Dive into the world of cybersecurity incident detection and response.

Answer Key P1C3

Incident	Log to Collect
Exploitation of a web vulnerability	Web server application logs Web server system logs
Attacker moving through the office network	EDR logs Firewall logs
Attacker compromising credentials from a cloud-based office suite	Logs from cloud-based office applications Cloud provider connection logs

Notes on the correction of the table:

- **Firewall logs:** We can use firewall logs to detect the movement of the attacker in two ways: by identifying connections between machines if the firewall is appropriately configured, and by seeing which infected machines contacted the attacker's command and control server.
- **Directory logs:** Directory logs can also be used to check which machines the attacker logged into and with which accounts. When logging into a computer with an account, the directory either authorizes or denies the connection. As a result, the directory has a global view of who logged into which machines on the network. The same applies to office suites, which in the case of Méditronique, still uses the directory for authentication.