IoT SECURITY:

25 QUESTIONS TO ANSWER ABOUT YOUR CONNECTED PRODUCT SECURITY

Seeing and securing every connected device, from end-to-end, over the entire lifecycle is a challenge for modern organizations. As attacks often cross IT and IoT/OT boundaries, now more than ever you need an up-to-date inventory and visibility of risks for every device connected to your network.

To help you improve your IoT security posture, we've outlined 25 questions you need to be able to answer:

1. Are your devices in secure mode?

2. Did you change all default passwords on new devices?

3. If any device functionality was unnecessary, did you turn it off?

4. Do the devices encrypt communications?

5. Is data encrypted at rest?

6. Have you recently and regularly scanned all of your devices for malware?

7. Can your devices be accessed remotely?

8. Are your identity and access management certificates current?

9. Are all devices up-to-date with the latest versions of firmware, operating systems, application software, libraries, etc.?

10. Do you perform regular assessments to identify vulnerabilities and establish a process for remediation?

11. When a new vulnerability is uncovered, can you easily identify impacted devices?

12. Do you perform monitoring across all systems on your network?

13. Do you have an incident response policy and corresponding procedures?

14. Do you perform annual tests on your incident response policy and corresponding procedures?

15. Are commands that can be sent to the device managed?

16. Are end-users interacting with devices in a secure manner?

17. Do you have a process for automatically revoking former employees' access?

18. Do any of your devices directly connect to the internet?

19. Do you document and signify all devices that are directly connected to the internet?

20. Can you identify when devices or users exhibit suspicious behavior that could compromise the overall solution?

21. Do you have real-time alerting of anomalous activity?

22. Have your recent IoT security efforts reduced the attack surface?

23. Can you easily report across product lines down to the device level from design through deployment?

24. Can you easily generate compliance reporting?

25. Do you maintain a live inventory populated through an automated discovery process of all internet-enabled devices on your network?

If you struggled to answer any of the questions, you are not alone. Identifying, classifying, and locating all network-connected devices and systems is a hardship that industries like healthcare and manufacturing face on a daily basis.

CADRE CAN HELP
At Cadre Information Security, we work with a variety of partners that help organizations like yours discover high-fidelity information about every connected devices within hours of deployment. Whether your concerns are about compliance or general data protection, we can help you choose the best solution that works from discovery and profiling of devices and risks, to automated response.

Get started improving your IoT security.
Contact us at info@cadre.net today!