CONCEPT

# التوعية بالأمن السيبراني للقيادات التنفيذية: التهديدات والرقابة وقرارات الأزمات

31 May - 04 Jun 2027

أمستردام - فندق حي الأعمال زوداس

# التوعية بالأمن السيبراني للقيادات التنفيذية: التهديدات والرقابة وقرارات الأزمات

المرجع: 1016_614 التاريخ: 31 May - 04 Jun 2027 الموقع: أمستردام - فندق حي الأعمال زوداس الرسوم: SAR 23500

العمق التقني: مفاهيمي · أسلوب التطبيق: محاكاة

## مقدمة

يستهدف المهاجمون القيادات العليا مباشرة بصورة متزايدة، عبر طلبات دفع منتحلة ومكالمات بالتزييف العميق وأجهزة شخصية مخترقة، وسرعان ما يتحول الحادث السيبراني إلى أزمة قيادية لها تبعات نظامية ومالية وأثر على السمعة. وما زال كثير من التنفيذيين يعدون الأمن السيبراني شأنا تقنيا، فيواجهون أول قرار حقيقي في أثناء الهجوم. تبني هذه الدورة من كور كونسبت الوعي والتقدير اللذين تحتاجهما القيادات لحماية أنفسها ومساءلة تقارير الأمن والتصرف تحت الضغط. ويتدرب المشاركون على القرارات في محاكاة محددة بزمن، ويخرجون بخطة الجاهزية السيبرانية للقيادات التنفيذية.

## أهداف الدورة

- التعرف على أنماط الهجوم الأكثر استهدافا للقيادات والمؤسسة، من برامج الفدية إلى الاحتيال بالتزييف العميق
- فهم إطار NIST CSF 2.0 والمواصفتين IEC/ISO 27001 وIEC/ISO 27014 بما يكفي لمساءلة قيادات الأمن والحكم على تقاريرهم
- تطبيق ممارسات الأمن الشخصي وبروتوكولات التحقق التي تحمي حسابات القيادات وأجهزتهم واعتماداتهم
- مساءلة التقارير الإدارية عن المخاطر السيبرانية ومستوى تقبل المخاطر ومخاطر الأطراف الثالثة بأسئلة مدروسة
- اتخاذ القرارات الحرجة زمنيا في أثناء الحادث السيبراني وإبلاغها ضمن هيكل متفق عليه لإدارة الأزمات
- الالتزام بخطة الجاهزية السيبرانية للقيادات التنفيذية للمتابعة على المستويين الشخصي والمؤسسي

## الفئة المستهدفة

- الرؤساء التنفيذيون والمديرون العامون المسؤولون عن المخاطر المؤسسية
- أعضاء مجالس الإدارة ولجان المراجعة المشرفون على المخاطر السيبرانية
- الرؤساء التنفيذيون للمالية المسؤولون عن ضوابط المدفوعات والتأمين السيبراني
- رؤساء الشؤون القانونية والامتثال والاتصال المؤسسي الذين يتحركون في الأزمات السيبرانية
- الرؤساء التنفيذيون للعمليات ورؤساء وحدات الأعمال الذين تعتمد خدماتهم على الأنظمة الرقمية
- القيادات العليا في القطاع العام المسؤولة عن الخدمات المقدمة للمواطنين

## محاور الدورة

### اليوم الأول: بيئة التهديدات التي تواجه القيادات

- أنواع الجهات المهاجمة ودوافعها بأمثلة من إطار MITRE ATT&CK لتكتيكات الهجوم
- نماذج أعمال برامج الفدية والابتزاز المزدوج
- اختراق البريد الإلكتروني للأعمال وأنماط انتحال صفة القيادات
- الاحتيال بالصوت والفيديو المزيفين عميقا لاستهداف القيادات العليا
- لمحة عن التعرض السيبراني للمؤسسة باستخدام ملفات NIST CSF 2.0

## اليوم الثاني: الأطر التي ينبغي أن يعرفها كل تنفيذي

- وظيفة الحوكمة Govern في NIST CSF 2.0 ومسؤوليات القيادة
- أساسيات نظام إدارة أمن المعلومات وفق IEC/ISO 27001:2022
- عمليات حوكمة أمن المعلومات وفق IEC/ISO 27014
- مبادئ ISA-NACD لرقابة مجالس الإدارة على المخاطر السيبرانية
- مفاهيم القياس الكمي للمخاطر السيبرانية بنموذج FAIR

## اليوم الثالث: سلوكيات القيادة وأسئلة الرقابة

- الأمن الشخصي للقيادات: الأجهزة والسفر والبصمة على وسائل التواصل الاجتماعي
- بروتوكولات التحقق من المدفوعات والاعتمادات لمواجهة الانتحال
- أسئلة لوحة معلومات الأمن السيبراني ومؤشرات الأداء الرئيسية في التقارير الإدارية
- مبادئ بيان تقبل المخاطر السيبرانية
- أسئلة مخاطر الأمن السيبراني للأطراف الثالثة وسلاسل الإمداد الموجهة إلى الموردين

## اليوم الرابع: الحوادث وقرارات الأزمات والصمود

- دورة إدارة الحوادث وفق IEC/ISO 27035-1
- اعتبارات قرار دفع الفدية ودور المستشار القانوني
- بروتوكول التواصل في الأزمات مع الجهات التنظيمية والعملاء ووسائل الإعلام
- أهداف التعافي وربطها باستمرارية الأعمال وفق ISO 22301
- أخطاء القيادات المستخلصة من مراجعات منشورة لحوادث اختراق

## اليوم الخامس: محاكاة الطاولة والتخطيط للعمل

- محاكاة طاولة لهجوم فدية: الساعات الأربع الأولى
- محاكاة احتيال بالتزييف العميق لصوت أحد التنفيذيين: اعتماد دفعة تحت الضغط
- استخلاص الدروس من المحاكاة ومراجعة سجل القرارات
- إعداد مسودة خطة الجاهزية السيبرانية للقيادات التنفيذية
- مراجعة الزملاء للخطط والتدرب على إحاطة مجلس الإدارة

## المهارات المكتسبة

- الوعي بالتهديدات السيبرانية
- الرقابة على المخاطر السيبرانية
- كشف أساليب الهندسة الاجتماعية
- اتخاذ القرار في الأزمات
- التواصل في الأزمات السيبرانية
- قراءة تقارير الأمن السيبراني
- مساءلة مخاطر الأطراف الثالثة
- التخطيط للصمود المؤسسي

## لماذا تحضر هذه الدورة

- تعود إلى عملك بخطة الجاهزية السيبرانية للقيادات التنفيذية وقد اختبرت في محاكاة لهجوم فدية واحتيال بالتزييف العميق
- تعرف القرارات التي تقع على عاتقك في الساعات الأولى من الحادث ومن يجب أن يكون إلى جانبك
- تسد الثغرات في أجهزتك وحساباتك وعادات الاعتماد لديك التي يستغلها المهاجمون للوصول إلى المؤسسة
- تستمع إلى تجارب قيادات من قطاعات ودول مختلفة في التعامل مع الاختراقات وما كانوا سيغيرونه

## الخاتمة

يحسم الأمن السيبراني في قاعات مجالس الإدارة ومكاتب القيادات بقدر ما يحسم في مراكز العمليات الأمنية. تنتقل هذه الدورة من التهديدات التي تستهدف القيادات، مرورا بالأخطر التي ينبغي أن يعرفها التنفيذيون وأسئلة الرقابة التي يطرحونها، وصولا إلى القرارات التي ترسم الساعات الأولى من الأزمة. ويضع اليوم الأخير المشاركين في محاكاة محددة بزمن، ويحول الدروس إلى خطة الجاهزية السيبرانية للقيادات التنفيذية، حتى تواجه المحاولة التالية على المؤسسة فريق قيادة مستعدا.