Überwachung, Analyse und Reaktion

Modell der Zugriffskette:

Schritt	Bedeutung
1. Erfassung	Was passiert?
2. Protokollierung	Wo wird es erfasst?
3. Detektion	Welcher Defender schlägt an?
4. Analyse	Welche Informationen werden zusammengeführt?
5. Reaktion	Welche Maßnahme ist sinnvoll?
6. Nachverfolgung	Was wird dokumentiert/verbessert?

Aufgabe (für jede Gruppe gleich):

Lest euch euer Szenario durch und nutzt im Anschluss die 6-Schritte-Zugriffskette, um die einzelnen Schritte zu beschreiben. Nutzt dabei vollständige Sätze.

Szenario 1: Phishing & Anmeldung

- Benutzer erhält eine E-Mail mit Link
- klickt darauf
- meldet sich kurz darauf erneut an

Szenario 2: Auffälliges Gerät

- Benutzer meldet sich korrekt an
- Gerät startet ungewöhnliche Prozesse
- Datenzugriff steigt stark an

Szenario 3: Admin-Aktion

- Admin aktiviert kurzfristig eine privilegierte Rolle
- ändert Sicherheitseinstellungen
- meldet sich aus einem ungewöhnlichen Land an

Szenario 4: Datenabfluss über Cloud-App

- Ein Benutzer lädt ungewöhnlich viele Dateien aus SharePoint herunter
- Kurz darauf werden Dateien in eine externe Cloud-App hochgeladen
- Die Aktivität findet außerhalb der üblichen Arbeitszeit statt