CIS Controls v8 Gap Analysis

Luigi's Case Study

Analysis of an enterprise compromise mapped to CIS Controls v8 and IG1/IG2 safeguards, with control-by-control remediation rationale.

CIS CONTROLS V8 | Safeguard Mapping | Gap Analysis | Segmentation | Malware Defense | Vulnerability Management | Incident Response

AT A GLANCE

Incident	An infected, unmanaged personal laptop joins corporate Wi-Fi, scans the network, reaches an anonymous FTP server and exfiltrates proprietary data over an encrypted VPN across a three-day weekend
Method	Reconstruct the attack chain in 12 steps, identify the CIS Controls that would have interrupted it, then specify IG1/IG2 safeguards for each
Coverage	10 CIS Controls · 27 safeguards across Implementation Groups 1 and 2
Outcome	Preventive and detective improvements spanning asset inventory, data protection, secure configuration, network defense, awareness and incident response

Sean Richard

sean@autom8ionlab.com · linkedin.com/in/a8l-sean-richard · +1.352.818.9694

Portfolio edition based on original Full Sail University coursework. Substantive project content is preserved; classroom-only submission headers were removed.

01 — CASE ANALYSIS

How the attack occurred

01	An employee connected a personally owned, unmanaged laptop to Luigi's corporate wireless network even though the device was not part of the approved corporate asset inventory.
02	The wireless network and DHCP service issued the personal laptop an internal IP address without first validating that the device was authorized, securely configured, patched, and protected by Luigi's standard security software.
03	The personal laptop was already infected with PSL malware and did not have Luigi's standard endpoint protection, allowing the malware to establish an outbound command-and-control connection immediately after joining the network.
04	The compromised laptop was able to scan the internal network for available services, showing that the user wireless segment was not adequately isolated from sensitive internal systems.
05	An internal FTP service was exposed and permitted anonymous access, allowing the attacker to reach the server without a valid Luigi's user account or an access approval process.
06	High-value data, including proprietary drawings, parts lists, price quotes, patents, purchasing information, and legal documents, was stored where an anonymously accessible FTP service could expose it.
07	The attacker was able to compress and remove the FTP data through an encrypted outbound VPN connection, showing that outbound traffic controls did not sufficiently restrict or investigate unusual encrypted connections.
08	Luigi's malicious-site or reputation list was four months out of date, so the command-and-control destination was not identified as malicious when the Network Operations Center reviewed the traffic.
09	The NOC detected a large volume of encrypted outbound traffic and identified the source and destination, but the event was handled as a routine help desk ticket instead of being immediately escalated, contained, and investigated as a security incident.
10	The employee noticed that the laptop was running unusually slowly on Friday but left it powered on through the three-day weekend instead of disconnecting it and promptly reporting the behavior to security or the help desk.
11	The delay between the first signs of abnormal activity and containment gave the threat actor an extended opportunity to scan the network, access the FTP server, and exfiltrate sensitive data.
12	Luigi's controls did not provide enough coordination between asset management, endpoint security, network monitoring, threat intelligence, user awareness, and incident response to stop the attack at an earlier stage.

02 — CONTROLS

CIS Controls v8 that could have prevented the attack

Luigi's is assumed to fall between IG1 and IG2. The controls below use IG1 safeguards and selected IG2 safeguards that directly address the facts of the case study.

01 Inventory and Control of Enterprise Assets

Luigi's must know which devices are authorized to connect to its environment and must quickly identify or quarantine unknown devices. If the personal laptop had been recognized as unauthorized before receiving normal network access, the infected endpoint would not have had the same opportunity to scan internal systems and reach the FTP server.

03 Data Protection

The stolen files contained proprietary and legal information that should have been identified as sensitive and protected according to its value. Proper classification, access permissions, and segmentation would have reduced the chance that an anonymous FTP session could reach high-value data and would have limited the amount of information exposed.

04 Secure Configuration of Enterprise Assets and Software

The attack depended on an insecure internal FTP configuration that permitted anonymous access. A documented secure configuration standard and removal or disabling of unnecessary services would reduce exposed attack surfaces and prevent legacy or unnecessary services from remaining available with unsafe settings.

07 Continuous Vulnerability Management

Recurring internal vulnerability scans could have identified the exposed FTP service, anonymous access, and other configuration weaknesses before the incident. A defined remediation process would then require Luigi's to correct the weakness instead of allowing a known or detectable security gap to remain available for exploitation.

09 Email and Web Browser Protections

Its safeguards include DNS and network-based URL filtering that can block connections to known malicious destinations. Luigi's relied on a malicious-site list that was four months out of date, so stronger and regularly updated filtering could have interrupted the malware's command-and-control communication.

10 Malware Defenses

The initial foothold was a laptop already infected with PSL malware. Anti-malware protection, current signatures, centralized management, and behavior-based detection would reduce the likelihood that an infected endpoint could remain active long enough to contact its command-and-control server, scan the network, and support data theft.

12 Network Infrastructure Management

Luigi's network allowed a personal wireless device to obtain normal internal connectivity and communicate with sensitive services. Secure network architecture, segmentation, and stronger authentication protocols can separate untrusted or personal devices from business systems and reduce the ability of a compromised endpoint to move laterally.

13 Network Monitoring and Defense

Luigi's already observed unusual network activity but did not stop it quickly. Centralized security alerts, network intrusion detection, and traffic filtering between segments can identify scanning and suspicious outbound behavior earlier and can limit the compromised device's ability to communicate with sensitive internal services.

14 Security Awareness and Skills Training

The employee noticed abnormal behavior but waited until after the long weekend to report it, while technical staff treated suspicious traffic as a routine ticket. Security awareness and role-specific training can help employees and support personnel recognize warning signs and escalate potential incidents immediately.

17 Incident Response Management

The NOC identified a large encrypted outbound transfer but the response did not immediately isolate the source system or initiate a coordinated investigation. A defined incident response process, clear ownership, reporting procedures, and practiced roles would support faster containment and reduce the time an attacker remains active in the environment.

Safeguards that should have been implemented

The safeguards below are limited to IG1 and IG2 because Luigi's falls between those two Implementation Groups.

CIS Control 01 Inventory and Control of Enterprise Assets

1.1 Establish and Maintain Detailed Enterprise Asset Inventory

IG1

An accurate inventory establishes which endpoints are approved to connect to Luigi's network and records ownership and authorization status. With that baseline, the personal laptop would stand out as an unmanaged device rather than being treated like a normal corporate asset after it received an internal IP address.

1.2 Address Unauthorized Assets

IG1

This safeguard requires a process to remove, deny, or quarantine unauthorized assets. Applying it to the personal laptop would have limited or eliminated its access to internal resources, preventing the infected system from freely scanning the network and reaching the anonymously accessible FTP server.

1.3 Utilize an Active Discovery Tool

IG2

Active discovery would help Luigi's identify newly connected devices on a frequent schedule instead of learning days later that the source system was not corporate-owned. Faster discovery of the personal laptop could trigger an authorization check, quarantine action, or security investigation before significant data loss occurred.

CIS Control 03 Data Protection

3.3 Configure Data Access Control Lists

IG1

Access control lists should restrict files, databases, and applications according to a user's need to know. Anonymous FTP access violated that principle because no verified user identity was required. Proper permissions would have prevented an unknown attacker from browsing and downloading proprietary program, patent, pricing, and legal files.

3.7 Establish and Maintain a Data Classification Scheme

IG2

A classification scheme would label the proprietary drawings, patents, legal records, pricing information, and other high-value files according to sensitivity. Once classified, Luigi's could apply stronger handling, storage, access, monitoring, and retention requirements instead of allowing sensitive information to reside behind an anonymously accessible file service.

3.12 Segment Data Processing and Storage Based on Sensitivity

IG2

Sensitive data should not be stored or processed on systems intended for lower-sensitivity information. Separating Luigi's high-value intellectual property and legal documents from general file-transfer services would have reduced the attacker's ability to reach critical information after compromising a normal user network segment.

CIS Control 04 Secure Configuration of Enterprise Assets and Software

4.1 Establish and Maintain a Secure Configuration Process

IG1

A documented secure configuration process would define approved settings for servers and software, including authentication requirements and prohibited insecure configurations. Regular review against that baseline could have identified the FTP server's anonymous access as an unacceptable configuration before the attacker used it to obtain sensitive files.

4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software

IG2

If the FTP service was not required for a current business purpose, it should have been disabled or removed. Eliminating unnecessary services reduces attack surface and would have removed the exact internal service the attacker discovered and exploited after scanning Luigi's network.

CIS Control 07 Continuous Vulnerability Management

7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets

IG2

Regular authenticated and unauthenticated internal vulnerability scans could have identified exposed services and insecure configurations such as anonymous FTP access. Discovering that weakness before the incident would give Luigi's security team an opportunity to correct it before an infected endpoint or attacker could exploit the service.

7.7 Remediate Detected Vulnerabilities

IG2

Scanning is only useful when discovered weaknesses are actually corrected. This safeguard requires remediation based on the organization's defined process, helping ensure that findings such as anonymous file access, unnecessary services, or weak configurations are assigned, prioritized, fixed, and verified instead of remaining available indefinitely.

CIS Control 09 Email and Web Browser Protections

9.2 Use DNS Filtering Services

IG1

DNS filtering can prevent enterprise assets from reaching known malicious domains. Because the infected laptop immediately contacted a command-and-control server, current DNS filtering could have blocked that connection and disrupted the attacker's ability to issue commands for internal scanning and data exfiltration.

9.3 Maintain and Enforce Network-Based URL Filters

IG2

This safeguard requires network-based URL filtering to be enforced and updated. Luigi's relied on a malicious-site list that was four months out of date, so a maintained reputation-based filtering process could have identified or blocked the command-and-control destination sooner and reduced reliance on stale threat information.

CIS Control 10 Malware Defenses

10.1 Deploy and Maintain Anti-Malware Software

IG1

The personal laptop was infected with PSL and lacked Luigi's standard protection software. Requiring effective anti-malware protection as a condition for connecting to the corporate network would help detect known malware and prevent an unprotected endpoint from receiving normal access to internal resources.

10.2 Configure Automatic Anti-Malware Signature Updates

IG1

Anti-malware protection loses effectiveness when its detection content is outdated. Automatic signature updates help ensure endpoints can recognize known threats such as established malware families. Luigi's should verify that devices allowed onto the corporate network have current protection before granting access.

10.7 Use Behavior-Based Anti-Malware Software

IG2

Behavior-based protection can identify suspicious activity even when a specific malware signature is unavailable or altered. The PSL infection performed command-and-control communication and network scanning, behaviors that advanced endpoint protection could flag and stop before the attacker reached the internal FTP server.

CIS Control 12 Network Infrastructure Management

12.2 Establish and Maintain a Secure Network Architecture

IG2

A secure architecture must address segmentation and least privilege. Luigi's should isolate personal or untrusted wireless devices from internal servers and sensitive data networks. Proper segmentation would have limited the infected laptop's ability to scan the corporate environment and directly reach the FTP service.

12.6 Use of Secure Network Management and Communication Protocols

IG2

Using secure network access technologies such as 802.1X and WPA2 Enterprise or stronger can require user or device authentication before internal access is granted. This would make it harder for an unmanaged personal laptop to connect to the corporate wireless network as though it were an approved asset.

CIS Control 13 Network Monitoring and Defense

13.1 Centralize Security Event Alerting

IG2

Centralized alerting would allow Luigi's to correlate events such as a newly connected device, internal scanning, unusual FTP activity, and a large encrypted outbound transfer. Correlation could raise the event's severity and prompt an immediate security response instead of a routine desktop support ticket.

13.3 Deploy a Network Intrusion Detection Solution

IG2

A network intrusion detection system can identify suspicious network patterns such as scanning, unusual service access, and command-and-control activity. Detecting those behaviors in real time would give the NOC better evidence that the traffic represented an active compromise requiring immediate containment rather than ordinary encrypted traffic.

13.4 Perform Traffic Filtering Between Network Segments

IG2

Traffic filtering between segments can restrict which user devices are allowed to communicate with sensitive servers and services. Even if the infected laptop obtained an IP address, filtering rules could have prevented the wireless user segment from reaching the FTP server or other high-value internal systems.

CIS Control 14 Security Awareness and Skills Training

14.1 Establish and Maintain a Security Awareness Program

IG1

A recurring awareness program should explain acceptable device use, warning signs of compromise, and required reporting behavior. The employee's decision to leave a malfunctioning personal laptop powered on for an entire long weekend shows why Luigi's workforce needs clear and repeated security expectations.

14.6 Train Workforce Members on Recognizing and Reporting Security Incidents

IG1

The employee noticed unusual system performance but delayed reporting until Tuesday. Training staff to recognize abnormal behavior as a potential security incident and report it immediately could have shortened the attacker's dwell time and allowed Luigi's to disconnect the device before the weekend data theft.

14.9 Conduct Role-Specific Security Awareness and Skills Training

IG2

NOC and help desk personnel need training tailored to their responsibilities. Staff responsible for monitoring should understand that large unexplained encrypted outbound transfers, internal scanning, and unmanaged endpoints may require urgent escalation, isolation, and incident response rather than routine troubleshooting workflows.

CIS Control 17 Incident Response Management

17.1 Designate Personnel to Manage Incident Handling

IG1

A clearly designated incident handler and backup provide ownership when suspicious activity is detected. If Luigi's NOC had an identified security lead responsible for coordinating containment, the encrypted outbound transfer could have been escalated immediately instead of waiting for local desktop services after the weekend.

17.3 Establish and Maintain an Enterprise Process for Reporting Incidents

IG1

A documented reporting process should define when, how, and to whom suspected incidents are reported. Both the employee and technical staff needed a clear path for rapid escalation so abnormal endpoint behavior and suspicious network traffic would reach security personnel without avoidable delays.

17.4 Establish and Maintain an Incident Response Process

IG2

An incident response process defines roles, responsibilities, compliance needs, and communication steps for handling security events. When the NOC observed a large encrypted transfer, this process should have triggered investigation and containment actions such as isolating the source device and preserving relevant evidence.

17.5 Assign Key Roles and Responsibilities

IG2

The case shows uncertainty between the NOC, help desk, desktop services, and forensics teams. Assigning incident-response responsibilities in advance would clarify who has authority to isolate a device, escalate a suspected breach, preserve evidence, notify leadership, and coordinate technical investigation during weekends or after hours.

Reference

Center for Internet Security. *CIS Critical Security Controls Navigator — v8.* https://www.cisecurity.org/controls/cis-controls-navigator/v8