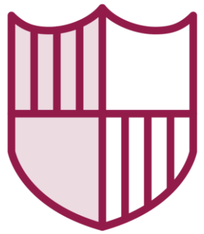
Distinguishing Wireless Countermeasures

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

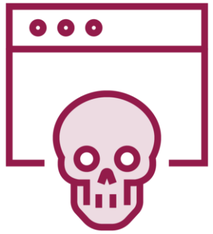
Wireless Security Layers



Wireless signal security

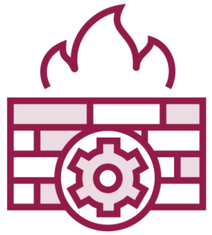
Data protection

Connection security

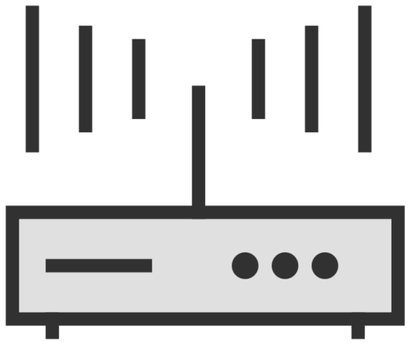


Network protection

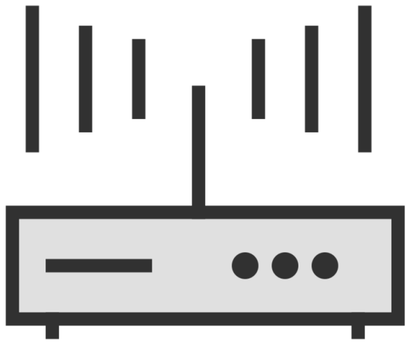
Device security



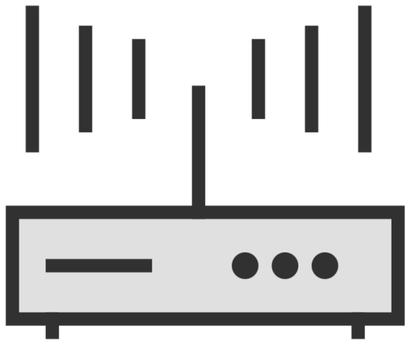
End-user protection

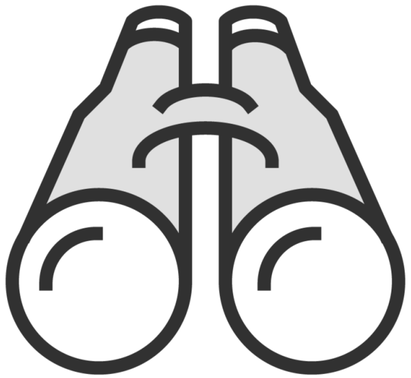


Wireless Intrusion Detection Systems (WIDS)

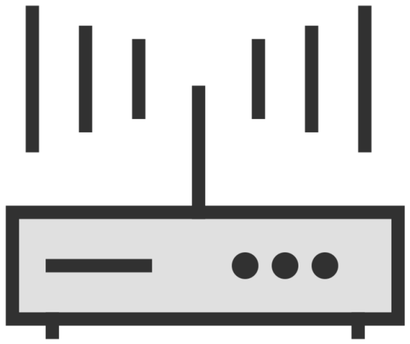


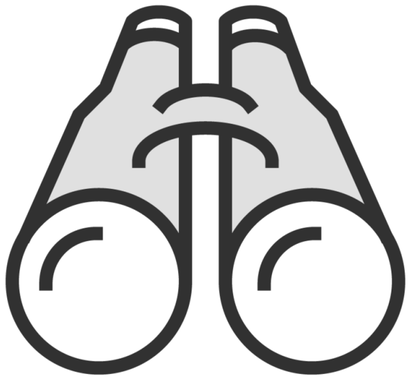
Wireless Intrusion Prevention Systems (WIPS)



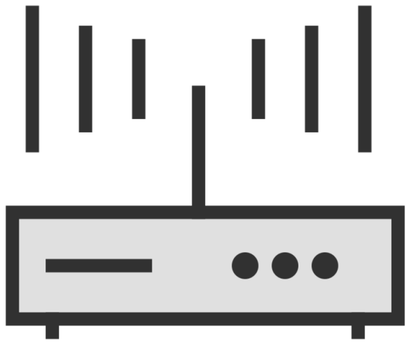


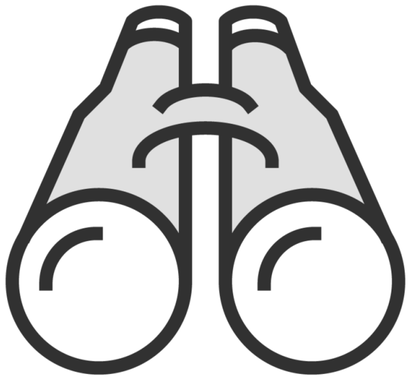
Continually monitoring will be needed

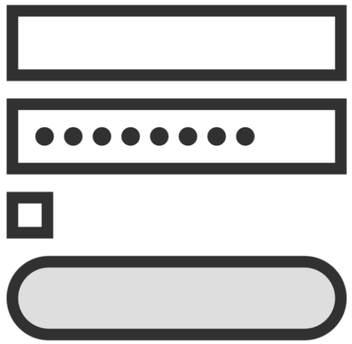




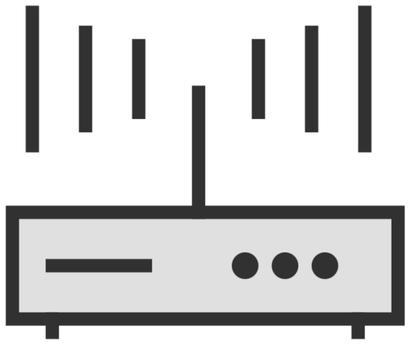

Secure access points to protect data in motion

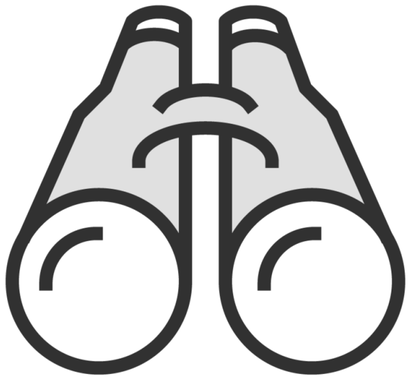


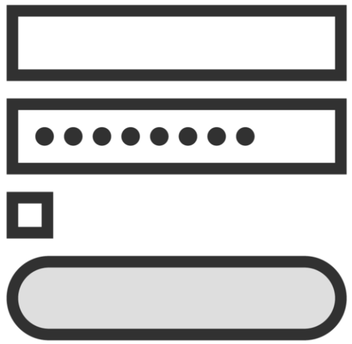




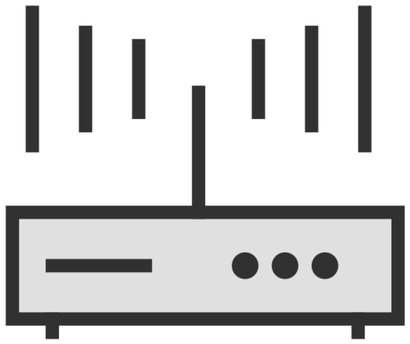
Connection security prevents MiTM and sniffing attempts

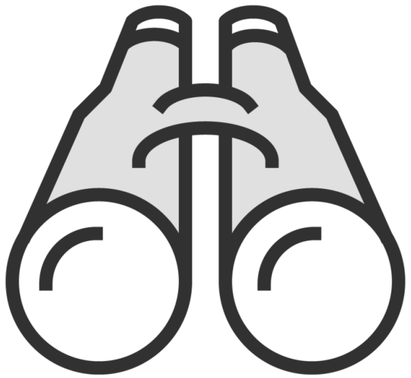


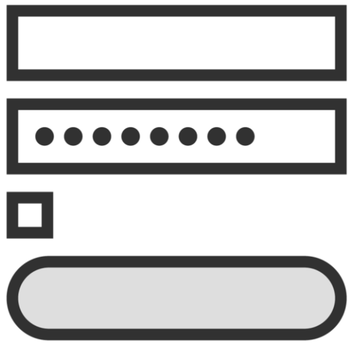


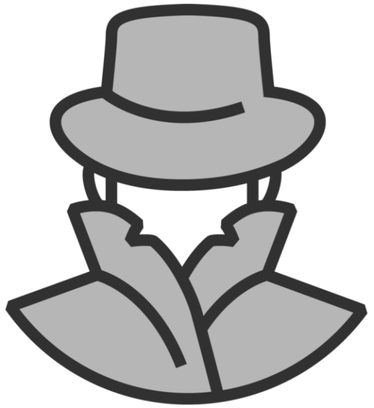



Continual device security is a must

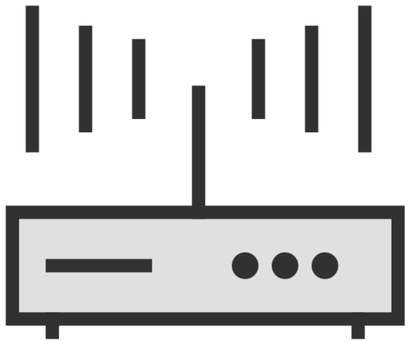


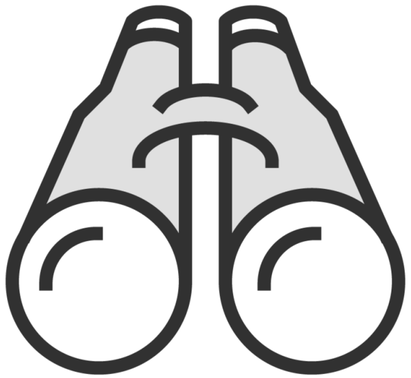


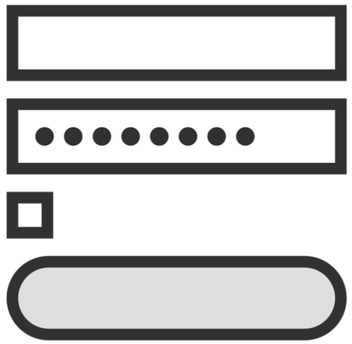


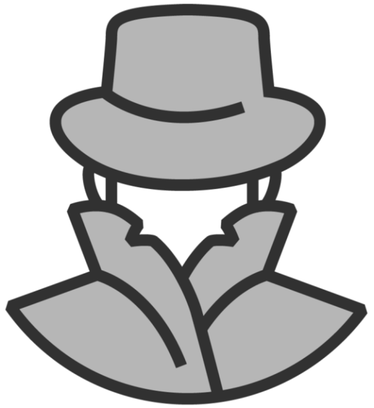
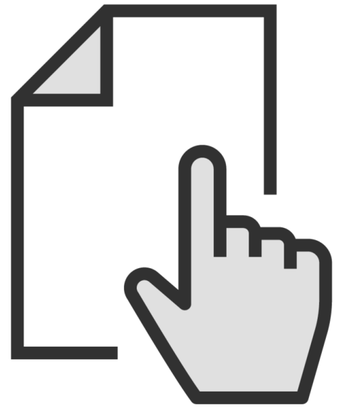


Strong authentication minimizes unauthorized users







End-user training on wireless security

Defending WPAs

Passphrases

The only way to break WPA is by sniffing the PMK password that corresponds with the handshake authentication process.

Use words not found in the dictionary

Use a minimum of 20 characters and change it often

Use a password manager service to secure passwords

WWW.b@tmanRul3sTheNite.c0m

Client Settings

Use WPA/2 or WPA/3 with AES/CCMP encryption

Specify server addresses

Regenerate keys for every new connection

Other Security Settings

Update firmware on all wireless devices

Use a VPN

Deploy communication protocols

Other Security Settings

Update firmware on all wireless devices

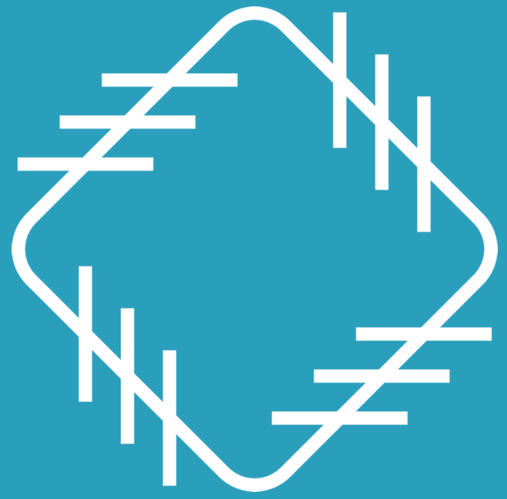
Use a VPN

Deploy communication protocols

Utilize NAP or NAC for connectivity

Stopping KRACK and aLTEr Attacks

KRACK Attack Countermeasures



Update

Avoid

Ensure

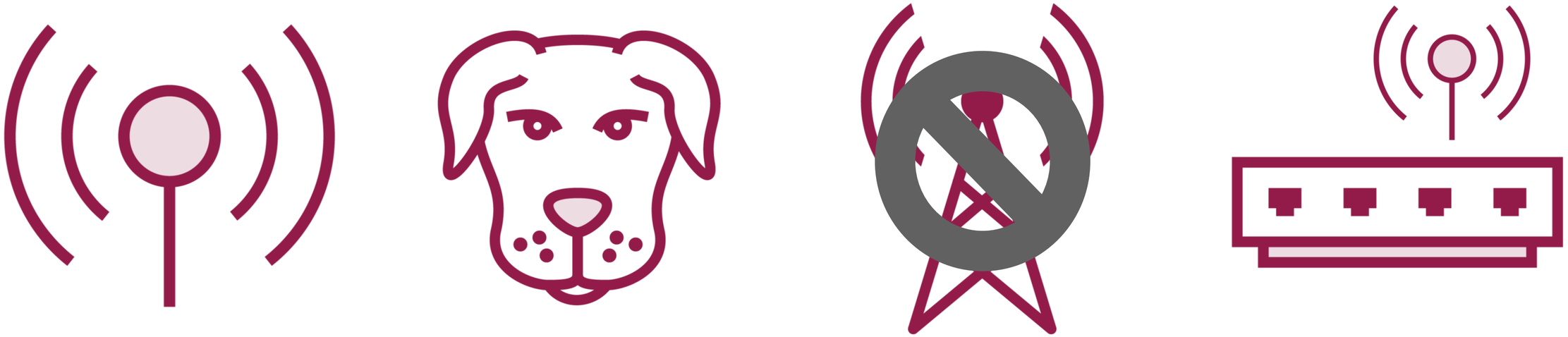
Utilize

aLTEr Attacks

- Encrypt DNS and use trusted servers
- Use DNS over TLS or DTLS to encrypt traffic
- Add the DNSCrypt protocol

Countermeasures for Rogue APs

Countermeasures



Wired side inputs

Overall Best Practices

Overall Best Practices

Disable SSID broadcasting

Disable remote router login

Enable MAC address filtering

Use SSID cloaking

Avoid using easy SSID names

Overall Best Practices

Use a firewall or packet filter

Limit the signal strength

Conduct routine configuration checks

Disable when not in use

Use a centralized server for authentication

Bluetooth Attack Countermeasures

Countermeasures

- Turn off when not in use
- Use a strong password or passcode
- Only pair trusted devices
- Turn off show notifications when paired
- Utilize ‘bluetooth’ visibility settings
- Set a timer
- Use a firewall program
- Upgrade the software

Learning Check

Learning Check

- Wireless Intrusion Protection System (WIPS)
- Minimum of 20 characters
- IPSec SSL/TLS
- WPA with AES/CCMP
- Centralized authentication server

Up Next:

Ethical Hacking Series