- Cryptomining
- Stalkerware
- Fileless malware
- Potentially unwanted program (PUP)

Episode 29.02

Episode title: **Malware Part II**

Objective: 2.4 Summarize types of malware and tools / methods for detection, removal, and prevention



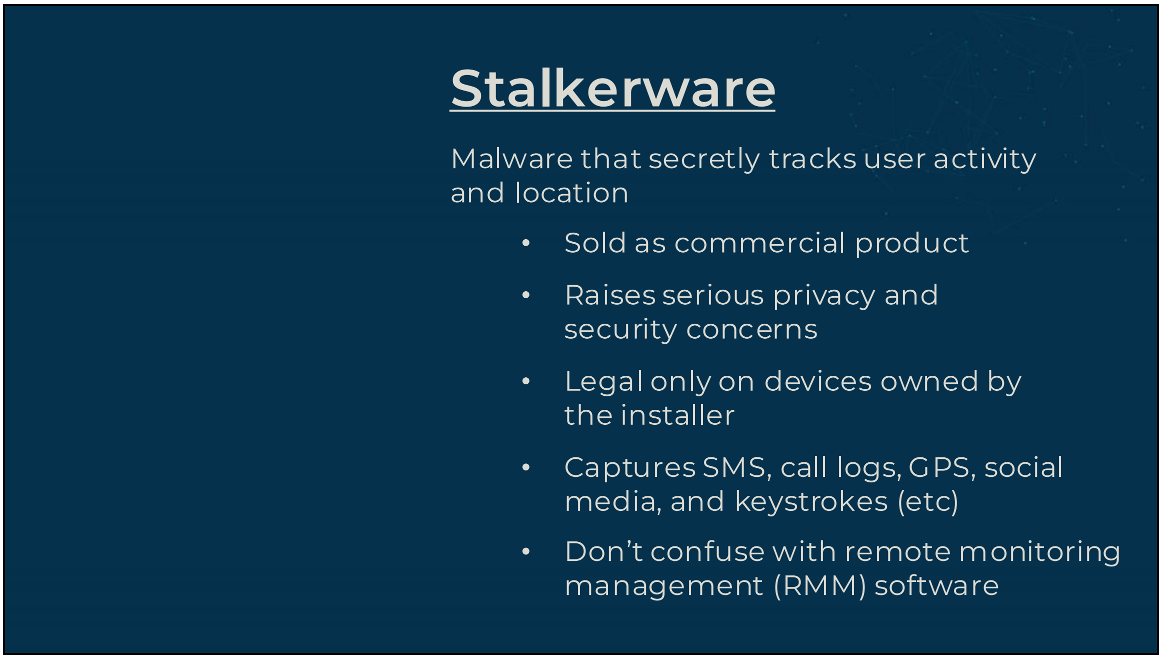
L3s

- Malware
- Cryptominer
- Stalkerware
- Fileless Malware
- Potentially Unwanted Program (PUP)
- Adware
- Spyware
- Dialers
- Fake Antivirus
- Fake Downloaders
- Poorly Made Applications
- Remote Monitoring and Management (RMM) Software

Cryptojacking Malware

Malware that secretly uses system resources to mine cryptocurrency

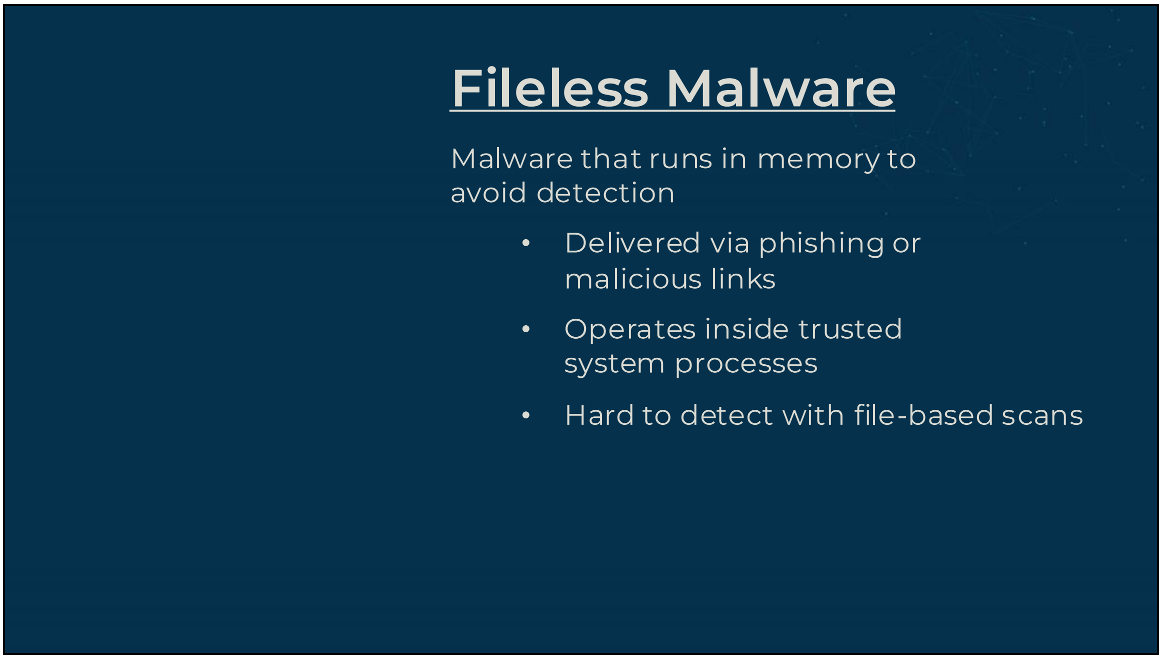
- Spreads via downloads or email attachments
- Hijacks CPU/GPU for mining operations
- Keeps network connections open unnaturally long
- Detected by monitoring persistent connections and anti-malware tools



Stalkerware

Malware that secretly tracks user activity and location

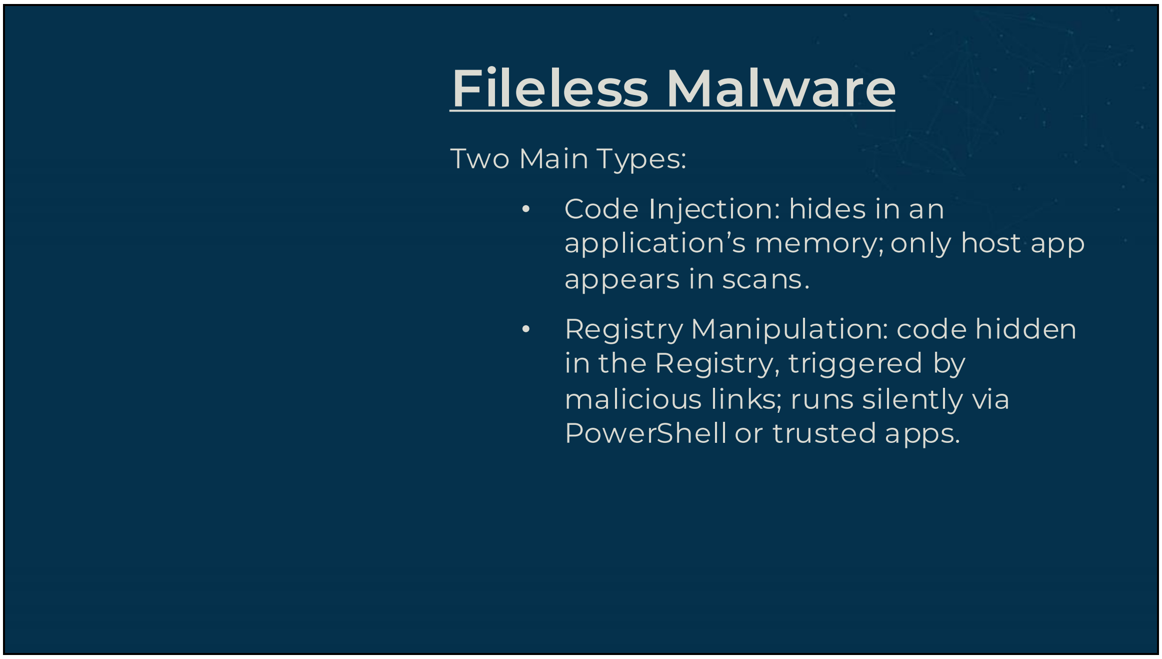
- Sold as commercial product
- Raises serious privacy and security concerns
- Legal only on devices owned by the installer
- Captures SMS, call logs, GPS, social media, and keystrokes (etc)
- Don’t confuse with remote monitoring management (RMM) software



Fileless Malware

Malware that runs in memory to avoid detection

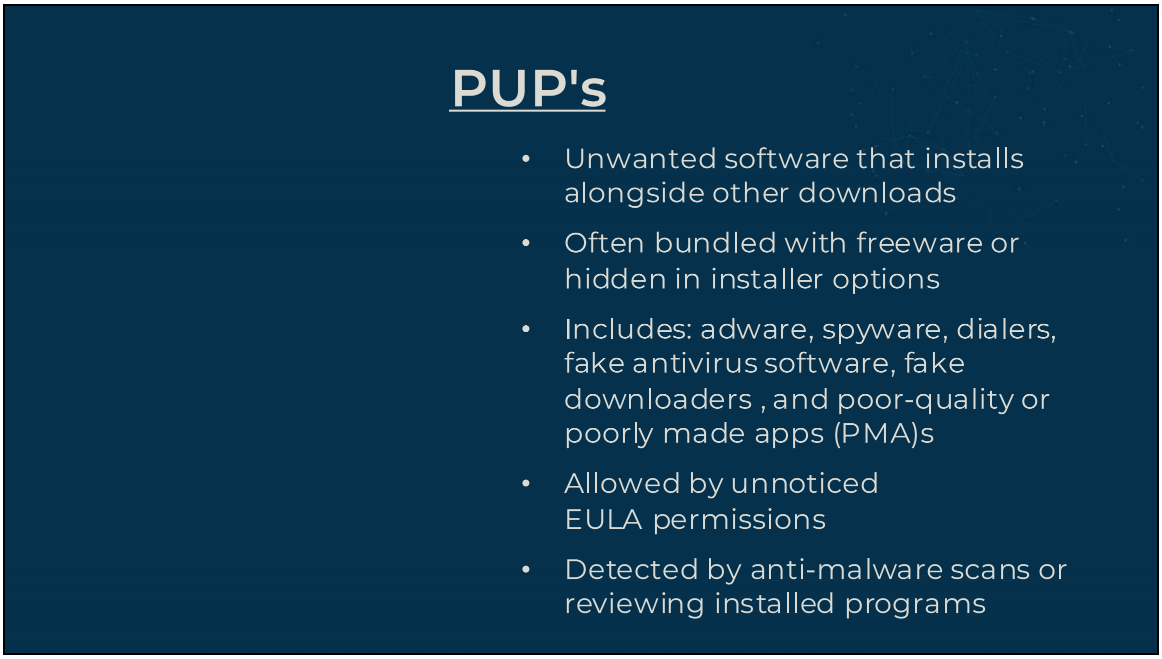
- Delivered via phishing or malicious links
- Operates inside trusted system processes
- Hard to detect with file-based scans



Fileless Malware

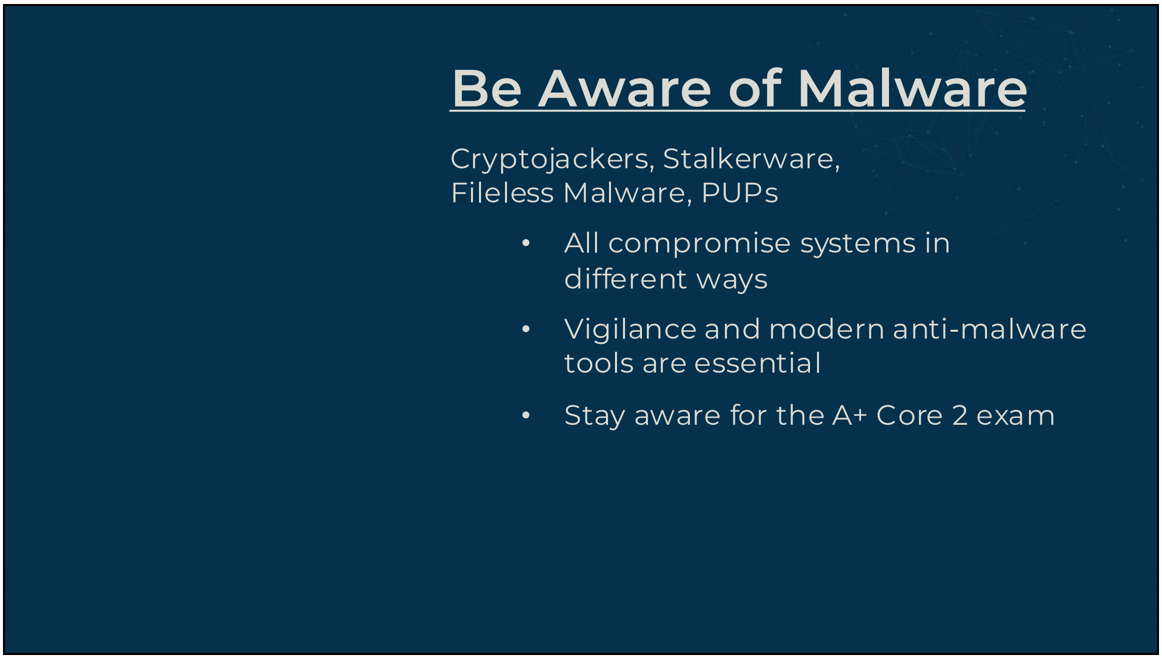
Two Main Types:

- Code Injection: hides in an application’s memory; only host app appears in scans.
- Registry Manipulation: code hidden in the Registry, triggered by malicious links; runs silently via PowerShell or trusted apps.



PUP's

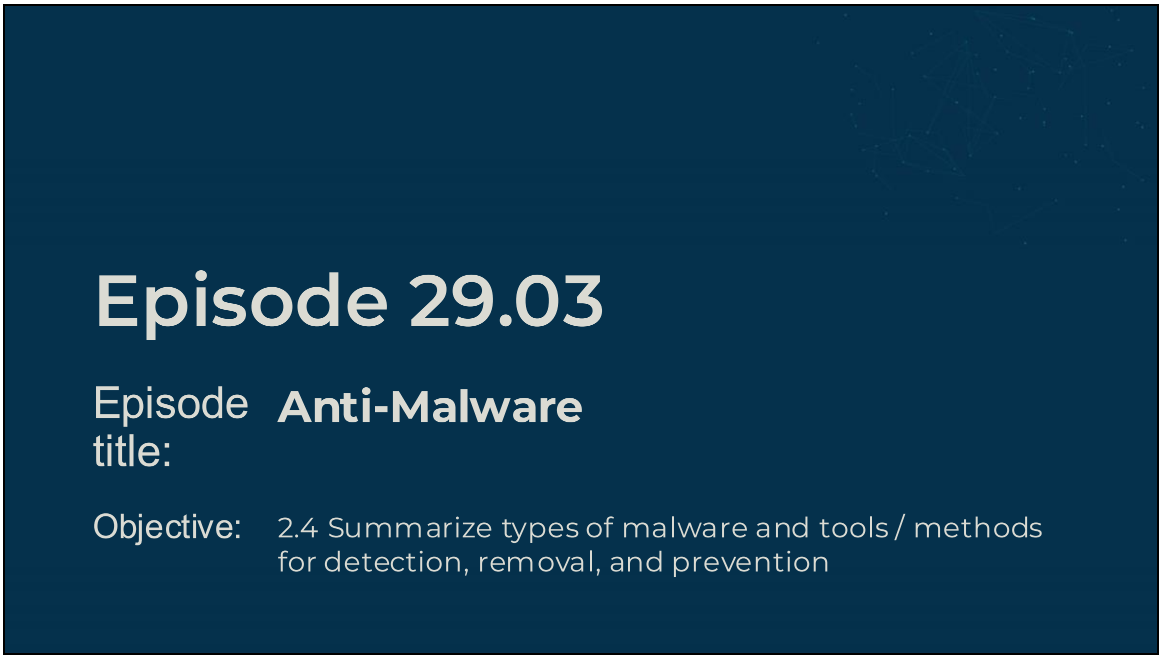
- Unwanted software that installs alongside other downloads
- Often bundled with freeware or hidden in installer options
- Includes: adware, spyware, dialers, fake antivirus software, fake downloaders , and poor-quality or poorly made apps (PMA)s
- Allowed by unnoticed EULA permissions
- Detected by anti-malware scans or reviewing installed programs



Be Aware of Malware

Cryptojackers, Stalkerware,
Fileless Malware, PUPs

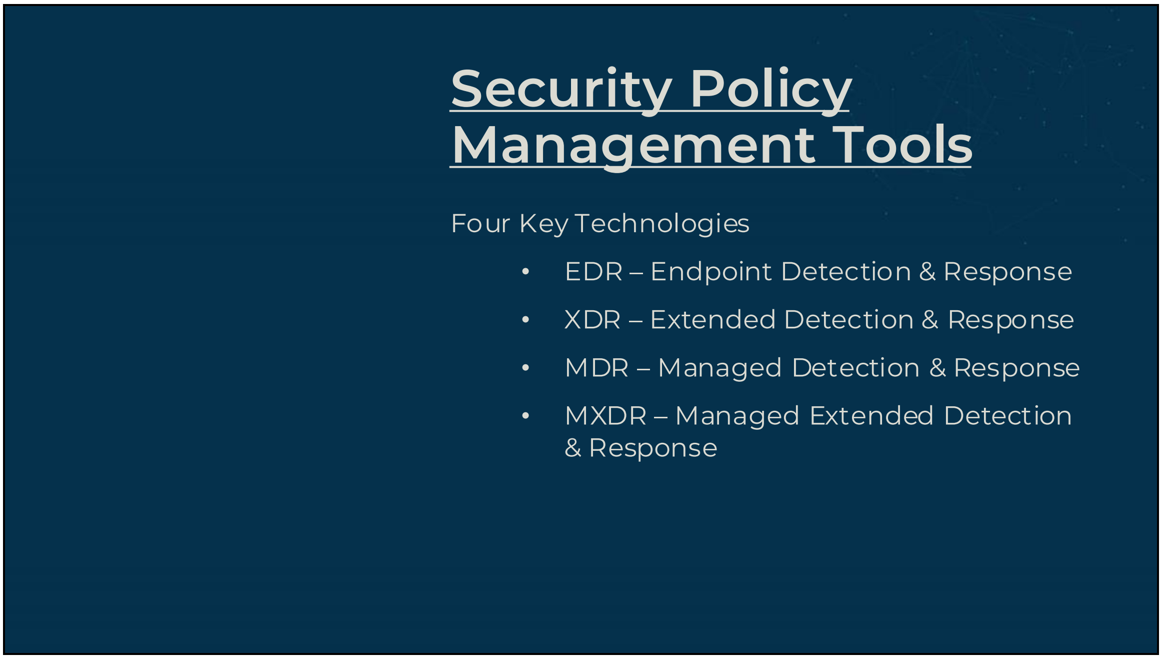
- All compromise systems in different ways
- Vigilance and modern anti-malware tools are essential
- Stay aware for the A+ Core 2 exam



Episode 29.03

Episode title: **Anti-Malware**

Objective: 2.4 Summarize types of malware and tools / methods for detection, removal, and prevention



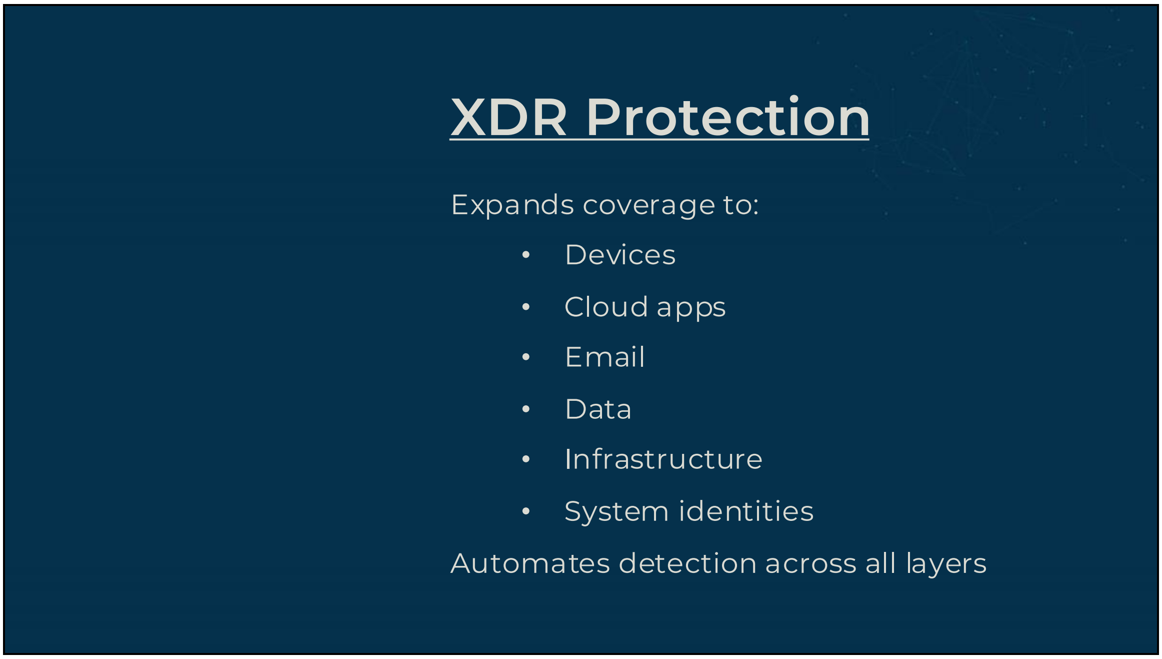
Security Policy Management Tools

Four Key Technologies

- EDR – Endpoint Detection & Response
- XDR – Extended Detection & Response
- MDR – Managed Detection & Response
- MXDR – Managed Extended Detection & Response

Endpoint Detection & Key Features

- Monitors endpoint devices
- Uses CTI, machine learning, automation
- Detects existing & potential threats
- Incident Triage: Filters false positives
- Threat Hunting: Finds hidden threats
- Data Aggregation: Makes informed security decisions



XDR Protection

Expands coverage to:

- Devices
- Cloud apps
- Email
- Data
- Infrastructure
- System identities

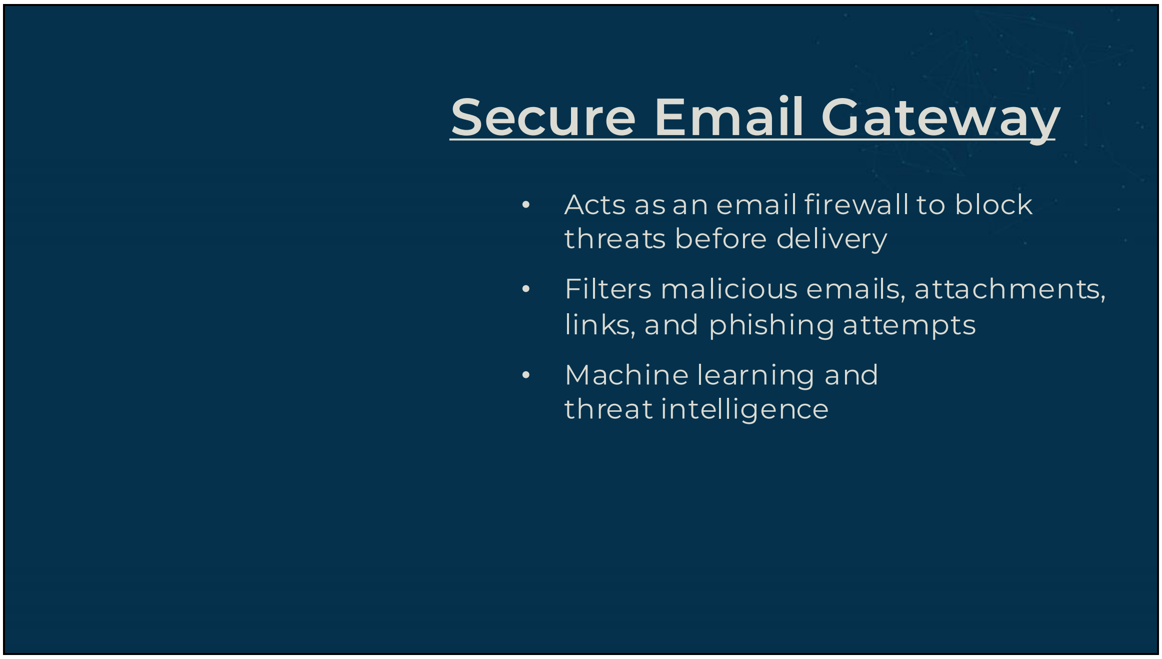
Automates detection across all layers

Managed Detection & Response

- Managed service using EDR technology
- Focuses on endpoints
- Delivered by a Managed Security Service Provider (MSSP)
- Remote monitoring, detection, and response

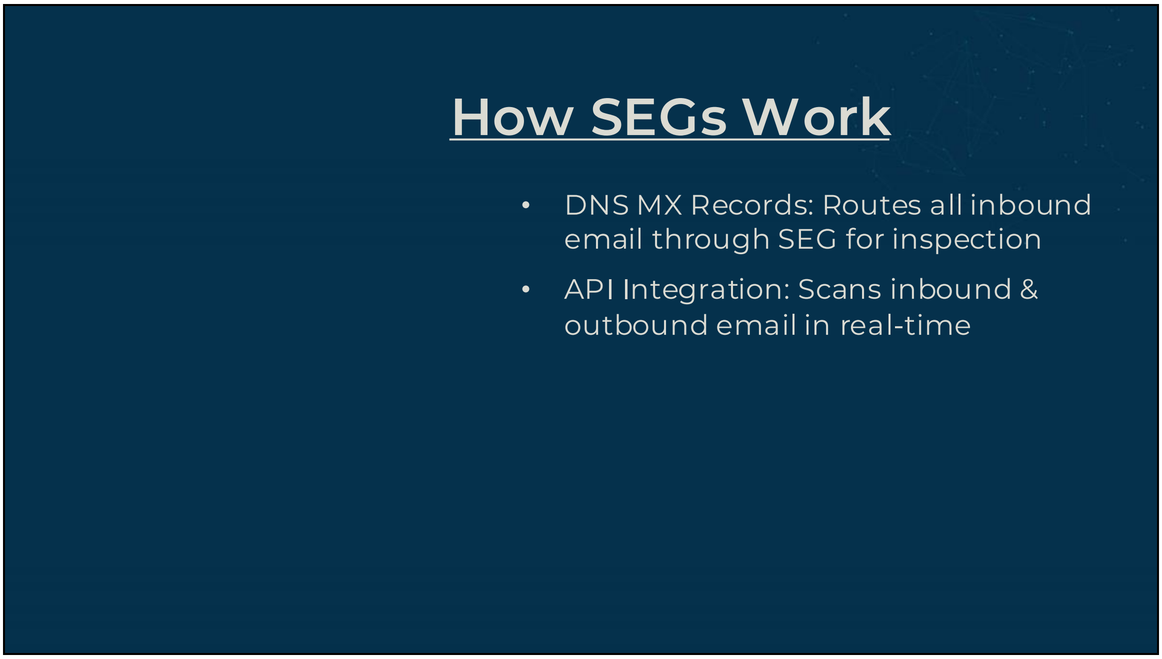
Managed Extended Detection & Response

- Managed service using XDR technology
- Covers full IT infrastructure
- Faster detection and broader protection
- Includes endpoints, cloud, and identity systems



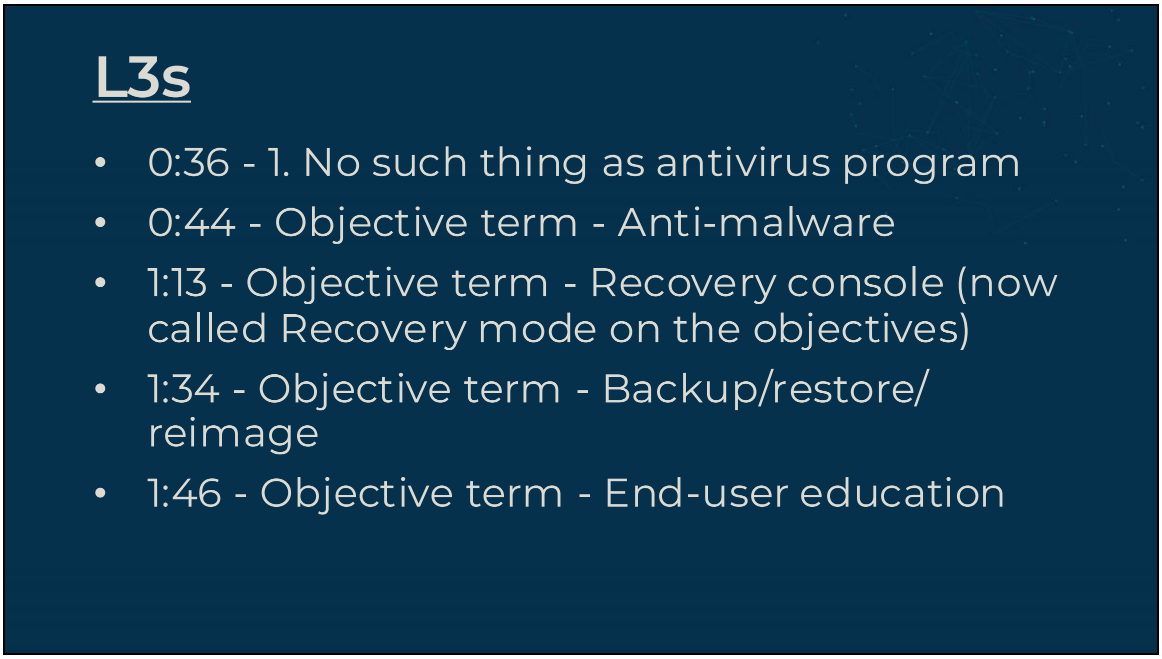
Secure Email Gateway

- Acts as an email firewall to block threats before delivery
- Filters malicious emails, attachments, links, and phishing attempts
- Machine learning and threat intelligence



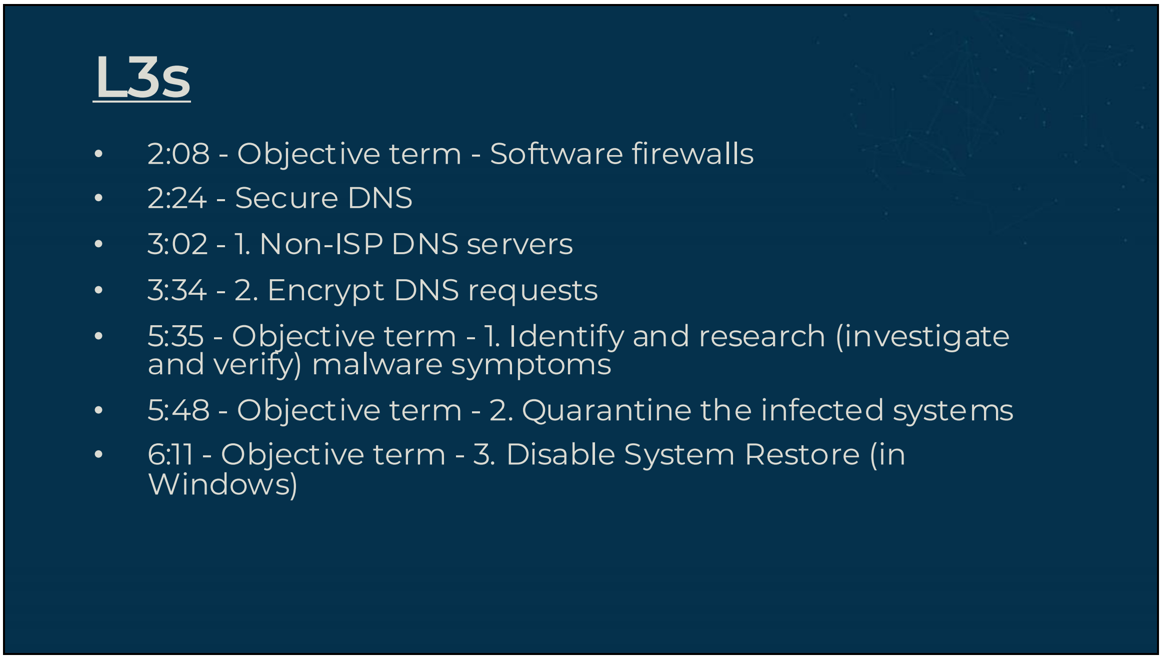
How SEGs Work

- DNS MX Records: Routes all inbound email through SEG for inspection
- API Integration: Scans inbound & outbound email in real-time



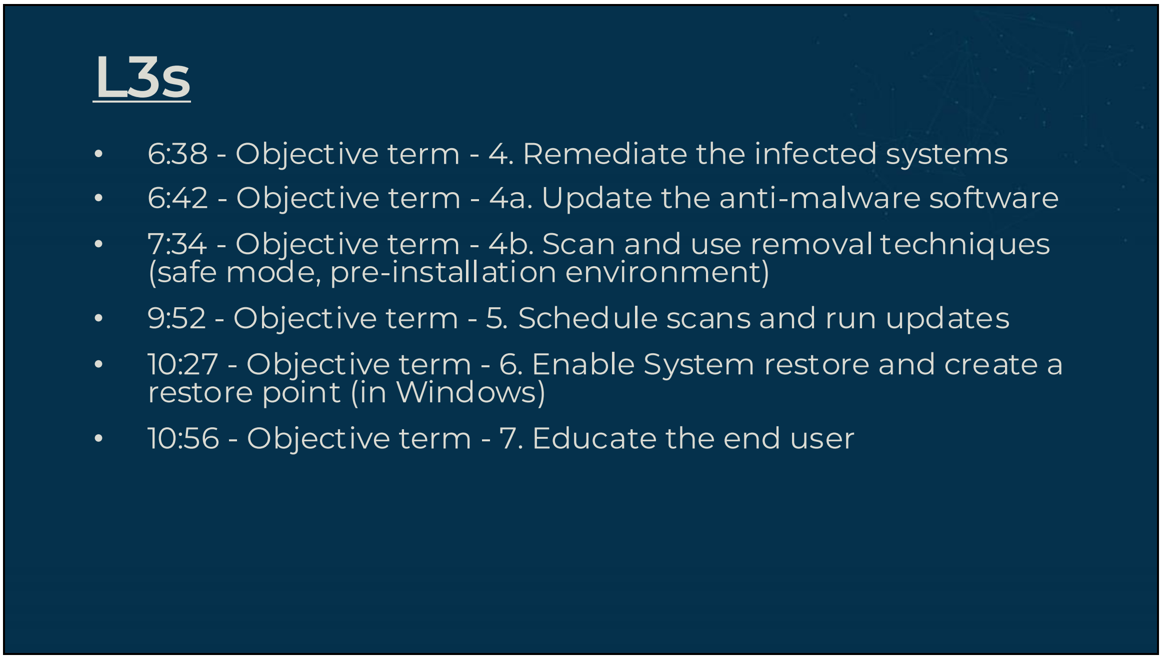
L3s

- 0:36 - 1. No such thing as antivirus program
- 0:44 - Objective term - Anti-malware
- 1:13 - Objective term - Recovery console (now called Recovery mode on the objectives)
- 1:34 - Objective term - Backup/restore/ reimage
- 1:46 - Objective term - End-user education



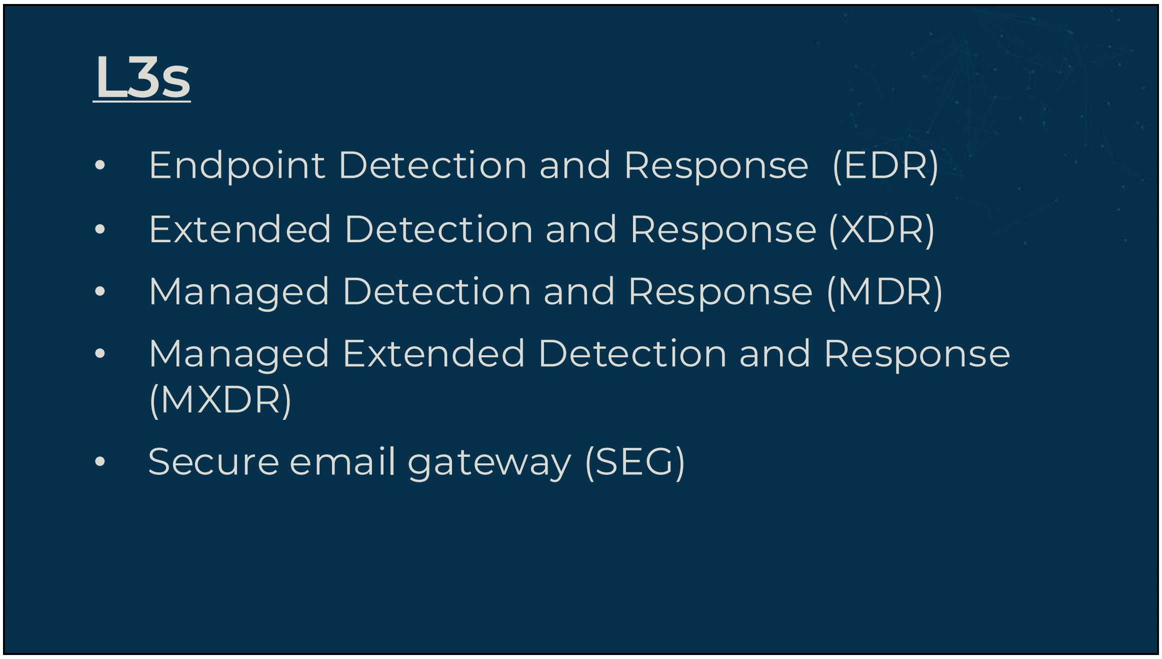
L3s

- 2:08 - Objective term - Software firewalls
- 2:24 - Secure DNS
- 3:02 - 1. Non-ISP DNS servers
- 3:34 - 2. Encrypt DNS requests
- 5:35 - Objective term - 1. Identify and research (investigate and verify) malware symptoms
- 5:48 - Objective term - 2. Quarantine the infected systems
- 6:11 - Objective term - 3. Disable System Restore (in Windows)



L3s

- 6:38 - Objective term - 4. Remediate the infected systems
- 6:42 - Objective term - 4a. Update the anti-malware software
- 7:34 - Objective term - 4b. Scan and use removal techniques (safe mode, pre-installation environment)
- 9:52 - Objective term - 5. Schedule scans and run updates
- 10:27 - Objective term - 6. Enable System restore and create a restore point (in Windows)
- 10:56 - Objective term - 7. Educate the end user



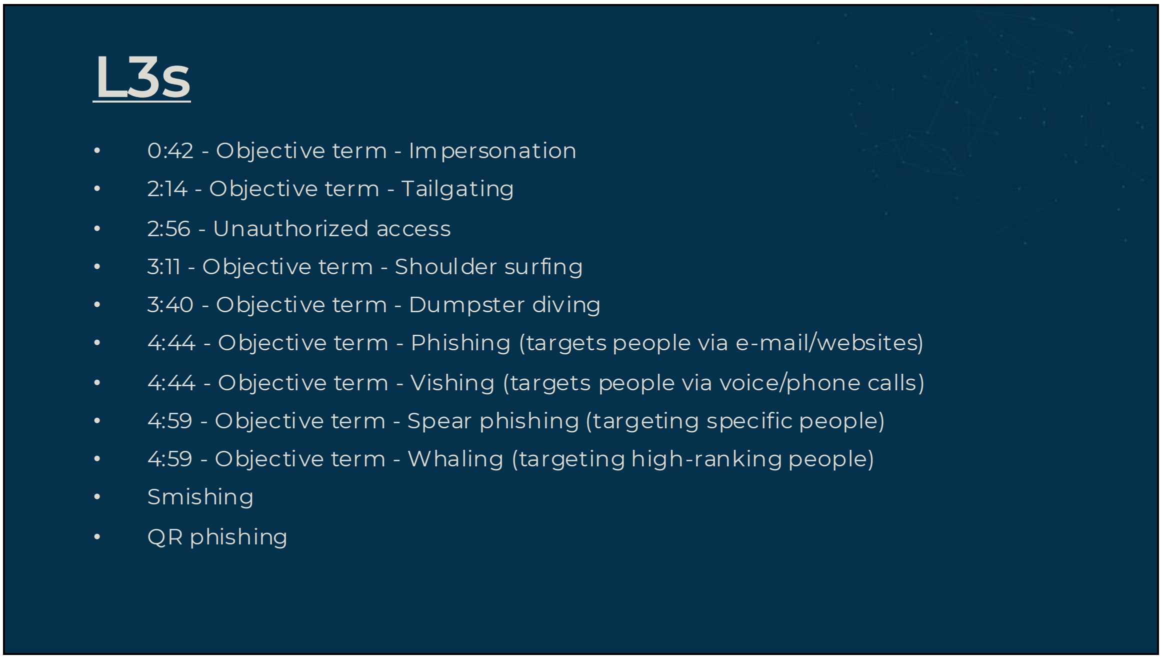
L3s

- Endpoint Detection and Response (EDR)
- Extended Detection and Response (XDR)
- Managed Detection and Response (MDR)
- Managed Extended Detection and Response (MXDR)
- Secure email gateway (SEG)

Episode 29.04

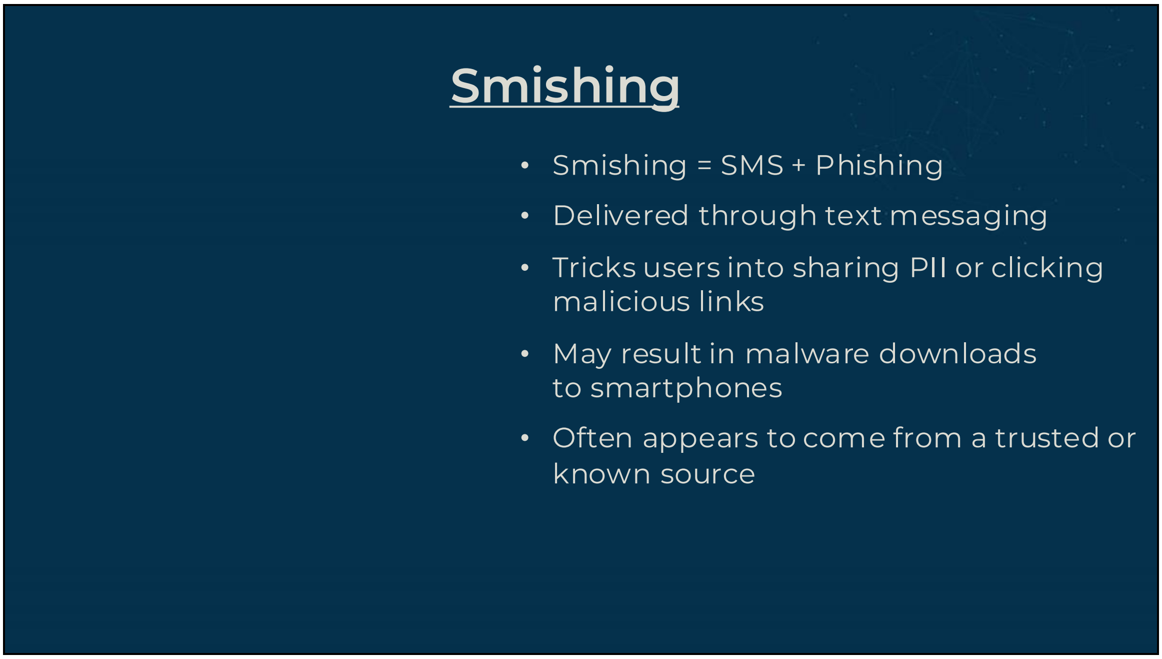
Episode title: **Social Engineering**

Objective: 2.5 Compare and contrast common social engineering attacks, threats, and vulnerabilities



L3s

- 0:42 - Objective term - Impersonation
- 2:14 - Objective term - Tailgating
- 2:56 - Unauthorized access
- 3:11 - Objective term - Shoulder surfing
- 3:40 - Objective term - Dumpster diving
- 4:44 - Objective term - Phishing (targets people via e-mail/websites)
- 4:44 - Objective term - Vishing (targets people via voice/phone calls)
- 4:59 - Objective term - Spear phishing (targeting specific people)
- 4:59 - Objective term - Whaling (targeting high-ranking people)
- Smishing
- QR phishing



Smishing

- Smishing = SMS + Phishing
- Delivered through text messaging
- Tricks users into sharing PII or clicking malicious links
- May result in malware downloads to smartphones
- Often appears to come from a trusted or known source

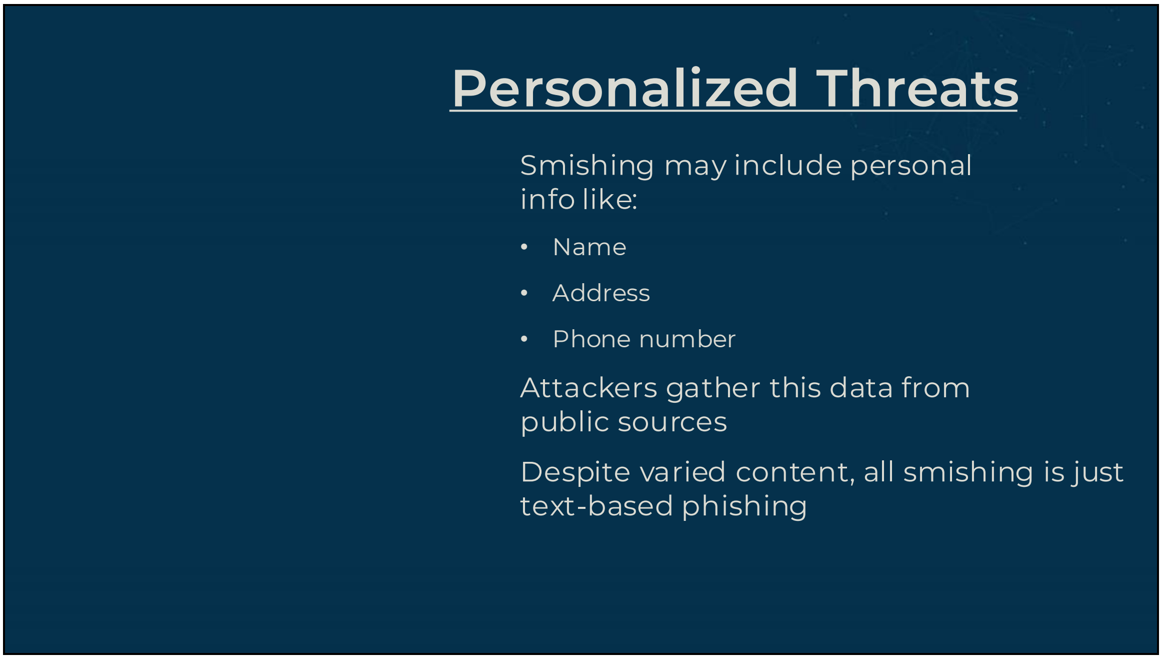
Triggers

Smishing messages create:

- Urgency
- Curiosity
- Fear

These emotional triggers pressure users to take quick action

Example tactics: fake account issues, rewards, or threats



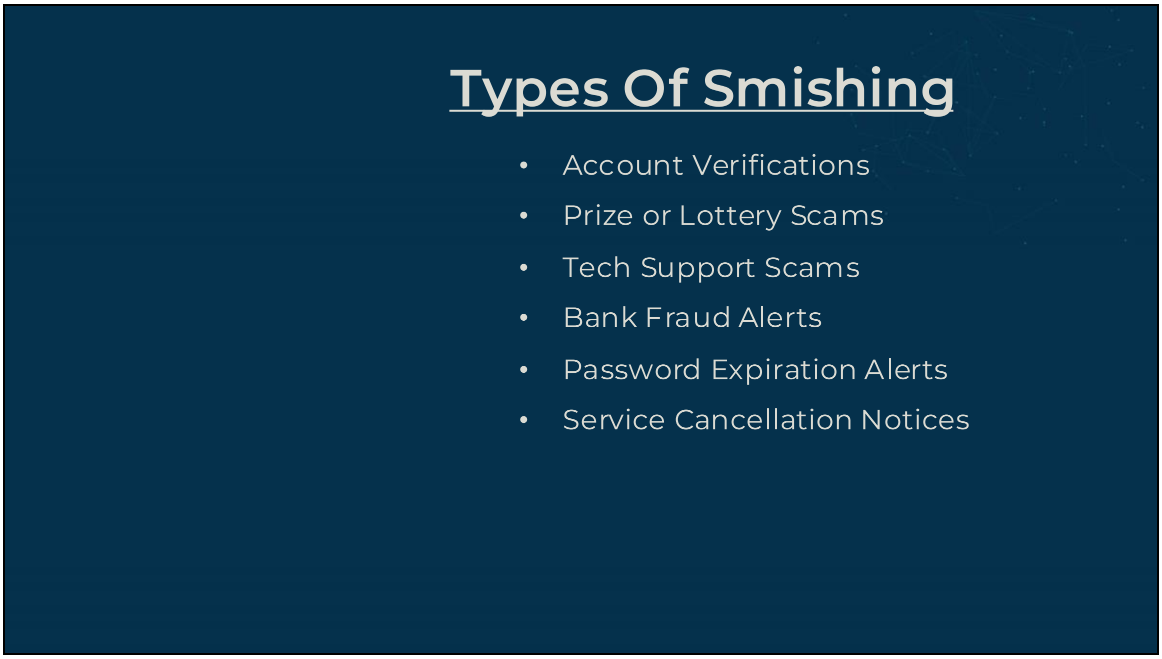
Personalized Threats

Smishing may include personal info like:

- Name
- Address
- Phone number

Attackers gather this data from public sources

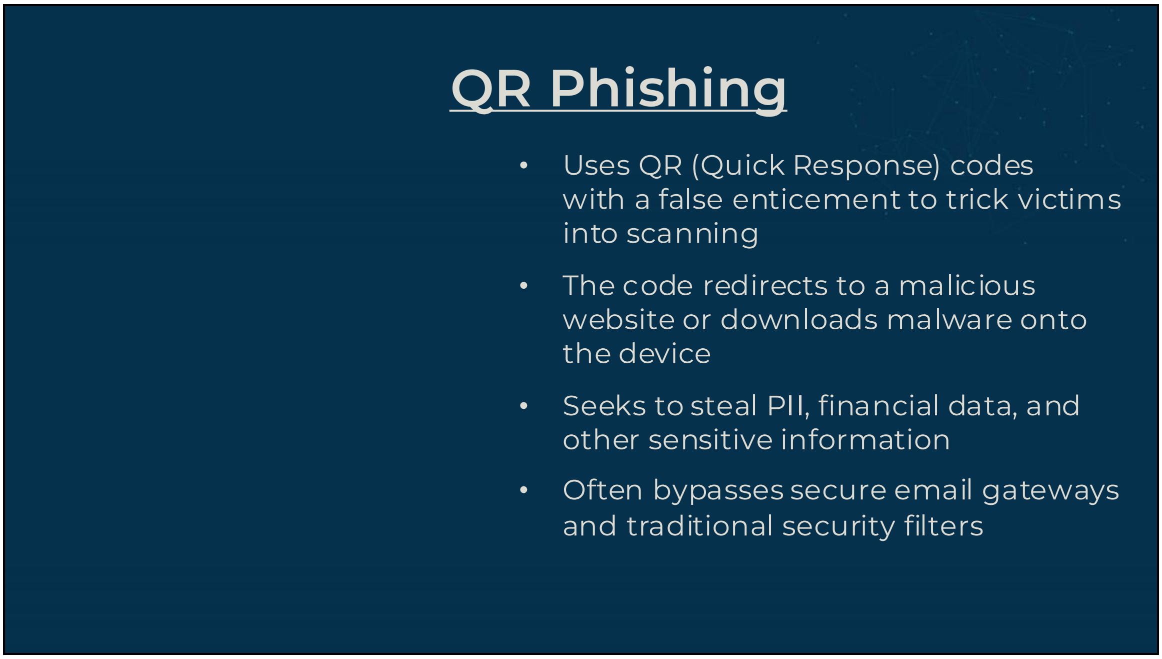
Despite varied content, all smishing is just text-based phishing



Types Of Smishing

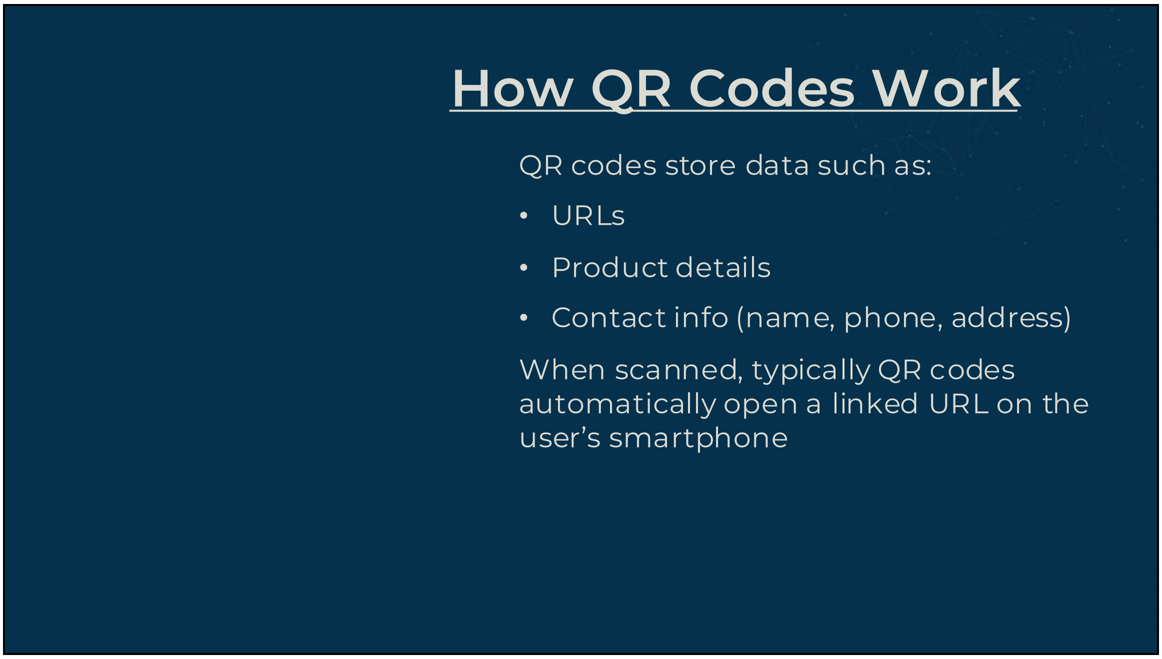
- Account Verifications
- Prize or Lottery Scams
- Tech Support Scams
- Bank Fraud Alerts
- Password Expiration Alerts
- Service Cancellation Notices

QR Code



QR Phishing

- Uses QR (Quick Response) codes with a false enticement to trick victims into scanning
- The code redirects to a malicious website or downloads malware onto the device
- Seeks to steal PII, financial data, and other sensitive information
- Often bypasses secure email gateways and traditional security filters



How QR Codes Work

QR codes store data such as:

- URLs
- Product details
- Contact info (name, phone, address)

When scanned, typically QR codes automatically open a linked URL on the user's smartphone

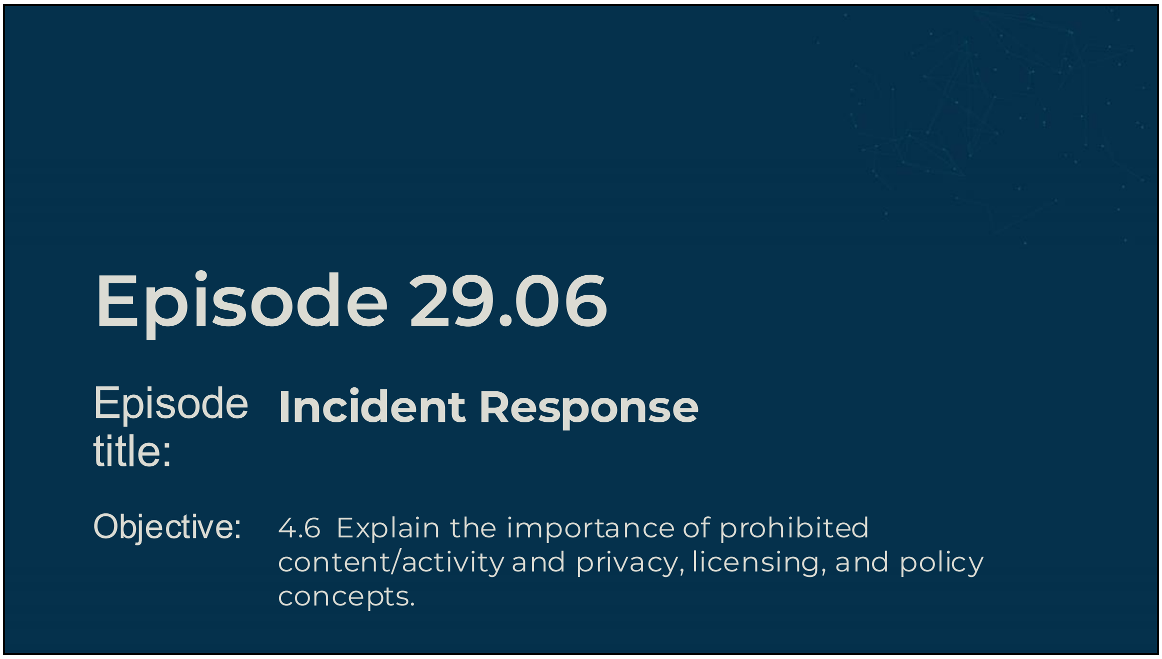
Episode 29.05

Episode title: **Licensing**

Objective: 4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

L3s

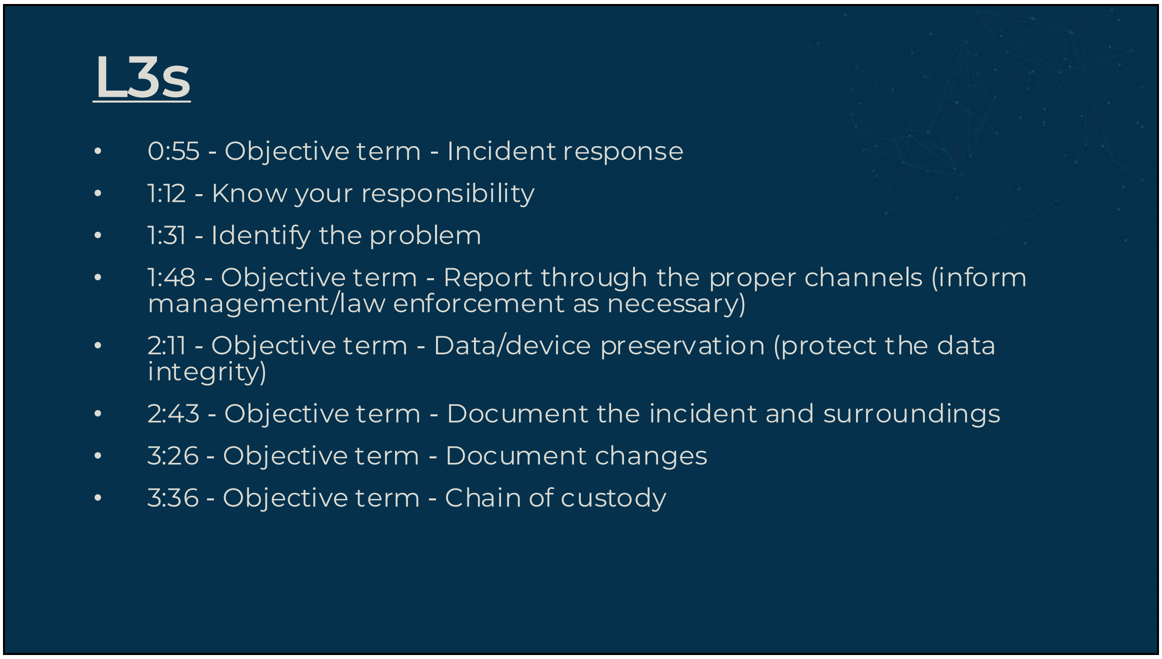
- 0:49 - “An Open Letter to Hobbyist” - Bill Gates, 1976
- 0:56 - Required licensing fee for the BASIC programming language
- 1:01 - Licensing
- 1:11 - Objective term - End-user license agreement (EULA)
- 1:55 - Objective term - Digital rights management (DRM)
- 2:55 - Objective term - Commercial/corporate license
- 3:11 - Objective term - Open-source
- 3:32 - GNU General Personal license (GNU GPL)
- 5:13 - Objective term - Personal license
- 5:31 - Enterprise license
- 6:26 - Per-processor license for Windows
- Non-disclosure agreement (NDA)
- Mutual NDA (MNDA)



Episode 29.06

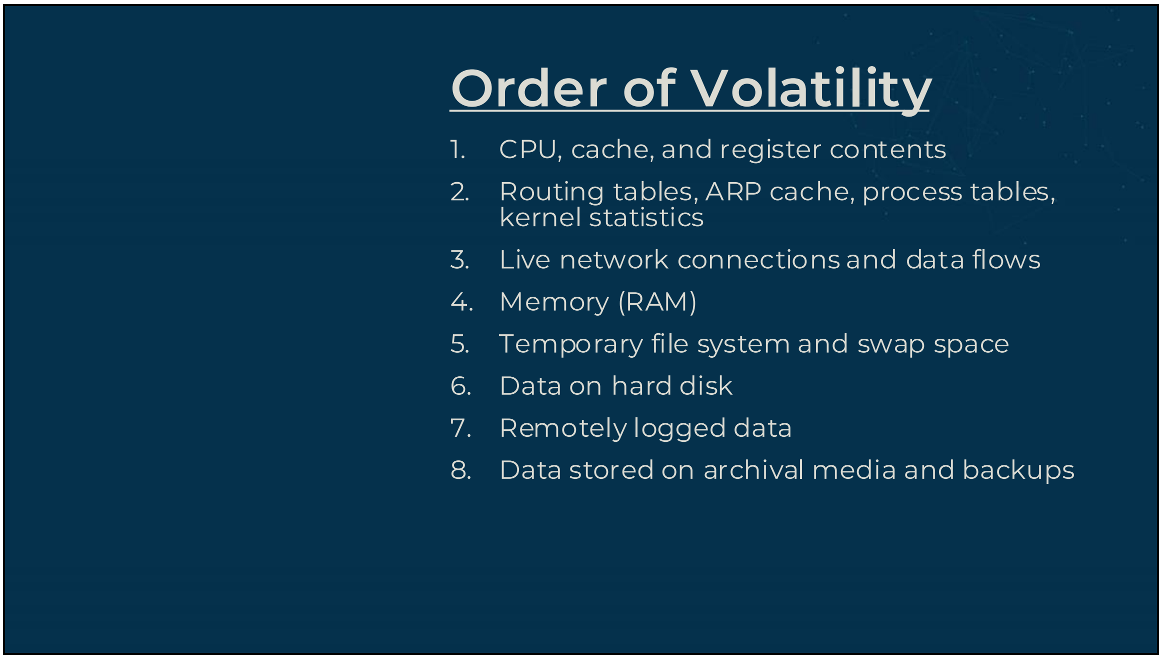
Episode title: **Incident Response**

Objective: 4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.



L3s

- 0:55 - Objective term - Incident response
- 1:12 - Know your responsibility
- 1:31 - Identify the problem
- 1:48 - Objective term - Report through the proper channels (inform management/law enforcement as necessary)
- 2:11 - Objective term - Data/device preservation (protect the data integrity)
- 2:43 - Objective term - Document the incident and surroundings
- 3:26 - Objective term - Document changes
- 3:36 - Objective term - Chain of custody



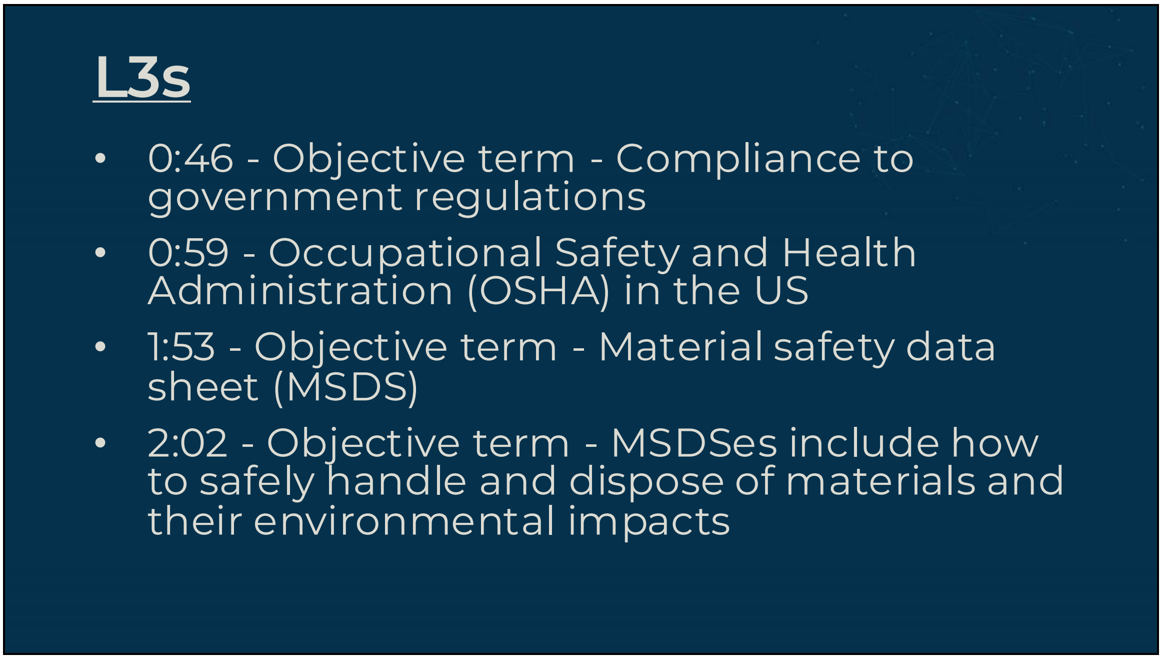
Order of Volatility

1. CPU, cache, and register contents
2. Routing tables, ARP cache, process tables, kernel statistics
3. Live network connections and data flows
4. Memory (RAM)
5. Temporary file system and swap space
6. Data on hard disk
7. Remotely logged data
8. Data stored on archival media and backups

Episode 29.07

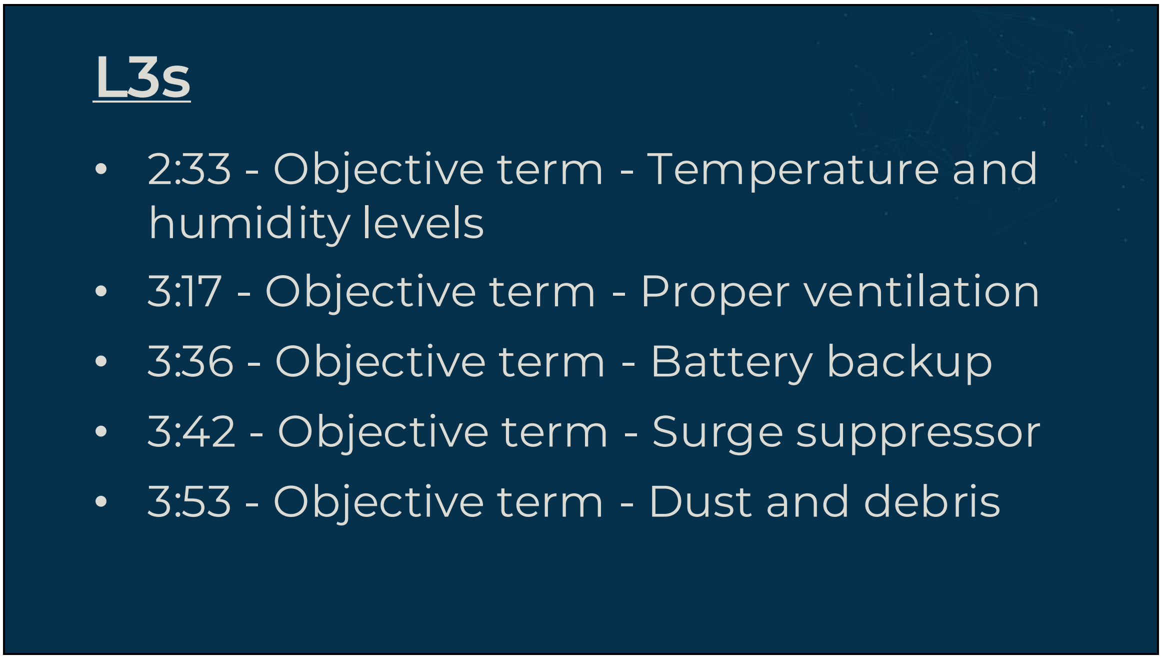
Episode title: **Environmental Controls**

Objective: 4.5 Summarize environmental impacts and local environmental controls



L3s

- 0:46 - Objective term - Compliance to government regulations
- 0:59 - Occupational Safety and Health Administration (OSHA) in the US
- 1:53 - Objective term - Material safety data sheet (MSDS)
- 2:02 - Objective term - MSDSes include how to safely handle and dispose of materials and their environmental impacts



L3s

- 2:33 - Objective term - Temperature and humidity levels
- 3:17 - Objective term - Proper ventilation
- 3:36 - Objective term - Battery backup
- 3:42 - Objective term - Surge suppressor
- 3:53 - Objective term - Dust and debris

L3s

- 4:21 - Enclosures
- 4:29 - Objective term - Air filters/mask
- 4:50 - Objective term - Compressed air
- 5:01 - Objective term - Vacuums
- 5:22 - Objective term - Anti-static vacuum
- Dust-free environmental enclosure
- Hot aisle/cold aisle
- Power surges
- Transient power fault
- Power sag or brownout
- Blackout