

???? ????? Cyber Crucible

EDR لولحبةً نراقم - نورتشمل اهرطي يتل ميققتل او نراقم الة لئسأ ىلع ةرشابم تاباجإ يطايتحال خسنل ىلع ةمئاقلا ةداعتسال او DLP و تاسوري فل ةحفاكم و MDR و XDR

- [Agentic AI لثم رخآ ءيش هنأ مأ MDR و XDR و EDR وه Cyber Crucible له](#)
- [يدل ىرخأل نامأل تامولعم تاحول لثم ةبقارم ةادأ هذه له](#)
- [ىرخأ ةينمأ تاجتنم عم Cyber Crucible شىاعتى له](#)
- [Cyber Crucible عم ضراعتى يدل نامأل تاجتنم دحأ ناك اذا ثدحي اذام](#)
- [MDR و XDR و EDR نع Cyber Crucible فلتخت فيك](#)
- [هعم بنج ىلإ أبنج لمعى مأ، ىب صاخلا EDR ل ح ل حم Cyber Crucible لحي له](#)
- [تاسوري ف داضم جم انرب وه Cyber Crucible له](#)
- [ةيدفلل جمارب عم لماعتلل دادرئسال او يطايتحال خسنل ىفكي ال اذامل](#)
- [أحل اصأ عفد ةيدفلل جمارب ريفشت حيتافم طاقئتلا دعي مل اذامل](#)
- [ةثيدحل تامجهل امامأ "ىباحسلل تانايبلل عماج" ىلع ةمئاقلا نامأل تاودأ زجعت اذامل](#)
- [ىتمطنأ ءاطبإ ىل Cyber Crucible ىدؤى له](#)

?? Cyber Crucible ?? EDR ??
XDR ?? MDR? ?? ??? ??? ???
??? Agentic AI?

لاؤسلا وه ءئفل نع لؤسل نكل ،XDR و EDR نم لك نم رصانع ىلع يوتحي :**ررصخملا ءباجلا** لمعي Cyber Crucible في ءباجتسالا قطنم .

نأل — موجهلا ءطحل في طقف كانه ءحاتملا تامولعمل ماخذتساب ءياهنلا ءطقن ىلع لماكلاب .ءشاهلاو (latency) ءباجتسالا نمز :نيتلتاق فعض يتطقن لخدُت دُعُب نع ليلحتلا مداوخ

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

- **EDR: هتفص**ب ةصاخلا (telemetry) دُعُب نع سايقل تانايب مدختسي EDR ناك اذا **هتفص**ب EDR. دُعُب Cyber Crucible في ةيلال ةباجتسالا نإف ، تارارقل داختال ةياهنلا ةطقنب تامولعمل مادختساب ، ةيناثلا نم ءانجأ في زازتبالا كولس ىلع اهتضب ق مكحُت يهف طقف ةيلحمل.
- **XDR: هتفص**ب ليمعلااب صاخ زاهج ءاوس) تانايب ةدعاق ىلإ اُضيأ سايقل تانايب لسرُت **XDR: هتفص**ب ، ةيلخلال تاديدهتلا ىلع لمعلاو ، تاديدهتلا دي صو ، ليلحتلاو طبرل صا رُغأل (يزكرم وأ قبطني كلذ نإف ، XDR -ل قيقوستلا في رعتلل آق فوو . ينقتلا قيقدتلا تاي لمعو هيلع .

(edge computing) هي فئة من الحوسبة موزعة، "تأخذ البيانات إلى أقرب مكان ممكن من حيثها". هذا يعني أن الحوسبة تتم في الطرف (edge) بدلاً من مركز البيانات (cloud). هذا يقلل من زمن الانتقال (latency) ويزيد من كفاءة الشبكة.

????? ???? ??????? ?? ????? ?????? —
??? ???????????? (Latency)

ةيبسوح ةوق رفوي اذهو .ةديعب مداوخ ىلإ ةيليلحتلا ةبسوحلا ةوق لقن XDR في "X" فرح لثم في
:ةنمزللا ءهه لوح مهيلالسا نومجاهملا ىنب دقو ،أ تقو فلل ءهه كل

- **سبق** انه ن ع ع ج ا ر ت ل ا ل ن ك م ي ا ل ي ت ل ا ت ا ع ا ر ج ا ل ا ل م ت ك ت ث ي ح ب ت ا م ج ه ل ا ع ي ر س ت ر ج : **ع ر س ل ا** ة ر ي غ ص ل ا ر ص ا ن ع ل ا ع م ص ا خ ح و ص و ب ك ل ذ ر ه ط ي و . ة ب ا ح ت س ا ل ا م ل ل ي ل ح ت ل ا م د ا خ ن ك م ت ي ن ا ر و ر م ل ا ت ا م ل ك ل ث م ة ل ا ل ع ل ا ة م ي ق ل ا ت ا ذ
- **ي ل ا ل ق ت ن ت م ث** ، ر ط ت ن ت ، ا د ح ا و ا ج ا م ا ن ر ب ص ح ف ت ة ي ا ه ن ل ا ة ط ق ن ت ا و ا د ا م د ي د ع ل ا : **ي ز ا و ت ل ا** ل و ص و ل ا ي ا — د ح ا و ت ق و ي ف ز ا ز ت ب ا ج م ا ر ب ة د ع ل ي غ ش ت ب ن و م ج ا ه م ل ا م و ق ي ا م ن ي ب . ي ل ا ت ل ا

500. نم آلدب يزاولاب فلم 5000 ىلإ

- **Cyber Crucible** تظحال .دحاوَنآ ي ف ةددعتم ةزهجأ ربع زازتبالا ذيفنت يرحي :**غيزوتلا** آزاهج 75 ربع آجامانرب 50 ةادألا هجاوت اهدنع .هسفن تقولا ي ف آزاهج 75 وحن ىلع كلذ عوقو .اهصحف بجي آجامانرب 3750 ي —
- **مكحت ةدحو ني مجاهملا ضعب لّغشي (Commander processes) ةدئاقلا تاي لمعلا** :اهفاقيا متي زازتبا ةادأ ي لّغشت أروف ديعت ةي لمح

آي لعف أدب دق موجهلا نوكتي ىتح ،اهتعي بطب ،رظتنت ةباجتسال او فشكلا تايحي تارتسا ةنيعم ةي مك نوكت نأ دعب مهفاقيا نم آلدب بابلا دنك كونبلا صوصل فاقيا وه قدألا هي بشتلا ةنخل نم تجرخ دق لاومألا نم

————
????? ???? ??????? ?? ????? ??????
????????

وحنلا ىلع لمعت يكل دُعْب نع ليلحت مداوخ ىلإ لوصول ىلإ جاتحت XDR و EDR لولح نم 80% وحن يباحسلا "غامدلا" اذه نود ةلاعف ريغ نوكت داكتو ،لثمألا

،ةي امحلا رادج دعاوق ريغيغت لّ فاك لوصو ىلع لوصحلا درجم ب ف :ةرشابم رمألا اذه نومجاهملا لغتسي اهتردق ةادألا دقف تف ،اهب ةصاخلا ليلحتلا مداوخ ىلإ لوصول نم ةياهنلا ةطقن ةادأ عنم مهنكمي ريغ اهنكل — ليغشتلا ديغو ،ةتّبثمو ،ةلّغتسُم ريغ ةادألا ىقبتو .ةباجتسال او ليلحتلا ىلع ل.لماك هبش لكشب ةلاعف

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

ي ف رارمتسال لباق ريغ أرم ةباحسلا ىلع دامتعالا نالعجي ةشاشهلاو ةباجتسال نمز نأل آرطن اهتاليلحت دمتعت ةباجتساو فشك ةردق Cyber Crucible تركتبا ،زازتبالا دض عافدلا يدصتلا ثدحي .**موجهلا تقو ةياهنلا ةطقن ىلع ةحاتملا تامولعمل ىلع طقف** ةيكلولسلا جرحلا راسملا نمض ةباحسلاب آباي او آباهذ لاصتا ي نود ،ةيناث ي لل م 200 نم لقأ ي ف ةداع آي لمح

ي — ةي امحلا سيلو قي قحتلا معدت يهف تانايبلا ةدعاق ىلإ قفدتت يتلا سايقلا تانايب ام ةهجاو حيتت امك — ينقتلا قي قدتلا تاي لمعو ،ةيلخادلا تاديدهتلا نع فشكلاو ،تاديدهتلا ديص اذه .RPA تاودأ او ،SOAR تاودأ او ،ةحوتفملا XDR تاصنم ةيذغت (API) ةحوتفم تاي بطت ةجمررب .ذيفنتلا ديقي موجه نيبو كن ي ب فقي ام آدب سيل هنكل ،مّيق لمعلا

نوكرتو، ةنورتكلإل Cyber Crucible ةبواب ىلإ لوخدلا لىجستب نوموقي ال ةطاسبب مهف...
ب.سح فاهل لمعب موقت ةتمتأل

???????????? +
????????

ةينغ ةعومجم [تاي لمعل اءاشن](#) او ،دامتعالا تانايب مادختسا ةبقارمو ،[تاي لمعل نقح](#) تاي ناكم رفوت .تاديدهتلا دي ص ءارجل ،ءاونلا ءوتسم ىلع ةيكلولس تاليلحت ربع اهطاقتلا متي ،تانايبلا نم

،(رورملا تاملك ،زورملا) دامتعالا تانايب ةقرس و ،تانايبلا ةقرس ءدب درجم ةيلال ءي امحل ادب .عئار دروم اذهف - كلذ ادع ام لكل ةبسنلابو .ةيدفل جمارب ريفشت و

يلوؤسم لبق نم لقالا ىلع) ةراؤملا ريغ دغب نع ةرادإلا تاودأ يه نالا ىتح آعويش جئاتنلا رثكأ يف تاودالا هذه يدؤت ،معن .اهتبيثتب نومدختسمل موقبي تالا (ني ليلال تامولعمل ءينقت نيلعافلا دحأ مدختسي ام دنع يا) زارتبالا دض ءيئاقلت ءي امح ليعفت ىلإ نايحالا ضعب ضغب ،أقبسم كتئي ب نع ديزملا ءفرعم آمائاد لصفالا نم نكل ،(ةراؤملا ريغ RMM ءادأ نيثيبخال كلذ نع رظنلا

تائي ب يف ،ني مءاملا لبق نم ءمادختسا اندءاش تامءهلا نم عونل عيرس ويديف عطقم كيلى ...ءامسالا ركذبحن ال نحن) ءالمءلاب ءصاخلا EDR لولح زواجتل حاجنب مدختسا دقو ،ءدعتم ءالمع .(تاسسؤم ءبرأ يف تاجتنم 3 كانه تناك

[rr-com-dll.mp4](#)

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

Cyber Crucible. تانايبلا مادختسالالا تالاح نم ناعون كانه

يف قيقتلا نم ،تامولعمل ءينقت يفظوم دحأ و ،ءكرشلا يف نمألا دارفأ دحأ نكم تي نأ وه لوألا تيبيثتب نوموقي ام ءداع نيذلا ،ءالمءال ضعب ةبسنلاب .جماربالا دحأ قيلعتل ريزجالا ببسلا دادعإلا ىلإ نوجاتحي دج نيفظوم دوجو دنع الإ رخأ ءرم لوخدلا ليجستب نوموقي ال مء ،انجمانرب ءالا ءولا ءرادإ ءففص ءانثتساب Cyber Crucible ءئاظو نم ءفيظو يا أقلطم اومدختسي مل

طيسبو لهس رمأ وه - [يريزجالا ببسلا لىلحت](#) ىلع فرعتلا ىلع مهءدعاسم اندعسي .ني نقتلا ءبشو ني نقتلا ني مدختسملل

يتلا DFIR تاكرش مه ثداحلا دعب ءيئانجالا ليلحتلا نومدختسي نيذلا ءالمءال نم يئانثلا عونلا ني مأتالا ءكرش بلط ىلع ءانب آنايحو ،ءالمءال دحأ ىدل ءلكشم يف قيقتلا لال ءب ناعتسؤي آمائاد انكمي ال ،عبطلاب) .ءلكشملا عوقو دعب Cyber Crucible تيبيثتب متي ثيح ،يناربيسلا

ملاعلا يف ةكرش لك تناكل الو...كلذ يف ةديدشلا انتبغر مغر، مجاهملا لبق دجاوتلا
(!يضاملا نم آئيش زازتبالا حبصألو، انمدختست

ءدب وأ تيبتتلا وبعص اننأل سيل. "ةيوضوف" وه زازتبا موجه دعب رشنلا ةيلمعل فصو لصفأ
،مظنلا ربعةءا اوكرحت دق نومجاهملا نوكي، ةلاحلا كلت يفف! امامت سكعلال يلعل لب. ةيماحلا
يهتنيو. ةركاذلا يف نولمعيو، Active Directory، ءكبشلا ءزهجأو، ليغشلا ةمظنأ يف اولغلغتو
رمألا. ةرطيسلا ءداعتسا ىتح نومجاهملا لواحي آنايحاو، ءددعتم ءزهجأ يف تايلمعلال قيللعتب رملألا
ةياهنلا يف نسحتتل هجاتحت كنكل، ةيادبلا يف ءوسلاب رعشت كللعي ءاود لوانتب هبشأ

نم "ديزمل" عم يفطاع لكشب آنايحا ديدش طغض تحت لعللاب مه نيذلا ءالمعلال لعافت
ببس لوح ةيعوتلا نم ريثكللا كانهو. مهتميزهو نيماجاهملا لاصئتسا آريخأ متي امنيب، جيجضلا
ديعتست، ةياهنلا يف نكل. نيماجاهملا مهيدل ةمئاقلا نمألا تاعومجم فاشتكا مدعة يففك وأ
80-90% لا نيب نم حبصت نلو. تامولعملال ةينقتل ةيتحتلا اهتنيب ىلعل ةرطيسلا ةكرشلا
".كارتشالاب زازتبالا داصتقا" هي مسن اميف، نيماع وأ ماع دعب اهزازتبا داغي يتلا تاكرشلا نم

Cyber لأكريش نوكي امأبالاغو، (MSSP) ءراؤم ةينمأ تامدخ دوزم وه انيدل ءالمعلال نم ثلاثلا عونلا
اهب ققح يتلا ةقيرطلا ءفرعم ىلإ نوجاتحي. Cyber Crucible. نم ةيلآ ةيماحل بيحتسي،
و HIPAA ل لاثلثمالا ريراقت نأ وه راسلا ربخالو. ةينمأ تارغت يأ قالاغو، تقؤم مدق ئطوم مجاهملا
ءباجتسالال ءعرسل ارظن، ةيرسلل آمودعم وأ آفيفط آقرخ رهطأ امءا ءداعتاب لطلتملا نم اهريغ
امم، "هنع غالبالل عيش دجوي ال" هنأب راؤملا نمألا تامدخ دوزم غلبُي، نايلألا نم ريثك يفو. ةيلآلا
مجملا ءانثتساب، آنسح. ةينعملال فارطألا عيجم دعسُي

?? ????? Cyber Crucible ??

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

!معن

صاخال Magic Quadrant ىلع دوجوم ينمأ دّروم لك عم هشياعتو Cyber Crucible رشن آيلاح متي
ةكرشب Gartner.

ةيارد ىلع نوكتل هتادادعإ طبضب موقيو ىرخألانامأل تاودأ ةطشنأ آيئاقلت انجمانرب فشتكي
اهب.

[ةفرعلملا ةدعاق ىف ةلاقملا هذه](#) ىلع عالطالال ىجرّي،ردان لم تحم ضرعات ثودح لاج ي ف

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

Gartner Magic Quadrant ريراقت انمدختسا اذا ،يسيئر نامأ عئاب لك عم آيلاح Cyber Crucible شيعاتي
ةعانصل داورل سايقمك Quadrant.

امب ،ىرخألا جماربلا نم قوثوم لكشب ةنورم رثكأ Cyber Crucible ـب صاخلا ةياهنلا ةطقن جمارب
ىرخألا نامألا جمارب كلمت ال ام ةداع ،كلذ ىلإ ةفاضلإاب .ىرخألا ةياهنلا ةطقن نامأ تاودأ كلذ ي
Cyber Crucible جماربلا ةلماك ةيؤر ىتح .

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

??????:

عئابلا ةادأ ربخت مل .كلذ اهنكمي ال . Cyber Crucible نم عزج ليغشت فاقيا ىرخألا ةادألا لواحت
وأ ىرخألا تاودألا لطعتت . "قلعأ نل ،ال" ، (Cyber Crucible ي) ىرخألا ةادألا لوقت امندنن ثدحي ام رخآلا
أطخ ةلاح ي ف لخدت .

??????? Cyber Crucible:

ةمئاقلا ىلإ Cyber Crucible جمارب ةفاضل وه لوألا .نيقش تاذ ةباجتسالان نوكت نأ نكمي
امم ، Cyber Crucible جماربلا ىرخألا ةادألا لهاجت ىلإ كلذ يدؤيس .رخآلا عئابلا ىدل ءاضيبلا
أطخ ةلاح ي ف لوخدلا نم ىرخألا ةادألا عنمي (لمأن).

نوكرتي ني رخآلا ني عئابلا نأ انملعت دقل .لح داجيإل انقيرفل كورتم رملأاف ،كلذ حجني مل اذا
مهبناج نم للخ حالصلإ (أدبأ وأ رهشأ ةدع) ريثكب أطبأ لكشب .

ىرخألا ةادألا لعجت ةئيپ ءاشنإب أساساً انمق ،كلذ اهيف ثدحي تلتا ةليلقلا تارملا يفو ،آيخيرات
وأ راغصلا كتلائع دارفأ دحلأ حامسلا وه يننقتلا ريغ هيبشتلا نوكتي دق .تجحن اهنأ دقتعت
امادل ةبعل ي ف كيلىل زوفلاب كللفط .

- Cyber Crucible لى طعت ىلع ،عورشم ريغ وأ عورشم لكشب ءاوس ،ةردقلا ىرخأ ةادأ ىدل تناك اذإ
كلذ لعف آضيأ ناصرقلل نكميف .

نع رظنلا ضغب ،لاكشألا نم لكش ي أب عجارت دق Cyber Crucible جم انرب نأ تطحال وأ تهبتشا اذإ
آروف انب لاصتالا ىجري ،كلذ يف ببست يذلا جم انربلا

فورظلا كلت يف فعضلل لاجم ال .ةيويحلا كئانايو بزتملا نيب ةدماص ةادأ رخآ ةداع نحن

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

EDR ?XDR ?MDR?

موجهه البقارت يهف :ةباجتساو فشك تاودأ MDR وXDR و EDR تاودأ دُعُت :ةرصتخمملا ةباجإلا Cyber أم. هل عف بجي ام نأشب رارقلا ذاختال ةبباجس ةمدخ وأ ناسنإ ىلع دمتعتو ،أهيبنت رصُتو ةيلمعلل فقتو ةياهنلا ةطقن ىلع لقتسم لكشب رارقلا ذختت :ةيئاقو ةادأ يهف Cyber Crucible .ررض يأ ثودح لبق ،ةينات يللم 200 نم لقاأ يف ةراضلا

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

	EDR / XDR / MDR	Cyber Crucible
ةباجتساللا نمز	تاعاس ىلإ قئاقد نم	ةينات يللم 200 نم لقاأ
فشكلل ةقيرط	ةيخيراتلا تانايبلاو عيقاوتلا	تاعيقوت نود ،ةكولسلل ةينلا
مويلا ةلوهجم تارغثلا ةيطغت (Zero-day)	ةيئزج	ريغ تاديدهتلل أصيصخ ةممصم ةفورعلملا
ناسنإلا ىلع دامتعالا	ةينمأ تايلمع زكارمو نوللحم — ةلاع (SOC)	لمالكلا بةلقتسم — مودعم
تارارقلا ذاختا ناكم	ةبباجس تاليلحت	(kernel) ةاونلا لخاد ،أيلحم

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

تامجهلا امأ .مايأ وأ تاعاس ىدم ىلع فشكتت تامجهلا هي ف تناك رصعل فشكلل تاودأ تممُص تانايبلا جارختسا دعب أقيقد أهيبنت رصُت تيلا ةادلأف نواثي ف لمكتف مويلا ةيلآلا اهتعنم اهنأ ال ،ةراسخلل تَقُثو دق نوكت

ينعي لب .نامهم نارمأ قيقحتلاو ةيئانجلل تاقيقحتلاف — ةميقلا مبدع فشكلل نأ ينعي ال اذه ةلآلا ةعرسب ثدحي موجه فاقيا هنكمي ال هذحو فشكلل نأ

ديحوت اهضعب راتخي ،اهيدل فاشتكال اتاودأ لعافت مدع راركت ىدم قرفلا طحالت نأ درجمب EDR لح لادبتسا مك نكمي — ةضورفم تالمكت الو ،نيعم درومب يمازل طابترا دجوي ال .اتاودأ لبولطم لدئاعل ققحي ال امثيح قافنلإ ضفخ ةطاسبب وأ ،لماك لاب مكب صاخلا

?? Cyber Crucible ?? ?????

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

هأنأب ةفورعملا تافللملا ديدحت ىلع تاسوريفلا ةحفاكم جمارب دمتعت .ال :**ةرصتخملا ةباجإ**إلا — قلاطإلا ىلع عيقاوت ي أمدختسي الف Cyber Crucible أم (signatures). عيقاوتلا مادختساب ةراض كلذ ي ف امب ،راضلا كولسلل فقويو ،أيلعف ليغشتلا دي قجم انربلا هب موقي ام مّيقي لب .لبق نم اهتيؤر دحلأ قبسي مل يتلا تاديدهتلا

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

ي ف جذومنلا اذه لشفيو .هليلحت ام صخشل قبس موجه ىوس فص ي نأ عيقوتلل نكمي ال :
نيتعئاش نيتلاح

- اهل عيقوت يأ دعب دجوي ال ثيح ، **(Zero-day) رفس مويلا تامجه** .
 - عيقوت عم هتقباطم نكمي فلم دجوي ال ثيح ، **(Fileless) ةيفلملا ريغ تامجهلا** .
- امم ،تاديدهتلا تامولعم رداصم نم أرم تسم أثيديحت عيقاوتلا ىلع مئاقلا فشكلا بلطتي امك .مجاهملا نع ةوطخ ةرأتم أمئاد لظت كتيامح نأ ينعي

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

تافللملا ىلإ لوصولو ،تايلمعلا طاشنو ،ةركاذلا طاشن — كولسلل ةجذمنب Cyber Crucible موقي ىلع رفس مويلا تامجه فاقيا عاطتسا ببسلا اذهلو .يلعفلا تقولا ي ف ةينلا مّيقيو — ةباجتسالا وأ أنلعل اهنع غالبلاب رخآ دوزم يأ مايق نم أموي 90 ىلإ لصي ام لبقة الماعلا تاكباش اهل .

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

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

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

يهو — ةيدفلل جمارب موجه نم طقف ةريخألا ةلحرملل ةيطايتحالل خسنلل جلاعت :**ةزوم ةباح!**
دامتعالل تانايب اوقرس دق نومجاهملا نوكتي ،ريفشتلل هيف أدبي يذلل تقوللا لولحبو .ريفشتلل
اهنكل ؛كتافل مديغت ةيطايتحالل خسنلل نم ةداعتسالل نإ .لعفللاب جراخلل ىللإ كتانايب اولقنو
مجاهملا ةزوح في لعفللاب تحبصأ يتلل تانايبلل لايح أئيش لعفلل

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

لحارم ثالثب يجذوملل قارتخالل رمي :

1. **مماطنلل ىللإ لوصولل دامتعالل تانايب قارتخا متي — ةيوهلا ةقرس** .
2. **ةساسح تانايبو ءالمعلل تالجسو ةيركفلل ةيكللملل لقن متي — تانايبلل ةقرس** .
ةسسؤملا جراخ ىللإ ىرخأ
3. **ةيدفب ةبللاطملاو تافللملل لفق متي — ريفشتلل** .

قرخ نوكتي ،تقوللا كلذل لولحبو .ةثلاثلل ةلحرملل في اللإ دادرئسالل تايحي تارتسلا لخدتلل
لعفللاب اعقو دق ةيلغيغشتلل ةرطيسلل نادقفو ةيرسلل

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

تاداريإلا لب — اهسفن ةيدفلل يه ةيدفلل جمارب نع ةمجانلل لامعألا رطاخم ربكأ نوكت الل ام ةداع
قارتخالل عنم نإ .كلذل ةحيثن ةعمسللاب قحلي يذلل ررضلاو ،دمألا ليوط عاطقنا ببسب ةدوقفملا
هنمآلدب سيلو ،دادرئسالل طيطختلل لبقةنملا يئأي نأ بجي اذهلو ،امهيلك يمحلي للوالا

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

جمارب بنجنت. 2021 ماع ذنم آي نقت أقو وثوم هونوك نع حي تافم لاطاقتل فقتو: **ةزجوم ةباح!**
نكمي حي تافم دجوت ال كلذلو، لي غشتل لاطنل ةسياسي قلا ريفشتل تابتكم ةثي دحل ةي دفل
اهقي بطت رذعتي ام آبل اغ، حي تافم لىل لوصحل دن ي تحو — اهضارغا ةي عافد ةادل

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

- نمّ الل دب ةثي بخلل ةي جمربل لخال ةرشابم ريفشتل دوك جمّدي: **ةصصخم تابتكم**
لخال لمالك لاب مدختسّو حي تافم لادّو ثي حب، لي غشتل لاطن تابتكم ةاعدتسا
تاءاعدتسالا بقاتر يتل تاودال ةي ررم ريغ اهل عجي ام وهو — هسفن مجاهم لةي لمع
ةسياسي قلا.
- لك عم فلتخي سياسي ريغ آري فشت تالالسل اضعب مدختست: **ةديرف تاق يبطت**
اهسفن ةي مزراوخل نال، هقي بطت نكمي ال هطاقتل متي يذل حاتفم لى تح. ذي فنن
أصي صخم ممصم.
- نع آي رذج فلتخم موهفم لىل ي نبّو: **ةق فدتم ل تارفي شل (Streaming ciphers)**
AES. حي تافم لاطاقتل دض ةطاسبب ةنصحم يهو، AES.

م، اهل عارغا ةارب لىل تلصحو حي تافم لاطاقتل ةي نقت لصالل ي Cyber Crucible تروط
لىل انلقتنا. 2021 ماع BSides Pittsburgh رمتؤم ي اهدودح رهظأ يذل ريفشتل لي لحتل تمّدق
كلذ تبلطت ةلدال نال كلذ دعب ام.

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

ةدحاو لشف ةطقن قلخي امم — آي زكرم ريفشتل حي تافم نيزخت حي تافم لاطاقتل بلطتي
ءاعدتسا ةركذم ربع اهيلي لوصولل ربحّو نأ ةيموكح ةهجل نكمي امك. ةيلاع ةميقي اذ أفدهو
لىل ةفاضل تانايبال ةدايس لىل أميسج أرطخ لثم ي اذهو. مكملع نود، يموق نم باطخ وأ ةي رس
آل اعاف دعي مل أعافد هونوك.

????? ????? ?????? ???????
????????? ??? "????? ??????????
?????????" ????? ??????????
????????????

نم ليئض ردق ب موق ي في فخ ةياهن ةطقن ليمع وه يباحسلا تانايبلا عماج :**ةرحوم ةباح**إ
اهتجلاعمل ةباحس ةصنم ىلإ ماخلا ةيعبتتلا تانايبلا لاسرإب يفتكيو ،يحملال ليحتلا
ىلع دمتعي ليمعلا نأ امك ،يلاآل موجهلا هايإ كحنمي ال أريخأت فيضت هذه بايإلاو باهذلا ةلحر
،مويلا نومجاهملا اهقرتخي يتلا اهتاذ ليغشتلا ماظن تانوكم .

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

ىلإ ةباحسلا ىلإ ةيعبتتلا تانايبلا لاسرإ يدا .ةفلكمو ةبعص (kernel) ةاونلا ىوتسم ةسدنه
تانايبلا نيزخت نم حابرأ قيقتو ،صرأ ةياهن طاقن تايجمر ب ءان ب نم نيعئابلا نيكمت
،ريوطتلا ليهستل جذومنلا اذه مُمص . "يباحسلا يعانطصالا اكدلا" تاردقل جيورتلاو ،يباحسلا
عافدللا .

????? ??????

1. نكمي ال .ةيناثلا نم ءازجأ يف ةيلاآل "عيرسلا فطخلا" تامجه لمتكت .**أدج ءيطب** 1.
بسانملا تقولا يف ةباحتسا رادصإ ةباحسلا تاليلحتلل .
2. ماظن تابتكم ىلع دمتعت ءالمعلا هذه نأل أرطن .**ةيمهأ رثكألا ةطحللا يف ىمعأ** 2.
تابتكملا كلت قرئخي يذلا مجاهملا إف ،تانايبلا عمجتو لمعتل ةيلصألا ليغشتلا
ةحول — ءيشيأ نع غلبُي نأ نود لمعلا يف ليمعلا رمتسي .ليمعلا تاكسإ هنكمي
،تانايبلا بّرسُت امنيب ماري ام ىلع ءيش لك نأ رهطُت تامولعم .

ةلحر دجوت ال كلذلو ،ةصاخلا اهتارارق ذختو ةاونلا لخاد آيلحم تانايبلا Cyber Crucible جلاعت
أقرتخم نوكي دق ليغشت ماظن ىلع دامتعا الو ةباحسلا ىلإ بايإو باهذ

?? ???? Cyber Crucible ???

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

ةينبل او ،لقأ وأ 1% يلاوح يجذومنل (CPU) جلاعمل مادختسا غلبي .ال :ةرصتخمل ةباجإلأ
يأ — ةياهنل طاقن ءالمع ؤطابت تالاح مطعم يف ببستتي يذل بولسألأ آدمع بنجتت ةيرامعمل
Windows. ماظن تابتكم لخاد (hooks) "تافاطخ" جاردإ

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

????????

ريبك لكشب ةنّسُخْمل ماظنل تابتكم لخاد "تافاطخ" جاردإ ةميدقل نامألأ تاودأ موقت
ةادأ موقت امदनعو .ليغشتلأ ءانثأ لّدْغْتل أدبأ تابتكملا هذه مّمصُت مل .ئيسلأ كولسلأ ةبقارمل
ماظنلأ ءادأ يف أريبك أروهت ةجيتنلأ نوكت ،هسفن تقولأ يف اهب بعالتلاب مجاهمو نامأ

موقيو ؤطابتلأ ىلع نامألأ ءادأ مدختسملأ مولتي :هب ؤبنتلأ نكمي كلذ عبتتي يذلأ طمنلأ
ىلع أمصخ نأ كُردي نأ نود ،ربتخملأ يف ةلكشملا جاتنإ ءداعإ ءوزملا عيطتسي الو .اهتلازإب
فاعضإ لالخنم — آدمع كلذ لالغتسا نومجاهملا مّلعت دقو .ماظنلأ ببعالتتي (root) رذجلأ ىوتسم
ةصاخلا مهتاعافد لي طعتب ايأحضللأ موقي نأ ىلإ ءادألأ

??? ?????

تافاطخ جاردإ نمّالذب (kernel) ءاونلأ لخاد ءلقتسم ةيعرف ةمطنأ لالخنم Cyber Crucible لمعي
ىلع — مجاهملا عم الو — ليغشتلأ ماظن عم سفانتي ال كلذبو ،ةشهلا Windows تانوكم يف
ةشهلا ءرفيشللأ تاراسم سفن