17 الموضوع الأول: مفهوم الحوادث الأمنية وتصنيفها (حدث أو مجموعة أحداث غير مرغوب فيها أو غير متوقعة تهدد أمان المعلومات أو تؤثر سلباً على العمليات التجارية للمؤسسة يعطل أو يهدد استمرارية الأعمال يتطلب إجراءات فورية للتعامل معه أي نشاط قابل للملاحظة في النظام أو الشبكة قد يكون طبيعياً أو مشبوها لا يتطلب بالضرورة استجابة فورية :)Security Incident(الحادث الأمني حدث أو مجموعة أحداث تشكل تهديداً حقيقيا له تأثير سلبي مؤكد أو محتمل الوصول غير المصرح به للأنظمة أو الشبكات استخدام بيانات اعتماد مسروقة أو مخترقة اختراق موقع إلكتروني وتعديل محتواه الوصول غير المصرح به لقاعدة بيانات العملاء تثبيت برمجيات ضارة على أجهزة الشركة استخدام حسابات موظفين سابقين لم يتم إلغاؤها :)Malware(البرمجيات الضارة . الفيروسات التي تصيب الملفات والبرامج الديدان التي تنتشر عبر الشبكة تلقائيا أحصنة طروادة التي تخفي وظائفها الحقيقية برمجيات الفدية التي تشفر الملفات وتطلب فدية انتشار فيروس في شبكة الشركة يعطل الأجهزة برنامج فدية يشفر ملفات مهمة ويطلب دفع مبلغ مال حصان طروادة يسرق كلمات المرور والمعلومات الحساسة دودة تستنزف موارد الشبكة وتبطئ الأداء :)DoS/DDoS(هجمات الحرمان من الخدمة إغراق الخوادم بطلبات مزيفة استنزاف موارد النظام (المعالج، منع المستخدمين الشرعيين من الوصول للخدمات هجوم على موقع التجارة الإلكترونية يمنع العملاء من الشراء استهداف أنظمة الدفع الإلكتروني وتعطيلها هجوم على البنية التحتية للاتصالات :)Data Breaches(تسريب البيانات . سرقة البيانات الشخصية أو المالية للعملاء انتهاك خصوصية الموظفين أو العملاء سرقة قاعدة بيانات تحتوي على معلومات بطاقات ائتمان تسريب رسائل بريد إلكتروني سرية للإدارة العليا نشر معلومات شخصية للعملاء على الإنترنت سرقة تصاميم منتجات أو خطط استراتيجية يمكن التعامل معه بالموارد العادية إصابة جهاز واحد بفيروس، تأثير كبير على العمليات الأساسية تسريب بيانات عملاء تأثير شديد على استمرارية الأعمال مثال: هجوم فدية على الأنظمة الرئيسية، يشمل المجرمين والهاكرز والمنافسين تحديد الأولويات في حالة حوادث متعددة عدد المستخدمين المتأثرين CSIRT(الموضوع الثاني: إنشاء فريق الاستجابة للحوادث الأمنية تعريف فريق الاستجابة للحوادث Computer Security Incident Response Team – فريق الاستجابة للحوادث الأمنية هو مجموعة متخصصة من الأفراد المدربين على التعامل مع الحوادث الأمنية تقليل تأثير الحوادث الأمنية على المؤسسة من خلال الاستجابة السريعة خبرة واسعة في أنواع مختلفة من الحوادث تكلفة أقل للمؤسسات الصغيرة قد يحتاج وقت أطول للاستجابة يجمع بين الموارد الداخلية والخارجية فريق داخلي صغير مع دعم خارجي عند الحاجة توازن بين التكلفة والفعالية مرونة في التعامل مع حوادث مختلفة الأحجام التنسيق بين أعضاء الفريق المختلفين التواصل مع الإدارة العليا والجهات الخارجية مهارات قيادية وإدارية قوية قدرة على العمل تحت الضغط تحديد سبب الحادث وطريقة حدوثه خبرة تقنية عميقة في أنظمة التشغيل والشبكات مهارات التحليل الجنائي الرقمي قدرة على التفكير التحليلي والمنطقي :)Systems Engineer(مهندس الأنظمة الحلول التقنية للاحتواء تطبيق مهارات استكشاف الأخطاء وإصلاحها قدرة على العمل بسرعة ودقة إعداد البيانات الصحفية عند الحاجة إدارة التواصل مع العملاء والشركاء مهارات تواصل وكتابة ممتازة قدرة على التعامل مع الإعلام :)Legal Advisor(المستشار القانوني تقديم المشورة القانونية أثناء الحادث فهم أنواع الحوادث الأمنية المختلفة التدرب على استخدام الأدوات المتخصصة تمارين على إدارة الأزمات تطوير مهارات التحليل الجنائي التدريب على التعامل مع الإعلام الأدوات والموارد المطلوبة مكان مخصص لإدارة الأزمات 18 الموضوع الثالث: مراحل الاستجابة للحوادث الأمنية (NIST) المعهد الوطني للمعايير والتقنية الأمريكي النشاط ما بعد Containment, المرحلة الأولى: التحضير :وضع السياسات والإجراءات تطوير سياسة شاملة للاستجابة للحوادث تحديد أنواع الحوادث وإجراءات التعامل مع كل نوع اختيار وضع جداول المناوبة والاستعداد :إعداد الأدوات والموارد شراء وتكوين أدوات التحليل والاستجابة SOC) تجهيز مركز عمليات الأمان : التدريب والتوعية إجراء تمارين محاكاة دورية تطوير مواد تدريبية وإرشادية Detection & Analysis) المرحلة الثانية: الكشف والتحليل أنظمة كشف ومنع التطفل تقارير من الموظفين عن التأكد من صحة التنبيه أو التقرير الحادث جمع المعلومات الأولية عن :التحليل التفصيلي تقييم نطاق التأثير والأنظمة المتضررة تحديد مصدر الهجوم أو سبب الحادث تسجيل جميع المعلومات والأدلة إنشاء خط زمني للأحداث الاحتواء الهدف تطبيق قواعد جدار الحماية الطارئة : الاحتواء طويل المدى تعزيز المراقبة والحماية إزالة الحسابات المخترقة أو المشبوهة : الأنشطة التحقق من سلامة البيانات والخدمات المرحلة الرابعة: النشاط ما بعد الحادث تحديد نقاط القوة والضعف تقدير التكاليف والأضرار الإجمالية تحديث السياسات والإجراءات مشاركة الخبرات مع المجتمع الأمني دقيقة تعريف التحليل الجنائي الرقمي التحليل الجنائي الرقمي تحديد هوية المهاجم أو المتسبب جمع جميع الأدلة المحتملة عدم إغفال أي مصدر للمعلومات :

الموضوعية أنواع الأدلة الرقمية البيانات المؤقتة والمخبئة جمع المعلومات الأولية فحص الملفات والبيانات المجمعة ربط الأدلة المختلفة ببعضها توثيق النتائج بطريقة واضحة إعداد تقرير قابل للفهم من غير المتخصصين منصة شاملة للتحليل الجنائي Autopsy: حل شامل للتحليل الجنائي: