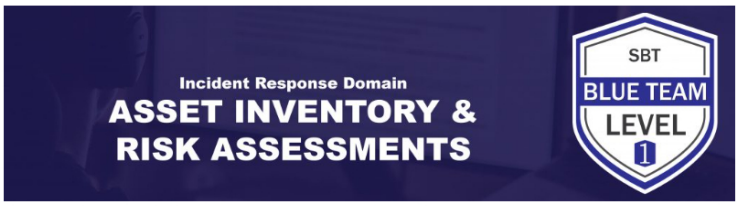
Preparation: Assest Inventory and Risk Assessments



If we want to protect systems, we need to know what assets our organization actually has, so keeping an up-to-date asset inventory can help to monitor production systems, test environments, and other devices that fall under our protection.

Whilst we would ideally protect all systems, sometimes it is not cost-efficient to protect certain assets, and that's where risk assessments come in. Using them, we can identify systems that are of high value to the business, and therefore require more protection than others. This is a huge part of incident response – if multiple incidents occur at the same time, it needs to be clear which incident has priority, and whether the response needs to be immediate or if it can be delayed.

If a security function is unsure of risk to different systems and assets, a good place to start is by looking at the Business Impact Plan and Business Continuity Plan, both of which should clearly outline the critical systems for business operations.

ASSET INVENTORY

Every organization should strive to have a complete inventory of all of their IT systems. Servers, desktops, laptops, and network equipment should be kept in an appropriate platform, and mobile devices and tablets should be kept in a Mobile Device Management (MDM) platform. This will allow for thorough risk assessments to be conducted, and ensure that if an incident occurs, the incident responders can quickly identify the system and contact anyone responsible for maintaining it (system owners). Sometimes system hostnames aren't a description, but if there is a record of that asset in a database with the IP and hostname, it makes it easier to work out what it is and what information, if any, it holds. There are three main ways to gather information about IT assets to build an asset inventory:

- Ask IT staff to make a list of all systems they are aware of.
- Conduct passive reconnaissance using a network sniffer that listens for network activity from hosts and records their details.
- Conduct an active reconnaissance scan using a network enumeration tool such as Nmap, or an enterprise-grade vulnerability management platform such as Nessus.

While all three of these methods can work themselves, using all three is arguably the most appropriate method of creating a complete list of all assets, especially with larger businesses and enterprises.

RISK ASSESSMENT

A risk assessment works to determine the systems that are the most critical to the business, therefore the most valuable. More protection and priority needs to be given to these systems, especially if two incidents occur at the same time, prioritization needs to be clear so that time and resources are focused in the right place.

When risks are identified (such as an internet-facing system, an unpatched system, or a business-critical system) appropriate measures should be taken to properly defend it, but only equal to the amount of risk. There's no point spending £100,000 on security controls for a server that isn't used for anything and isn't facing the internet. By determining risk, the right amount of resources can be given to protect that system. As we covered at the start of the course, there are four approaches to risk:

- Transfer the risk (such as purchasing insurance)

- Accept the risk (a decision that is made to not spend any resources as the impact would be low and the cost too high)
- Mitigate the risk (apply security and other controls to protect the asset and reduce the risk)
- Avoid the risk (an asset that is at too high a risk may simply be taken offline so it can't be exploited)

You can read how cybersecurity risk assessments are conducted on the IT Governance UK website.

Previous Topic
Mark Complete
Next Topic
Back to Lesson