

TOUR THE CIS CONTROL WINGS

*Every door hides a clue. Every floor holds a test.*

WELCOME TO

# CHÂTEAU DE SÉCURITÉ

*Can your security stack handle a stay at the Château?*





*Welcome to*

# CHÂTEAU DE SÉCURITÉ

Château de Sécurité is a lavish hotel, with each wing devoted to a key area of cybersecurity best practices and CIS Controls. Each room supports the hotel's mission of fortified protection. The wings operate in harmony, and the staff check the floors daily

for optimal operations. One misstep or threat could trigger disaster. Guests are encouraged to explore each wing and discover how their own security measures stack up. Your stay is confirmed. Take a stroll through each wing and reimagine security like never before.



## THE INVENTORY WING

### *Asset Management*

Knowing who and what comes in and out of the hotel: Everything that enters the hotel is identified and logged, from digital devices, guest bags and hotel assets. Nothing is anonymous in this wing.

#### ASSET STORAGE UNIT



This room represents **CIS Control 1: Inventory and Control of Enterprise Assets**. Think of the asset storage unit as a grand warehouse for the hotel and guest inventory. All devices and personal assets (smart locks, tablets, monitors, phones) are logged and monitored here. If an unauthorized device attempts to access the network, red flags fly, triggering an immediate isolated response.

**Example security protections:** A guest tries to plug in an unauthorized device to stream movies. The network immediately isolates it and alerts staff to investigate.



#### SOFTWARE RECORDS ROOM



This room represents **CIS Control 2: Inventory and Control of Software Assets**. Digital inventory is of top importance in the records room. There are digital and physical records of every software application the hotel runs, from the check-in kiosk to the restaurant POS system. Staff must check the approval list before installing new programs.

**Example security protections:** A staff member attempts to reinstall an outdated hotel ID verification application. The system flags the attempt, blocking the process until review.

## THE VAULTS WING

### *Data Protection*

Where the valuables are protected and hotel operations are restored. Here, digital secrets are guarded more fiercely than physical ones. This wing ensures resilience when things go wrong.



### THE PRIVATE SUITE



This room represents **CIS Control 3: Data Protection**. The private suite is where guests' data, encrypted servers and PII (names, credit card numbers, room key info, hotel blueprints and CCTV footage) are kept secure under lock and key. Only a handful of executives have authorized access. For an MSP, this is the epitome of customer trust and data security.

**Example security protections:** An imposter posing as a vendor tries to request a copy of CCTV footage. Without proper credentials, they're turned away and flagged for suspicious behavior.

### THE RESURGENCE ROOM



This room represents **CIS Control 11: Data Recovery**. While the hotel operates, the Resurgence Room is lined with backup storage and emergency response systems in case the hotel experiences a disaster. Backup tapes run silently in the background, and shelves are lined with emergency recovery tools. Downtime is a foreign concept for this wing.

**Example security protections:** A ransomware attack encrypts a reservation server. Within minutes, backups kick in and full service is restored without guest impact.





## THE KEY CONTROL WING

### *Access Management*

The Key Control Wing controls access and ensures no one goes where they shouldn't. All guest and staff members are identified with specified permissions, and anyone with unauthorized access is dealt with.

### ACCOUNT MANAGEMENT LOBBY



The lobby represents **CIS Control 5: Account Management**, brimming with elegance and debonair. It's home to the employee profile desk and guest check-in. Every account is created, deactivated or updated. Identity verification is multi-layered and strict.

**Example security protections:** A staff member leaves the hotel. Their keycard and digital credentials are instantly revoked to prevent ghost access.

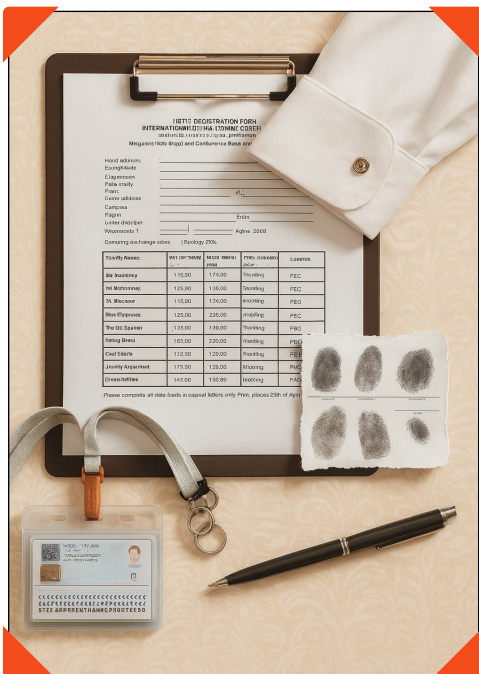


### ACCESS CONTROL OFFICE



This room represents **CIS Control 6: Access Control Management**. The Access Control Office manages all restricted entry points. The staff programs the keycards and monitors attempts to enter unauthorized zones, revoking access immediately when rules are broken.

**Example security protections:** A guest keycard attempts to open the hotel server room. The system flags it, locks all access points and dispatches the security team.



## THE WATCHTOWER WING

### *Threat Management*

Potential hotel dangers are monitored and managed. This is an active protection wing, always watching, waiting and prepared to eliminate threats.



### THE PHISH BOWL CAFÉ



This café represents **CIS Control 9: Email and Web Browser Protections**. The Phish Bowl is a quirky café serving up real-time education on social engineering. Guests learn phishing tactics over espresso, while the waiters monitor emails for malware-filled links. If an email smells phishy, it gets tossed in the bin.

**Example security protections:** A fake survey offers guests a free spa day. The link gets flagged as phishing by the café's security filter before anyone can click.

### MALWARE MOP UP CLOSET



Representing **CIS Control 10: Malware Defenses**, this sterilized janitorial closet quarantines infected devices in isolation chambers. A dedicated team monitors for new strains and develops digital "disinfectants," ensuring malware doesn't spread through the hotel.

**Example security protections:** A guest plugs a USB device into a shared workspace. The system detects malware and locks the device. The response team isolates the device, removes the infected malware and updates the hotel's security firewalls.







## THE DIGITAL LOOKOUT LOUNGE



This lounge represents **CIS Control 13: Network Monitoring and Defense**. The Digital Lookout Lounge is where guests and staff go to spot and track suspicious threat activity in real-time.

**Example security protections:** A rogue access point is discovered hidden in a potted plant on the rooftop terrace, or a guest tries to download 500 GB of suspicious software on the network.



## THE RAPID RESPONSE ROOM



This crisis room represents **CIS Control 17: Incident Response Management**. The rapid response team gathers here during emergencies and hosts threat response drills for incident preparation. Think of this room as the "911 dispatch center" for cyber crises.

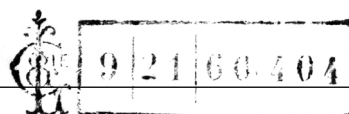
**Example security protections:** An attacker compromises a guest-facing system. The incident response team initiates lockdown and responds within minutes.



## THE PENTESTER PENTHOUSE



A penthouse ruled by **CIS Control 18: Penetration Testing**. A luxury suite for professional hotel-appointed hackers to test the cracks in the hotel's systems (security strength, camera blind spots and software flaws) and fix them before real criminals exploit them. They are always thinking like an attacker.



## THE MAINTENANCE WING

### *Security Operations*

The behind-the-scenes team, where security configuration, patching, logging and vendor reviews never sleep. This wing keeps the whole hotel secure and running smoothly.



#### THE SOFT-WEAR SPA



This spa represents **CIS Control 16: Application Software Security**. In this relaxing development spa, apps are massaged into shape before going live. Custom booking platforms and mobile apps are tested for bugs, hardened against attacks and exfoliated to perfection. Only the most secure codes go live.

**Example security protections:** A reservation system update includes deprecated JavaScript libraries. It's sent back for rework before deployment.

№77 3

#### THE PATCH AND POLISH PARLOR



Representing **CIS Control 7: Continuous Vulnerability Management**. In this polished parlor room, hotel systems are inspected for weak spots, scanned and patched. Security holes are filled, updates applied and newly discovered vulnerabilities are addressed quickly to stay ahead of threats.

**Example security protections:** A vulnerability surfaces in the spa's appointment app. Within hours, a patch is applied and documented.







## SERVICE PROVIDER PANTRY



This pantry represents **CIS Control 15: Service Provider Management**. Before third-party chefs, electricians or IT contractors touch a hotel system, they check in here. Background checks, contract reviews and access approvals are part of the “ingredient list” to ensure only trusted vendors contribute to the hotel’s 5-star services.

**Example security protections:** A new email vendor is missing documentation. The pantry denies access until compliance is verified.



## THE CONFIGURATION CORRIDOR



This corridor represents **CIS Control 4: Secure Configuration of Enterprise Assets and Software**. The maintenance corridor is where systems and equipment are assessed, configured and updated to minimize security vulnerabilities before being put into use (servers, network devices, apps, operating systems, etc.).

**Example security protections:** A new point-of-sale system is flagged during onboarding due to default admin credentials. The system is reconfigured before it goes live.



## SECURITY TRAINING GYM



This gym represents **CIS Control 14: Security Awareness and Skills Training**. The training gym is where employees and guests take part in daily drills in phishing recognition, password strengthening and scam avoidance to ensure everyone is security fit.

**Example security protections:** All front desk staff receive a simulated phishing call. Those who fall for it are automatically enrolled in a refresher course.





## ENDPOINT TRACKING EATERY



This restaurant represents **CIS Control 12: Network Infrastructure Management**.

A trendy hotel restaurant where every endpoint (guest device, staff phone, register, sensor) connects to the hotel's central nervous system. With everything monitored and mapped, no rogue router or sketchy switch can go unnoticed.

**Example security protections:** A catering tablet suddenly disconnects and attempts a reconnection from an odd IP. Staff track it down and isolate it from the network.

## THE AUDITORIUM



Representing **CIS Control 8: Audit Log Management**, the Auditorium is filled with security camera footage, email records, door logs, system logins and alarm history. Everything is recorded here in the event of an incident or investigation.

**Example security protections:** At 2:47 am, the Auditorium recorded the file after a suspected insider threat breached the network.











## STAY SECURE AND SERVE WITH CONFIDENCE

The real work begins back at your MSP. With every CIS Control in place, you hold the keys to stopping threats, protecting your clients and keeping operations seamless.

			N°	13467	
<p><i>Make yourself at home in the Château de Sécurité and get to know the CIS Controls, but be aware, there's more to this hotel than meets the eye. Keep a lookout for the next release of this guide coming to your email, where you'll get to meet your fellow guests.</i></p> <p><i>Then, the real game will begin.</i></p> <p><b>CONFIDENTIAL</b></p>					

→ SCHEDULE YOUR CIS CONSULTATION

→ BECOME A PAX8 PARTNER

