What is Incident Response?

Forcepoint perfectly describes incident response as the following: "**Incident response is the methodology an organization uses to respond to and manage a cyber attack.**"

Security events happen every day, and will typically be dealt with by security analysts (often within a Security Operations Centre, or SOC) whereas security incidents will be handled by specialist incident responders. When a cyberattack is successful, the actions taken by security professionals to analyze, contain, and eradicate the threat are extremely important in order to limit the damage that the attackers can cause, and return operations to normal as quickly as possible to reduce the overall impact on the business. The NIST incident response lifecycle also includes a preparation stage, where security controls are considered and deployed to reduce the likelihood and impact of a successful cyberattack.

Incident response is a reactive approach, and is closely aligned with disaster recovery efforts. Responding to these events in an organized manner with the right resources can save the business money by reducing recovery time and costs. By taking detailed notes and expanding on existing incident response plans and runbooks, organizations can learn from their weaknesses to better defend against future attacks.

Large organizations will typically have their own dedicated team, often called a CSIRT – Computer Security Incident Response Team. This team isn't just comprised of security professionals, it should also include general IT staff, employees from departments such as HR, communications/public relations, and legal, and C-suite level members. We'll cover this in more detail in a future lesson.