

نموذج تقرير الحادث السيبراني الشامل

Comprehensive Cybersecurity Incident Report

Report Information / معلومات التقرير

رقم التقرير / Report Number: IR-2024

تاريخ إعداد التقرير / Report Date:

معد التقرير / Prepared by:

المنصب / Position:

تاريخ المراجعة / Review Date:

1. الملخص التنفيذي / Executive Summary

نظرة عامة على الحادث / Incident Overview

الأثر الرئيسي / Key Impact

- الأثر التشغيلي / Operational Impact:
- الأثر المالي / Financial Impact:
- الأثر على السمعة / Reputational Impact:
- الأثر القانوني / Legal Impact:

الإجراءات الرئيسية المتخذة / Key Actions Taken

التوصيات الأساسية / Key Recommendations

2. تفاصيل الحادث / Incident Details

معلومات أساسية / Basic Information

- تاريخ ووقت الحادث / Incident Date & Time: __
- تاريخ ووقت الاكتشاف / Discovery Date & Time: __
- مدة الحادث / Incident Duration: __
- الموقع / Location: __
- المكتشف / Discovered by: __

تصنيف الحادث / Incident Classification

- نوع الحادث / Incident Type:
 - [] برمجيات خبيثة / Malware
 - [] اختراق الشبكة / Network Intrusion
 - [] تسريب البيانات / Data Breach
 - [] هجوم الحرمان من الخدمة / DoS/DDoS
 - [] هندسة اجتماعية / Social Engineering
 - [] تصيد إلكتروني / Phishing
 - [] انتهاك السياسات / Policy Violation
 - [] أخرى / Other: __
- مستوى الخطورة / Severity Level:
 - [] منخفض / Low
 - [] متوسط / Medium
 - [] عالي / High
 - [] حرج / Critical

وصف مفصل للحادث / Detailed Incident Description

3. الأنظمة والبيانات المتأثرة / Affected Systems and Data

الأنظمة المتأثرة / Affected Systems

اسم النظام / System Name	نوع النظام / System Type	مستوى التأثير / Impact Level	حالة النظام / System Status

البيانات المتأثرة / Affected Data

- أنواع البيانات / Data Types:
 - [] بيانات شخصية / Personal Data
 - [] بيانات مالية / Financial Data
 - [] بيانات طبية / Medical Data
 - [] معلومات سرية / Confidential Information
 - [] ملكية فكرية / Intellectual Property
- كمية البيانات المتأثرة / Amount of Affected Data:
 - عدد السجلات / Number of Records: ____
 - حجم البيانات / Data Size: ____
 - نوع الملفات / File Types: ____

تقييم الأثر / Impact Assessment

- الأثر على العمليات / Operational Impact:
 - [] توقف كامل / Complete shutdown
 - [] توقف جزئي / Partial shutdown
 - [] تباطؤ في الأداء / Performance degradation
 - [] لا يوجد أثر / No impact
- الأثر على العملاء / Customer Impact:

- عدد العملاء المتأثرين / Number of affected customers: __
- نوع التأثير / Type of impact: __

4. التحليل التقني / Technical Analysis

نقطة الدخول / Entry Point

طريقة الهجوم / Attack Method

الأدوات المستخدمة / Tools Used

المؤشرات الأمنية (IOCs) / Indicators of Compromise

• عناوين IP المشبوهة / Suspicious IP Addresses:

• أسماء الملفات المشبوهة / Suspicious File Names:

• التوقيعات الرقمية / Digital Signatures:

الجدول الزمني للحدث / Incident Timeline

Source / المصدر	Event / الحدث	Date & Time / الوقت والتاريخ

5. الاستجابة والإجراءات المتخذة / Response and Actions Taken

فريق الاستجابة / Response Team

الاسم / Name	المنصب / Position	الدور / Role	معلومات الاتصال / Contact

الإجراءات الفورية / Immediate Actions

الوقت / Time	الإجراء / Action	المسؤول / Responsible	النتيجة / Result

إجراءات الاحتواء / Containment Actions

--

إجراءات الإزالة / Eradication Actions

--

إجراءات الاستعادة / Recovery Actions

--

--

6. التكاليف والأضرار / Costs and Damages

التكاليف المباشرة / Direct Costs

- تكلفة الاستجابة / Response Cost: ___
- تكلفة الإصلاح / Repair Cost: ___
- تكلفة الاستشارات الخارجية / External Consulting Cost: ___

التكاليف غير المباشرة / Indirect Costs

- تكلفة التوقف / Downtime Cost: ___

- فقدان الإنتاجية / Productivity Loss: ____
- تكلفة الفرص الضائعة / Opportunity Cost: ____

التكلفة الإجمالية / Total Cost

التكلفة الإجمالية المقدرة / Estimated Total Cost: ____

7. الإبلاغ والتواصل / Notification and Communication

الإبلاغ الداخلي / Internal Notification

المسؤول / Responsible	طريقة الإبلاغ / Method	تاريخ الإبلاغ / Notification Date	الجهة / Party

الإبلاغ الخارجي / External Notification

المسؤول / Responsible	طريقة الإبلاغ / Method	تاريخ الإبلاغ / Notification Date	الجهة / Party

التواصل مع وسائل الإعلام / Media Communication

- هل تم التواصل مع الإعلام؟ / Was media contacted? [] نعم / Yes [] لا / No
- تفاصيل التواصل / Communication Details:

8. التحليل الجنائي / Forensic Analysis

الأدلة المجمعة / Evidence Collected

نوع الدليل / Evidence Type	الوصف / Description	الموقع / Location	تاريخ الجمع / Collection Date

نتائج التحليل / Analysis Results

التوصيات الجنائية / Forensic Recommendations

9. الدروس المستفادة / Lessons Learned

ما سار بشكل جيد / What Went Well

ما يحتاج للتحسين / What Needs Improvement

الثغرات المكتشفة / Identified Gaps

10. التوصيات والإجراءات المستقبلية / Recommendations and Future Actions

التوصيات الفورية / Immediate Recommendations

الموعد المستهدف / Target Date	المسؤول / Responsible	الأولوية / Priority	التوصية / Recommendation

التوصيات طويلة المدى / Long-term Recommendations

الموعد المستهدف / Target Date	المسؤول / Responsible	الأولوية / Priority	التوصية / Recommendation

خطة التحسين / Improvement Plan

11. المرفقات / Attachments

قائمة المرفقات / Attachment List

- [] السجلات التقنية / Technical Logs
 - [] لقطات الشاشة / Screenshots
 - [] تقارير الأدوات / Tool Reports
 - [] المراسلات / Correspondence
 - [] الوثائق القانونية / Legal Documents
 - [] أخرى / Other: ____
-

12. التوقيعات والاعتمادات / Signatures and Approvals

إعداد التقرير / Report Preparation

معد التقرير / Prepared by: الاسم / Name: ____ - المنصب / Position: ____ - التوقيع / Signature: ____
- التاريخ / Date: ____

مراجعة التقرير / Report Review

مراجع التقرير / Reviewed by: الاسم / Name: ____ - المنصب / Position: ____ - التوقيع / Signature: ____
- التاريخ / Date: ____

اعتماد التقرير / Report Approval

معتمد التقرير / Approved by: الاسم / Name: ____ - المنصب / Position: ____ - التوقيع / Signature: ____
- التاريخ / Date: ____

ملاحظات إضافية / Additional Notes:

تصنيف التقرير / Report Classification: [] عام / Public [] داخلي / Internal [] سري / Confidential [] سري للغاية / Top Secret

تاريخ انتهاء السرية / Declassification Date: ____