WYZE Camera Security Mastery Course

"Unfuckwithable Digital Security Camera System"

Target: 10/10 mastery across all critical security functions **Scope:** Multi-location enterprise-grade security using consumer hardware **Philosophy:** Defense in depth, redundancy, and proactive monitoring

---

COURSE STRUCTURE

Module 1: Foundation Assessment & Network Security (25 points)

Module 2: Device Configuration & Access Control (25 points)

Module 3: Recording & Data Protection (20 points)

Module 4: Monitoring & Alert Systems (15 points)

Module 5: Multi-Location Management (15 points)

Total: 100 points = 10/10 mastery

MODULE 1: FOUNDATION ASSESSMENT & NETWORK SECURITY (25 POINTS)

1.1 Current State Audit (5 points)

TASK: Complete comprehensive inventory

Checklist:

- [ ] List all WYZE devices (cameras, doorbells, sensors) by location
- [ ] Document current firmware versions for each device
- [ ] Map network topology (main router, access points, VLANs)
- [ ] Identify internet upload speeds at each location
- [ ] Document current storage solutions (cloud, local, hybrid)

SCORING:

- 5/5: Complete inventory with documentation
- 3/5: Most devices catalogued, some gaps
- 1/5: Basic list exists
- 0/5: No systematic inventory

1.2 Network Segmentation (10 points)

TASK: Implement IoT network isolation

Requirements:

☐ Dedicated IoT VLAN or guest network for all cameras
☐ Firewall rules blocking IoT-to-main network communication
☐ IoT devices cannot access internet except for necessary services
☐ Regular network scanning to detect unauthorized devices

Implementation Steps:

1. Access router admin panel

2. Create dedicated 2.4GHz network (IoT_Secure_[LocationName])

3. Configure bandwidth limits (reserve upload for camera streams)

4. Set up access control lists (ACLs)

5. Move all WYZE devices to isolated network

SCORING:

- 10/10: Full network segmentation with monitoring

- 7/10: IoT network separated, basic rules in place

- 4/10: Guest network used, minimal configuration

- 0/10: All devices on main network

1.3 Router Security Hardening (10 points)

TASK: Secure network infrastructure

Requirements:

☐ Change default admin credentials
☐ Disable WPS and unnecessary services
☐ Enable WPA3 (or WPA2 if WPA3 unavailable)
☐ Configure automatic security updates
☐ Set up VPN access for remote management
☐ Enable logging and monitoring

SCORING:

- 10/10: All security measures implemented with documentation

- 7/10: Most measures in place, minor gaps

- 4/10: Basic security changes made

- 0/10: Default configuration unchanged

MODULE 2: DEVICE CONFIGURATION & ACCESS CONTROL (25 POINTS)

2.1 Account Security (8 points)

TASK: Secure WYZE account and access

Requirements:

☐ Unique, complex password (min 16 characters)
☐ Two-factor authentication enabled
☐ Regular password rotation schedule
☐ Shared account access documented and limited
☐ Account recovery methods secured

Implementation:

1. Generate strong password using password manager

2. Enable 2FA via authenticator app (not SMS)

3. Document authorized users and access levels

4. Set calendar reminder for quarterly password rotation

SCORING:

- 8/8: All security measures plus documentation

- 6/8: Strong password + 2FA enabled

- 3/8: Password improved but 2FA missing

- 0/8: Weak security or default settings

2.2 Device Firmware & Updates (7 points)

TASK: Maintain current security patches

Requirements:

☐ All devices on latest firmware
☐ Automatic updates enabled where possible
☐ Update notification system configured
☐ Testing procedure for major updates
☐ Rollback plan documented

Automation Setup:

1. Enable auto-updates in WYZE app

2. Set up monitoring for available updates

3. Create testing schedule for major firmware releases

4. Document known good configurations

SCORING:

- 7/7: Automated update system with testing protocol

- 5/7: Regular manual updates performed

- 3/7: Some devices updated, inconsistent process

- 0/7: Outdated firmware, no update process

2.3 Camera Configuration Security (10 points)

TASK: Optimize individual camera settings

Per-Camera Checklist:

☐ Unique device names (no default "WYZE_CAM_XXX")
☐ Appropriate privacy zones configured
☐ Motion detection zones optimized
☐ Recording quality set appropriately for bandwidth
☐ Night vision settings optimized
☐ Audio recording configured per legal requirements
☐ Time zone and timestamps accurate

Advanced Settings:

☐ RTSP firmware for critical cameras (enables 3rd party recording)
☐ Local storage backup configured
☐ Bandwidth optimization for multi-camera setups

SCORING:

- 10/10: All cameras optimally configured with documentation

- 7/10: Most cameras properly configured

- 4/10: Basic configuration completed

- 0/10: Default settings unchanged

MODULE 3: RECORDING & DATA PROTECTION (20 POINTS)

3.1 Storage Strategy (8 points)

TASK: Implement redundant recording system

Requirements:

☐ Primary: Local NVR or NAS system
☐ Secondary: WYZE cloud backup for critical cameras
☐ Tertiary: Offsite backup for high-value locations
☐ Retention policy documented and automated

Implementation Options:

Option A: Professional NVR

- Dedicated NVR with RAID storage
- 30+ day retention for all cameras
- Automated backup to cloud storage

Option B: DIY NAS Solution

- Synology/QNAP NAS with Surveillance Station
- RTSP streams from WYZE cameras
- Automated offsite replication

Option C: Hybrid Cloud

- WYZE cloud for motion events
- Local storage for continuous recording
- Third-party cloud for long-term archive

SCORING:

- 8/8: Triple redundancy with documented procedures
- 6/8: Local + cloud backup implemented
- 3/8: Single backup method in place
- 0/8: No systematic backup strategy

3.2 Data Encryption & Access (7 points)

TASK: Secure recorded data

Requirements:

- [ ] Local storage encrypted
- [ ] Cloud storage with end-to-end encryption
- [ ] Access logs maintained
- [ ] Data sharing policies documented
- [ ] Legal compliance verified (retention periods, privacy laws)

SCORING:

- 7/7: Full encryption with compliance documentation
- 5/7: Encryption enabled, basic access control
- 2/7: Some security measures in place
- 0/7: No encryption or access control

3.3 Backup Verification (5 points)

TASK: Ensure backup reliability

Requirements:

- [ ] Monthly backup integrity tests
- [ ] Recovery time objectives documented
- [ ] Restoration procedures tested quarterly
- [ ] Backup monitoring and alerting

SCORING:

- 5/5: Automated testing with documented procedures
- 3/5: Regular manual verification
- 1/5: Occasional backup checks
- 0/5: No verification process

MODULE 4: MONITORING & ALERT SYSTEMS (15 POINTS)

4.1 Motion Detection & AI (8 points)

TASK: Optimize detection and reduce false positives

Requirements:

- [ ] Person detection enabled on all appropriate cameras
- [ ] Detection zones configured to avoid high-traffic areas
- [ ] Sensitivity adjusted per camera location
- [ ] AI features (person/vehicle/pet detection) properly configured

☐ Integration with other security systems

Advanced Configuration:

☐ Time-based detection rules (different sensitivity day/night)
☐ Weather-based adjustments
☐ Integration with alarm systems

SCORING:

- 8/8: Advanced AI detection with minimal false positives

- 6/8: Good detection setup with occasional false alerts

- 3/8: Basic motion detection configured

- 0/8: Default detection settings

4.2 Alert Management (7 points)

TASK: Create actionable notification system

Requirements:

☐ Tiered alert system (critical vs. informational)
☐ Multiple notification channels (app, email, SMS)
☐ Alert escalation procedures
☐ Response protocols documented
☐ Alert fatigue mitigation strategies

Alert Categories:

- **Critical:** Person detected in restricted areas after hours

- **High:** Motion during defined "quiet" periods

- **Medium:** General motion detection

- **Low:** System status updates

SCORING:

- 7/7: Sophisticated alert system with documented responses

- 5/7: Multi-channel alerts with basic categorization

- 2/7: Basic app notifications enabled

- 0/7: No customized alert system

MODULE 5: MULTI-LOCATION MANAGEMENT (15 POINTS)

5.1 Centralized Monitoring (8 points)

TASK: Unified view across all locations

Requirements:

☐ Dashboard showing all locations
☐ Standardized naming conventions
☐ Unified alert management
☐ Centralized storage and backup
☐ Performance monitoring across sites

Tools:

- WYZE app with multiple locations

- Third-party NVR software for unified view

- Custom dashboard using API access

SCORING:

- 8/8: Professional centralized monitoring system

- 6/8: Good visibility across locations

- 3/8: Basic multi-location setup

- 0/8: Individual location management only

5.2 Scaling & Standardization (7 points)

TASK: Repeatable deployment process

Requirements:

☐ Standardized equipment lists per location type
☐ Deployment checklists and procedures
☐ Configuration templates
☐ Training materials for local staff
☐ Maintenance schedules synchronized

SCORING:

- 7/7: Complete standardization with documentation

- 5/7: Good standardization across most elements

- 2/7: Some standards established

- 0/7: Ad-hoc deployment per location

ASSESSMENT MATRIX

Self-Assessment Tool

Rate each item 1-10, then calculate module scores:

Module 1: Foundation (25 points)

- Current State Audit: ___/5
- Network Segmentation: ___/10
- Router Security: ___/10
- **Module 1 Total: ___/25**

Module 2: Configuration (25 points)

- Account Security: ___/8
- Firmware Updates: ___/7
- Camera Configuration: ___/10
- **Module 2 Total: ___/25**

Module 3: Data Protection (20 points)

- Storage Strategy: ___/8
- Data Encryption: ___/7
- Backup Verification: ___/5
- **Module 3 Total: ___/20**

Module 4: Monitoring (15 points)

- Motion Detection: ___/8
- Alert Management: ___/7
- **Module 4 Total: ___/15**

Module 5: Multi-Location (15 points)

- Centralized Monitoring: ___/8
- Scaling: ___/7
- **Module 5 Total: ___/15**

OVERALL SCORE: ___/100

Mastery Levels

- **90-100:** Security Master - "Unfuckwithable" status achieved
- **80-89:** Advanced - Strong security, minor improvements needed
- **70-79:** Intermediate - Good foundation, key areas need work
- **60-69:** Beginner - Basic setup, significant improvements required
- **Below 60:** Critical - Major security vulnerabilities present

IMPLEMENTATION ROADMAP

Week 1: Foundation

- Complete current state audit
- Implement network segmentation
- Secure router configuration

Week 2: Device Security

- Upgrade account security
- Update all firmware
- Configure cameras optimally

Week 3: Data Protection

- Implement backup strategy
- Enable encryption
- Test recovery procedures

Week 4: Monitoring & Multi-Location

- Optimize detection systems
- Set up centralized monitoring
- Document all procedures

Ongoing: Maintenance

- Monthly security reviews
- Quarterly penetration testing
- Annual complete reassessment

QUICK START CHECKLIST

Priority 1 (Do Today):

☐ Change WYZE account password

☐ Enable 2-factor authentication

☐ Update all device firmware

☐ Create IoT network

Priority 2 (This Week):

☐ Configure camera detection zones

☐ Set up local backup system

☐ Document current setup

☐ Test alert notifications

Priority 3 (This Month):

☐ Implement comprehensive backup

☐ Set up monitoring dashboard

☐ Create response procedures

☐ Train authorized users

Ready to achieve 10/10 mastery? Let's start with your current state audit.