1. اختراق البيانات مثل معلومات الصحة الشخصية أو المعلومات المالية أو معلومات التعريف الشخصية (PII) أو الأسرار التجارية أو الملكية الفكرية . تكون البيانات التي يحصل عليها المخترق ذات قيمة لأطراف أخرى فمثلا قد تكون المعلومات المالية أو الصحية أو الشخصية كافية للقيام بأنشطة احتيالية ؛ كما قد يرغب النشطاء في كشف هذه المعلومات التي يمكن أن تسبب أضرارًا أو إحراجًا لأصحابها ، 2. انتهاك البيانات من خلال الوصول إلى الهوية وضعف استخدام كلمة المرور ، والافتقار إلى التدوير الآلي المستمر لمفاتيح التشفير وكلمات المرور ، حيث يمكن للمخترقين التنكر كمستخدمين أو مشغلين أو مطورين والتطفل على البيانات أو إصدار البرامج الضارة التي يبدو أنها تنشأ من مصدر موثوق، 3. واجهات التطبيقات غير آمنة يجب تصميم واجهات مستخدم البرنامج (UIs) وواجهات برمجة التطبيقات (APIs)بنظام حماية قوي للوقوف ضد كل المحاولات الخبيثة للتحايل للوصول إلى داخل الأنظمة ، حيث تعد واجهات برمجة التطبيقات وواجهة المستخدم عمومًا الجزء الأكثر ظهورا، 4. نقاط الضعف في النظام نقاط الضعف في النظام هي أخطاء قابلة للاستغلال في البرامج والتي يمكن للمهاجمين استخدامها للتسلل إلى نظام كمبيوتر بغرض سرقة البيانات أو السيطرة على النظام أو تعطيل الخدمات ، 5. سرقة الحسابات إلا ان الحلول السحابية تضيف تهديدًا جديدًا إلى هذه النوعية القائمة ، فسيمكنه التنصت على أنشطته ومعاملاته ، أو يمكنه الاستفادة من قوة سمعة العميل في شن هجمات لاحقة . فعند سرقة بيانات الاعتماد يمكن للمهاجمين في كثير من الأحيان الوصول إلى مناطق حرجة في خدمات الحوسبة السحابية ، 6. التهديدات الداخلية التهديد الداخلي الخبيث يمكن أن يأتي عن طريق موظف حالي أو سابق أو شريك تجاري قد سمح له بالوصول إلى شبكة أو نظام أو بيانات مؤسسة وتجاوز ذلك أو أساء استخدامه للوصول بطريقة تؤثر سلبًا على سرية أو سلامة نظم معلومات المنظمة ، من IaaS إلى PaaS و SaaS ، كما يمكن أن يكون لدى الشخص القدرة على الوصول إلى مستويات أكثر أهمية من البيانات ،