Smart Home Cyber Threat Analysis Sample

1. Overview

This sample presents a brief cyber threat analysis for a typical smart home environment comprising interconnected devices such as smart speakers, cameras, thermostats, and lighting systems.

2. Assets Identified

- Home Wi-Fi Router
- Smart Speaker (Voice Assistant)
- IP Security Camera
- Smart Thermostat
- Smart Lighting System
- User Mobile Devices

3. Threat Landscape

Asset	Potential Threat	Impact
Wi-Fi Router	Unauthorized access, weak password exploitation	Network compromise, device control
Smart Speaker	Voice command spoofing, eavesdropping	Privacy invasion, unauthorized actions
IP Security Camera	Live feed hijacking, data leakage	Surveillance, loss of privacy
Smart Thermostat	Remote manipulation	Comfort disruption, energy waste
Lighting System	Denial of service, remote control	Discomfort, potential safety issue

4. Risk Assessment

Threat	Likelihood	Severity	Risk Level
Unauthorized Wi-Fi Access	Medium	High	High
Eavesdropping via Smart Speaker	Low	High	Medium
Camera Hijack	Low	Critical	High

5. Recommendations

- Change default device credentials and apply strong passwords.
- Regularly update firmware and security patches for all devices.
- Utilize network segmentation (guest network for IoT devices).
- Enable device-specific security features, such as two-factor authentication.
- Monitor network traffic for unusual behavior.

6. Conclusion

Smart home devices offer convenience but increase exposure to cyber threats. Periodic security reviews and user awareness are essential to mitigate risks in the smart home environment.