

Plot the path to a counter-drone defense

Building out requirements for a counter-drone physical security program

Next steps

Our [recent white paper](#) addresses the proliferation of unmanned aerial vehicles (UAVs)—better known as drones—and the unique challenges they present for physical security. In our last few articles, we've provided guidance on assessing your risk, designing your program, and planning a multi-sensor counter-drone defense.

Next comes gathering the requirements you'll use for specifying your counter-drone solution and qualifying different vendor systems to see whether they meet your needs. The high-level steps for getting to this requirements list are similar to the steps you'd follow on other technology investment projects, but the questions you ask as you go along will be unique to drone-related planning.

As you assemble this information, be mindful of specific considerations pertaining to drone threats and counter-drone capabilities in your environment, as you understand them based on discussions in our previous articles, as well as by completing an assessment such as the ZBeta Drone Vulnerability Risk Assessment (DVRA). The physical security consultant you engage for your assessment is ideally positioned to help you gather and organize these requirements in detail. For now, here's a high-level overview.





1. Determine high-level objectives

What are your primary goals for implementing a counter-drone solution? Typically, your objectives will fall into one or more of the following categories:

- + **Risk management.** Minimize the risk of physical security and data breaches, as well as the physical damage caused by unauthorized drones.
- + **Security enhancement.** Strengthen and augment your facility's existing security capabilities to include identifying and mitigating suspicious drone activities.
- + **Regulatory compliance.** Ensure compliance with relevant laws, regulations, and standards for drone detection technologies as they pertain in your jurisdiction.

2. Gather functional requirements

Ask about the functional capabilities the new program must provide, such as:

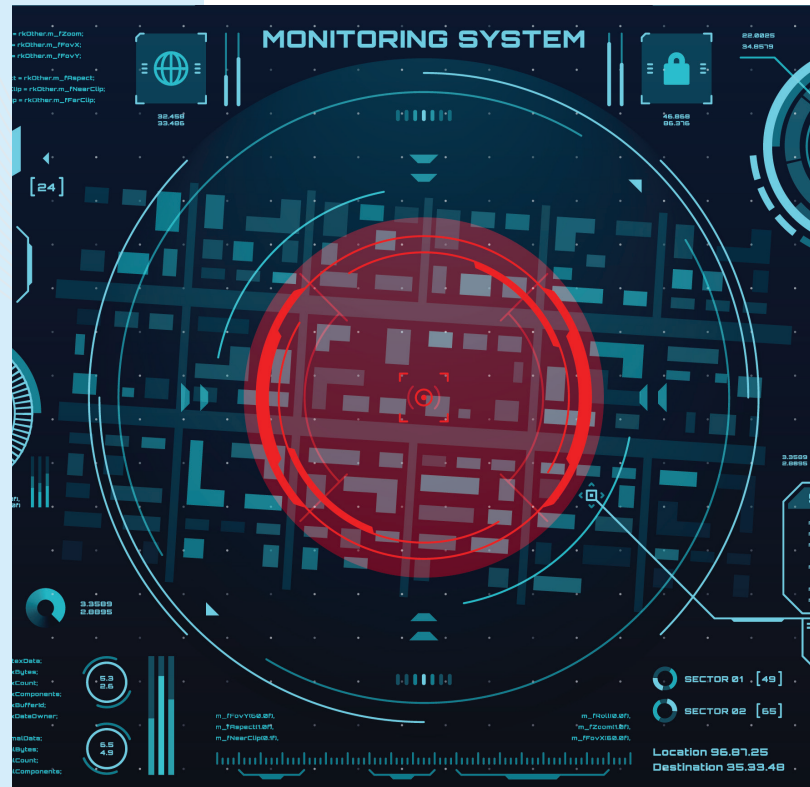
- + What detection capabilities will you need, and what combination of sensor modalities will provide these capabilities?
- + What methods and technologies will you use to identify and classify the drones you detect?
- + What capabilities do you require for tracking and monitoring detected drones as they continue to fly around your airspace?
- + What system of alerts and notifications will you implement to support your counter-drone response?
- + To what extent will your counter-drone system be integrated with other technologies, such as existing security systems and third-party applications?

3. Gather technical requirements

Ask about the technological capabilities of the system you use for the new program, including:

- + How close to 24/7 will the system operate? What is the minimum downtime, detection latency, and notification latency you will tolerate?
- + To what extent must the system be scalable to accommodate future facility growth?
- + What redundancies must be built into the system to avoid single points of failure?
- + What network architecture will you use—for example, cloud-based, on-premises, or air gapped?
- + How will you achieve a user-friendly system interface that's easy for training your personnel?
- + With what federal, state, and other jurisdictional laws and regulations must the system comply?
- + What data security and privacy standards must the system meet for data encryption, access control, audit trails, and required response based on a drone's determined place of origin?

After you've discussed these requirements with your team and any consultants, you and your consultant can use the data you've collected to evaluate and select the appropriate vendors and manufacturers for implementing your counter-drone program.



Read our white paper [Physical security in the drone dimension: Assessing and addressing new threats from the air](#) to learn more about how the recent surge of drone activity affects physical security strategies at companies like yours.

Our Office:

700 Larkspur Landing Circle, Suite 150
Larkspur, CA 94939

E-mail and Web:

info@zbeta.com
www.zbeta.com

Phone:

(855) 559 2382

