

?????? ?????

????????

فعضل طاقنو تاحيحصتلا ةرادإو، رييغتلا ةرادإ — ينمأل اهجمانرب Cyber Crucible ريڈت فيك
طاقن في مكحتلاو، تاقارتخالو ثداوخلل ةباجتسالو، لامأل ةرارمتساو ثراوكلا نم فيفاعتلاو
ةيقافتا بحومب مّدقّي امو قّثوم وه ام حوضوب نّيبُت. نيدرولم رطاخم يعجارمل ةحضوم — ةياهنلا
تاداهش يأل علل لوصحلل يّغت الو، (NDA) حاصفإ مدع.

- [رييغتلا ةرادإل ةيلمع Cyber Crucible كلتمت له](#)
- [\(Patch Management\) تاتيحتلا ةرادإل آجمانرب Cyber Crucible كلتمت له](#)
- [لامأل ةرارمتساو ثراوكلا دعب ةطشنأل ةداعتسال ةطخ Cyber Crucible كلتمت له](#)
- [تاقارتخالاب راطخالو ثداوخلل ةباجتسالل ةيلمع Cyber Crucible كلتمت له](#)
- [اهب مكحتتو ةياهنلا طاقن Cyber Crucible نّمؤت فيك](#)
- [اهبلط يننكمي فيكو، Cyber Crucible اهب ظفتحت يتل نامأل تاسايس يه ام](#)

?? ????? Cyber Crucible ????? ???????? ???????????

ةقثوم رييغت ةرادإ ةي لمعل جاتنإل ةئي ب ي ف تارييغتال عضخت .م عن :ةرصتخملا ةباجإل
نإف ،(kernel) ةاونلل ةوتسم ىلعل لمعي جتنملا نأل ارطنو .ةقفاوملاو رابتخالو ةعجارملا لمشت
ةيسدنه ةسرامم درجم سيلو ينمأ طباضك لمأغي رييغتال ةرادإ ي ف طباضنالا

?? ????? ?????????

،مداوخل تادادعإو ،(kernel drivers) ةاونلل تالغشمو ،قيبطتال ةرفيش ىلعل تارييغتال رمت
ةلحرم ي ف ةنمأل تابلطتملا ددخت :ةدحم ةايح ةرود لحارم ربع ةمعادل ةتحتال ةينبلو
؛ةحيرص ةيصن ةغيصب رارسأ ي أ نيمضت مدع عم تارادصلإ ةرادإل ردصملا عضخيو ؛ميمصتال
ةعجارملا جاتنإل تارييغت عضختو ؛ةتيقرت لبقت تارييغتال ةحص نم ي لآل رابتخال ققحتيو
ةهجلال وه رييغتال دغم نوكتي ال ثيحب ،ماهمل نيب لصفلا ىلعل طفاخي امك .نيتي مسر ةقفاومو
تامدخلال لي طعت عم ،ةدمتعم ةئيهت ةلدأ ةيساسأل مداوخل تادادعإ عبتتو .هل ةدمتعمل ةديحو
أي لمعل كلذ نكمأ امثي ةمدختسملا ريغ

???????? ?????????? ????????????

أفدهتسم أرابتخاو أضيوفت ب ل طتت لازت ال ةلجعم تاراسم ئراوطلال تارييغتال مدختست
ىلعل لوصحلل مّدقتو ،يلخاد ةدوج نامضل Windows ةاون تالغشم عضختو .ذيفننلل ةقحال ةعجارمو
لقتسم صحف وهو — اهراصلإ لبقت Microsoft نم Windows (WHCP) ةزهجأ قفاوت جم انرب ةداهش
أزايتما تانوكملا رثكأل يجراخو

???????? ?? ?????? ??????????? ?????????? ?????????

الو .A.8.32 دنبلال ISO/IEC 27001:2022 رايعمو (CM ةلئاع) NIST SP 800-53 عم ةي لمعلال هذه قفاوتت
ةيليصفتال رييغتال ةرادإ تاءارجإ مّدقت .دامتعا ةداهش ي أ لعل لوصحلل Cyber Crucible ي دّت
(NDA) ءاشفإ مدع ةيقافاتا بجومب ني عجارملا ةمعادل ةلدأللو

?? ????? Cyber Crucible
 ?????????? ??????? ??????????????
 (Patch Management)?

يُلعق عيونهم أَلأ تارغثلاو تاتثي دحتلا ةرادإل رطاخم الما لىل عئاق جامن رب ظفاحي .معن : **ةزجوم ةباح** إ جئاتنللا عبتت متي و ،ةياهنللا طاقنو مداوخلالو (kernel drivers) ةاونللا تاكرحمو جامربللا ثي دحت اهلح يتح .

???

يؤدي قارتخا رابتخا ىرْجُو، ريوطتال بيبياناً طخنمضة رمتسم ةيلا ةنم تارابتخا ءارجإ متي، يرهوج ريغت لك دنع ثادألاب زَّفُحُت تارابتخا ذي فننت متي، ويونس ىندأ دحب رطاخم الىل عمئاق تاحالصل او ةينمأل تاتي دحتل قيبطت متي. ةيجراخ لاو ةيلخادلا تاكبشلا نمألك ي طغتو ةبك او مةيلوؤسم ةكلاملا تاعومجمل لمحتتو، دُروملا تايصوتل آقفو (hot-fixes) ةلجاعلا ةيامحل ايو تسم سफल ةلومحمل او ةلازال ةلباقلا طئاسولا عرضت. اهل لومعمل تاتي دحتلا ةتباتلا طئاسولا الىل قبطملا صحلل او

???? ???? ???? ???? ?

تارغلثالجالغُتثيح، لالغسالاةيلباقوروطخاللىعْءانبجئاتالنلتايولوأديدت مثة
 ةراداةيلمع ثاثي دحتالعبتت، داتعلم الاطنالجرأوخويعيرس راسم ربعايل عف لَغتسم
 تاكرحم ثاثي دحت عضخت امك — جاتنإلاةئيةبلىإيقرتاللبق اهنم ققحتال متيو — ريعيغتال
 اهرادصا لبق Microsoft WHCP لالخال نم ققحتال دعالإ (kernel-driver) ةاونال

?????? ?? ????? ????????? ??????????
 ?????????

ISO/IEC CIS Control 7 و NIST SP 800-53 (SI-2, RA-5) و NIST SP 800-40 عم جم ان رب ل ق فاوتي فدهت سمل حال ص إل تار تف مّ دقّت . دام تعا ةداهش ي أ يل ع لو صل ح اى عّ دّي ال 27001:2022 A.8.8. (NDA). حاصل ف مدع ى قافتا بجومب ني عجارم ال يل إل حال ص إل ةلدأو ةدحم ال

?? ????? Cyber Crucible ??

????????? ?????????? ???

????????? ?????????????????? ?????????????

ثراوكلال دعب ةطشنأل ةداعتسال ةرّبتخم ةطخب Cyber Crucible ظفتحت .معن :**ةزجوم ةباج** قيقحتل ةممصم ةيرامعم ةينب بناج ىلإ ،اهنع ةيولوؤسمال تامولعمل ةينقت ةرادإ ىلوت ةطقن ةيامح رمست ،ةياهنلال ةطقن ىلع آي لحم لمعي تاديدهتل عنم نأل آرطنو .يلاعلا رفاوتل ةرادإلل ةيفللخال ةمدخل اعاطقنا ءانثأ ىتح ةياهنلال .

????????? ?? ????? ????????? ?????????????

يدؤي ال ثيحب (replicated) ررّكمو رركتم نينخت مادختساب ةرادإلل ةيفللخال ةهجالو ءانب مت ةمدخل ىوتسم ةيقافتا مزلتلتو .ةمدخلال فقوت وأ تانايبال نادقف ىلإ ةيدرف ةدقع نادقف ءانثتساب ،ريراقتل دادعإو ةرادإلل ةيفللخال ةهجالول 99.9% ةبسننبرهش رفاوتب ةروشنمل ةياهنلال ةطقن ةيامح رثأتت الو .ةلوقعمل ةرطيصلال نع ةجراخل بابسألاو ةلودجمل ةنايصلل ةيفللخال ةهجالو اعاطقنا ابهسفن .

????? ?????????????? ????????????? ???????????

تانايب مادختساب عقومال جراخ نم آنينخت ىلإ رارمتساب آيطايتحا خسُنُتو تانايبال ررّكت اعم لماعتل لالخنم ةيدفلل جمارب نم ةيطايتحالل خسنلل ةيامح عم ،ةلصفنمو ةزيمم دامتعا ماطتنا ابهرا بتخا متيو ،(immutable) رييغتلل لباق ريغ وأ (offline) لصتم ريغل لكشب ةيمهأل ةساردو ،يفيظولاب قاعاتلل ةطخو ،ةيوساخال ئراوطللل ةباجتسا ةطخب ةطخلال ظفتحتو تايحي تارتساو ،لامعأل ريثأتل آل ليحت نمضتتو ،تامدخل ةيمهأ ةيولوأب ةمئاقو ،تانايبال نيرامت رابتخال لمشيو .ةداعتسالل ةدحم آفادهأو ،ءالمعلا راطخإ لمشت لاصتا ةطخو ،ةداعتسالل ةيلعفل ةداعتسالال ىلع تابي ردتو (table-top) ةيرطن ءاكاح .

????????? ?? ?????? ????????????? ???????????

?????????

A.5.29-A.5.30. نيدنبلال ISO/IEC 27001:2022 رايعمو NIST SP 800-34 رايعم عم ةطخلال قفاوت ؛ةيفللخال ةهجالول (RTO) ةداعتسالال تقوو (RPO) ةداعتسالال ةطقن فادهأ Cyber Crucible ددحتو مدع ةيقافتا بجومب نينعجارمل ىلإ ،اهسفن ةطخلال كلذكو ،ةدحمل ةفدهتسمال ميقلال مّدقُتو

يُعرف عوج في أودية النالطقنات اعافد رمتست، أي لحم دُفنت في امحل أل ارظنو. (NDA) ءاشف إ (air-gapped). ءلوزعمل رشنل ائلمم ف وأة فللل ءه اول اعاطقن اءنأ ءءاعس السال تقو ف

?? ????? Cyber Crucible ?????

???????????? ?????????? ???????????

????????????????????

ةصاخلا تاوطخلا وراودألا تانايبلا قارتخالا ةباجتسالا ةقثوم ةيلمع ددحت .معن :**ةجوم ةباج** ، فاشكنال اهضرعت وأ اهقارتخا وأ ةيمحمل تانايبلا ةقرس يف هابتشا ةلاح يأل ةباجتسالا ب ةبسنلاب دقعل بجومب راطخإلل مزلُم ينمز راطإ ديدحت نكمي و .ءالمعل راطخإ كلذ يف امب ميظنتلل نيعضاخل ءالمعلل

????? ???????????

تامولعلم نم أة فيظو اهبقارت يتلا ةيلخادلا تاونقلا ربع أروف هب هبتشم ثداح ي نع غلبُي ثداوحلل ةباجتسالا قيرف لكشُي و ،رثأتمل دروملا إلوصولا لأُي ،ثداحلا ىلع فترعتلا دنعو يناربيسلا نيأتملا ةيطغت مهرفُوت ،نويئانج ءاربخو نوققحم موقي .ةيذيفنتلا ةرادإلا ةسائر ب فارطألا و ،ةينعلم تانايبلا و ،ثداحلا عوقو ةي فيك ديدحت ب Cyber Crucible - ةصاخلا ينقتلا و تالاصتالا ةرادإ و ةينوناقلا ةرادإلا عم نواعتلاب لاصتا ةطخ عضُوت و .يرنجل ببسلا و ،ةرثأتملا كلذ يف امب — ءاضتقالا بسح ةرثأتملا فارطألا و روهمجلال و ني فظوملا راطخإل ةيرشبلا دراوملا و ،ثداحلا دعب امل ةعجارم اهبقعي — لدابت لكشب اهيلع قفتم ةانق ربع ءالمعل راطخإ

???????????? ??????????? ?????????? ??????????

يوتسم ةيقافتا يف ةروشنملا ةروطخلا تاويوتسمل أقفو ءالمعل سمت يتلا ثداوحلا عباتُت ثداحلا و قارتخالا ب راطخإلل ينمز راطإب أي دقاعت مازتلالا نكمي و ،(SEV4 إىل SEV1 نم) ةمدخل ميظنتلل نيعضاخل ءالمعل ةبسنلاب

????????? ?? ?????? ??????????? ??????????

????? ??????????

ISO/IEC رايعم نم A.5.24-A.5.26 ني دنبلال عم و NIST SP 800-61 رايعم عم ةيلعمل هذه قفاوتت ثداوحلل ةباجتسالا لماكلا ءارجلإل مَّدقُي و .دامتعا ةداهش يأل ىلع لوصلحلا ىغْدُي الو . 27001:2022 (NDA) حاصفإ مدع ةيقافتا بجومب ني عجارُملا إىل تاقارتخالا ب راطخإلا و

??? ????? Cyber Crucible ???? ?????????? ????????

ىلع لمعي ةياهنل طاقنل لقتسم ةياقو لح وه هسفن جتنملا .نيتقي رطب :ةجوم ةباح!
يوتسم ىلع اهب ةصاخلا ةياهنل طاقن ي Cyber Crucible مكحتت امك ،(kernel) ةاونل يوتسم
ةيجمربلل ةرفيشلا ءانب ىلع ناتقي رطلل زكترتو .يمسرر جمانرب بجومب ةسدنهلل ةكرشل
أيلخاد ةيخالص ىلعأل

????? ?????? ?????????? ?????????? ??????????

نقحو ،(fileless) ةركاذلا ىلع ةمئاقلا تامجهللو ،ةيدفلل تايجمرب دض ةلقتسم ةياقو جتنملا رفوي
نوكيل دصق نع مُمُص دقو .ةاونل يوتسم ىلع اهقي بطت متيو ،(process injection) تاي لمعل
كلت فاطتخا وأ قارتخاب نومجاهملا ماق اذا ثيح ،ليغشتلا ماظن تابتكم نع ألصفنم
ةباجتسالل اوشكلا نألو .غالبلل اوزيفنتلاو لمعلل ي جتنملا رمتسي ،ةركاذلا ي تابتكملا
نع لوزعم رشن ي وأ ةرادلل ةيفلل ةهجالو عاطقنا ءانثأ ةيامحل رمتست ،أيلحم ناڊفني
دصق نع (air-gapped) ةكبشلل

????? ?????? ?????????? ?????????? ??????????

جماربو ،راعشتسالل ةزهجأو ،ةاونل يوتسم ىلع تاللدتساللو ،فاشتكالل تاي مزراوخ ميمصت متي
تاودأ وأ ةقووم ريغ ةيجراخ تابتكم ي أجمانربل ي جَمُدت الو ؛أيلخاد اهيلع ظافحللو ليغشتلا
ةلسلس رطاخم نم ةلماك ةئف لازت ،ةصاخ ةيكللم وه ةيخالص ىلعأل نوكمل نألو .ةيفخ غببت
Windows ةاون ليغشت جمارب عيمج نم ققحتل متيو .اهترادإ درجم نم ألدب ةيجراخل ديروتلا
Windows (WHCP) ةزهجأ عم قفاوتلل Microsoft جمانرب بجومب اهعيقوتو

????? ?????? ?????????? ?????????? ??????????

صحفللو ةيامحل للغشُتو ،نمآل نيوكتلل ةدمتعمل اساسأل طوطخ ةراڊمل ةياهنل طاقن عبتت
عملل احو وه امك ةلومحمللو ةلازالل ةلباقلا طئاسولا ىلع طباضلل سفن قُبُطُتو ،ةياهنل طاقنل
تايجمربلل تيبثت عضيوي .اهب حرصملا ريغ طئاسولا ماخستسا ديقت عم ،ةبائلا طئاسولا
رارمتساب ةياهنل طاقن تَدْحُتو ،ةياهنل طاقن ىلع ةنكاسلا تانايبلل رَفْشُتو ،ةدحم ةسايسل
تاتيدحتلا ةرادإ جمانرب نمض

(CIS Critical Controls) تدرت إلإ نم أ زكرم ل ءرل ة ن م ألأ طباوض لا عم ة ي اهللا طاقن طبابوض قفاوت
و لعل لوصلال عؤي الو . NIST SP 800-53 (SI-3, CM-2, MP-7) راي عمل اعمو (8 راصلإ، Security Controls,
بجوم ب ني عارم لل عم اءلال الءال وني وكتلل ري اعم مءقؤؤ . اءامعا ءاهاش أ
(NDA). ااصفإ مءع ة يقافات

???? ???? ???? ???? ???? ???? ???? ???? ???? ?

لمشت — تامولعمل انم اتاسايس نم ةلماك ةومجمب Cyber Crucible ظفتحت : **ةرصتخم ةباج** ا ، ثراوكلا نم يفاعتلاو ، تاريخيتلا ةراڭو ، ريفشتلاو ، ةقداصملاو لوصولو ، لوبقملا مادختسالا ، رفوتت . كلذ ريغو ، اهفالاتو اتانايابلاب ظافتحالو ، اتاقرتخالو ثداوحلل ةباجتسالاو (NDA) . ءاشف ا مدع ةيقافتا بجومب نييعجارملا اهل ةمعادل ةلدالو اتاسايسلا

????? ????????? ??????????

دُعْبُ نَعْلُوصُولُو قَدَاصُمْلُو لُوصُولُو؛ تَايِقَالْخَالُو لُوبَقْمَلْ مَادْخَسَالُو تَاسَايَسَالُو عَوْمَجْم لَمَشْت
؛ عِيَفِرْطَلْ زَهْجَالُو مَدَاوْخَلْ نَمُو؛ تَارِييْغَتَلْ عَادَاوْ نَمَالْ رِيوْطَتَلُو؛ حِيَتَا فَمَلْ عِيَامْ حَوْرِي فَشْتَلُو
طَا فَتْحَالُو؛ تَا قَارْتِخَالُو ثَدَاوْحَلْ قَبَا جَسَالُو؛ لَامْعَالْ عِيَارْمَتْسَاو ثَرَاوْكَ لْ نَمْ يَفَاعَتَلُو
جَمَارْبَلْ تَا صَخْلَمْبْ طَفْتَحْ يَمَكْ. يَنُورْتَكْلِلْ دِيرْبَلْ بَطَا فَتْحَالُو اَهْفَالْتَاو تَانَايِبْلْ ب
(SDLC) تَايَجْمَرْبَلْ رِيوْطَتْ عَايَحْ عُرُودْ يَغَانْطَصَالُو اَكْذَلْ عَمْكَوْ حَوْقِي قِدْتَلُو لَاتْ ثَمَالْ بَعْلَعْتَمَلْ
تَاسَايَسَالُو عَمْبَنْجْ يَلْ اَبَنْجْ.

?????? ? ???? ?

،ةيعجرم ل رطألأ عم هقفاوت ىدمو جمانرب لك ئدابمو دوجو ةماعلا ةفرعملا ةدعاق تاحفص فصت
،ةدحمل تاسايسلا قئاثو امأ لعلل عوسم ىلع ماعلا عضولا مهف نم عجارملا نكمتي ثحب
ةلدأو ،(يفاعتلا فادهأو تانايبلاب طافتحالا لواذج لثم) ةقيقدلا ماقرألأو ،ةئيهتلا ريعامو
ةمزح بناج ىلإ ،(NDA) ةلدابتم ءاشفإ مدع ةيقافتا بجومب اهميدقت متيو ةيرسيهف ،قيقدتلا
ةزهاجلا ني دروملا نم بجاو لا ققحتلا

????? ?????

لإلحاقكم بعملة الدال، عزه الجال ني درومال عمزح، نام ألال تاسايس عمومجم بلط ني عجارم لل نكمي
 ةلدابتم لءاشف إلال مدع ةيقافاتا رفوت. **dpo@cybercrucible.com** ني نورتك لإلال دي رب
 ب لاطم ي أمؤت ال. أقبس م ةيراس ةيقافاتا دوحو مدع ل احي في Cyber Crucible. ب ةصاخ ل ةيسايق ل
 لك طبابوض ل و ةينبل معدت فيك حضور قئاثولاف؛ لمع راطل ي ألال دامتعا ةءاش ل ل لوصح ل باب
 تامازت لال هءه نم مازت لال.