الAuditing بيحصل لما مجموعة فى شركة يعملو review على طريقة الشغل وهل هيا بتم بشكل صحيح وطريقة حديثة ولا لا

لما بتعمل audit انت بتحاول تكتشف ايه الى بيحصل بالظبط :

بتشوف مشاكل الsecurity

بمكن الemployers انهم ياخدو قرارات افضل بما انى بشوف الطرق الافضل ديما اثناء المراجعة ديه
طبعا بـevaluate السيستم بحث اشوفه شغال كويس ولا لا هو والprocesses وبعرف ايه الrisks الى ممكن تهدد الsystem

طب ازاى انت هتعرف ايه الى بيحصل بالظبط فالSystem

بعرف الtopology بتاعة الnetwork

بعرّف كل الhosts الى داخلين على الnetwork

بحدد كل الservices الى بتكون running فى الوقت الحالى على كل الhosts

بشوف كل الاعدادات بتاعة الservices ديه متظبطة ولا لا لكل host

وبنشوف حاجة اسمها logs

ايه هيا الlogs : ده عبارة عن document بيتسجل فيه اى event بيحصل جوا الsystem

وكدا احنا عرفنا الauditing

طيب عندنا حاجة اسمها logging .. لما بتعمل log انت بتسجل data .. صح .. طب احنا عندنا انواع من الlog منها الaudit logs والtransaction log والconnection log
الaudit log ده الى اتكلمنا عليه بنعرف مين دخل ع السيستم وخرج امتا وعمل ايه

الtransaction log ده بيستخدمه الDB administrator عشان ي protect الDB

السيستم بيكون معرض لنقط تأثر لو مبيتعملش Auditing and logging بشكل كافى وده بيكون ليه تأثير سلبى على السيستم هو اه هيطلع logs بس هتكون غامضة ومش مفيدة لا للadministrator ولا للdevelopers الى هما مش هيعرفو يتصرفو لو فى حاجة مش واضحة قصادهم
انك تخلى الlogs متسجلة على local storage ده بسهل الدنيا على اى حد انه يدخل ويعدل ف الlogs ويقدر يلغى اى event يكون خطر ع السيستم

ولو الalerts مش معمولة كويس ده نقطة ضعف طبعا لانى ببقى عايز alert لو فى اى event مختلف عن المعروف حصل

طب ايه فايدة ال Auditing and logging بقى عموما كدا :
الشركات بتستخدمه عشان يحسنو الsecurity بأكثر من طريقة .. عشان بتعرفهم ايه الى بيحصل فى السيسم ومين الدخلاء وايه الevents الى بتتم وبيحددو ايه المشاكل الاداء الضغيف او ان السيستم بأدى وظائف غير المطلوبة