Cyber Security Analyst / Engineer

Kernellix Company Limited သည် ၂၀၁၄ခုနှစ်တွင် စတင်တည်ထောင်ခဲ့သော ၂ နှစ်သက်တမ်းရှိ ရန်ကုန်အခြေစိုက် cyber security အဖွဲ့အစည်းတစ်ခု ဖြစ်ပါသည်။ စတင်တည်ထောင် ချိန်မှစ၍ Kernellix သည် ပြည်တွင်းပြည်ပ ဘဏ်များ၊ ငွေပေးချေမှုလုပ်ငန်းများ၊ ICT နည်းပညာအဖွဲ့အစည်းများ နှင့် e-commerce လုပ်ငန်းများ အစရှိသည့် လုပ်ငန်းအဖွဲ့အစည်းများကို မသမာသူများ၏ cyber တိုက်ခိုက်မှုများ၏ အန္တရာယ်လျော့ပါးစေရန် cyber security ဝန်ဆောင်မှုနှင့် ဖြေရှင်းချက် များကို အကောင်ထည်ဖော် ဆောင်ရွက်ပေးလျက်ရှိပါသည်။

Kernellix သည် သင့်တင့်လျောက်ပတ်သော နည်းပညာ၊ နောက်ဆုံးပေါ် နည်းစနစ်များကို အချိန်နှင့်မပြတ် လေ့လာအသုံးချ၍ ပြည်တွင်းအခြေစိုက် ကမ္ဘာ့အဆင့်မှီ cyber security ဝန်ဆောင်မှုနှင့် ဖြေရှင်းချက် များ ကို အကောင်အထည်ဖော် ဆောင်ရွက်လျက်ရှိပါသည်။

တက်ကြွမှုရှိပြီး ရိုးသားကြိုးစားသော အဖွဲ့အစည်းတွင် ပါဝင်၍ cyber security နှင့် ပတ်သက်သော ပညာရပ်များကို လေ့လာသင်ယူ အသုံးချရင်း လုပ်ဖော်ကိုင်ဖက်များနှင့်အတူ အဖွဲ့အစည်း၊ လုပ်ငန်းကဏ္ဍ နှင့် ပညာရပ်တိုးတက်အောင် ဆောင်ရွက်လိုပါက အောက်ပါ အချက်အလက်များကို ဖတ်ကြားပြီး Kernellix တွင် အလုပ်လျောက်ထားနိုင်ပါသည်။

လျောက်ထားရန်

၁။ သုံးမျက်နှာထက်မပိုသော CV ကို PDF Format ဖြင့် careers@kernellix.com သို့ပို့ပေးရန်။

၂။ CV တွင်အနည်းဆုံး အမည်၊ မွေးသက္ကရာဇ် (လနှင့်ရက်မလို) ၊ ဆက်သွယ်ရန် email နှင့် ဖုန်းနံပါတ်တို့ ပါဝင်ရမည်။

၃။ ပမာဏအဆင့် ရွေးခြယ်ခံရပါက လူတွေ့စစ်ဆေးရန် ဆက်သွယ်ပါမည်။

လိုအပ်ချက် (မရှိမဖြစ်)

၁။ ရိုးသားဖြောင့်မတ်သူ ဖြစ်ရမည်။

၂။ လူပုဂ္ဂိုလ် အဖွဲ့အစည်းများ၏ အတွင်းရေး (Privacy) ကို အသိအမှတ်ပြု နားလည် လေးစားသူ ဖြစ်ရမည်။

၃။ အကျွမ်းတဝင်မဟုတ်သော ဘာသာရပ်နှင့် အကြောင်းအရာများကို နားလည်တတ်ကျွမ်း လိုသော ဆန္ဒပြင်းပြသူ ဖြစ်ရမည်။

၄။ မသိကျွမ်းသော နည်းပညာကိုကိုင်တွယ်၍ အလုပ်ပြီးမြောက်အောင် လုပ်ကိုင်ဆောင်ရွက်နိုင်သော စိတ်ဓာတ်၊ သတ္တိနှင့် စွမ်းအားရှိရမည်။

၅။ GNU Linux / Unix distribution တခုခုကို ကျွမ်းကျင်စွာ အသုံးပြုနိုင်ရမည်။

၆။ Programming ၏အခြေခံအုတ်မြစ်ကို နားလည်၍ C, C++, Bash Shell, Java, JavaScript, Python, Ruby အစရှိသည့် programming language တခုခုဖြင့် နိစ္စဒူဝ ကိစ္စများကို automate ပြုလုပ်နိုင်ရမည်။

၇။ Networking အခြေခံအုတ်မြစ်ခိုင်မာ၍ TCP/IP, HTTP, SSH အစရှိသော protocol များကို နားလည်ရမည်။

၈။ Open source tool, framework များနှင့် နားလည်ရင်းနှီးမှုရှိပြီး ပြင်ဆင်အသုံးချနိုင်ရမည်။

၉။ အဖွဲ့အစည်းတွင် အနည်းဆုံး ၂၄လ တာဝန်ထမ်းဆောင်လိုသူ ဖြစ်ရမည်။

လိုအပ်ချက် (အနည်းဆုံး ၅ခု)

၁။ Android နှင့် iOS mobile application များကို စ၊ လယ်၊ ဆုံး ရေးသားဖန်တီးနိုင်ရမည်။

၂။ Mobile application များ၏ အခြေခံလုံခြုံရေးသဘောတရားကို နားလည်ရမည်။

၃။ SQL query များကို ကျွမ်းကျင်စွာ ရေးသားနိုင်ရမည်။

၄။ Web application တခုကို စ၊ လယ်၊ ဆုံး ရေးသားဖန်တီးနိုင်ရမည်။

၅။ Web application များ၏ အခြေခံလုံခြုံရေးသဘောတရားကို နားလည်ရမည်။

၆။ Network, application နှင့် အခြား ICT system များ၏ လုံခြုံရေး အားနည်းချက်များကို သုံးချ၍ အသုံးပြုသူနှင့် အဖွဲ့အစည်း ဆုံးရှုံးနစ်နာအောင် လုပ်ဆောင်ချက်များကို လက်တွေ့ ပြသနိုင်စွမ်း ရှိရမည်။

၇။ GNU Linux, Unix, Windows အစရှိသော Operating System များကို administrator အဆင့်တတ်ကျွမ်း၍ လုံခြုံရေးအခြေခံကိုနားလည်ရမည်။

၈။ GNU Linux, Windows Server များကို လုံခြုံအောင် ကာကွယ်သောနည်းစနစ်များကို နားလည်တတ်ကျွမ်းရမည်။

၉။ Firewall, IDS/IPS, SIEM အစရှိသော security appliance နှင့် solution များ၏ အခြေခံကို နားလည်တတ်ကျွမ်းရမည်။

၁၀။ Open source IDS/IPS framework များကို နားလည်တတ်ကျွမ်း အသုံးချတတ်ရမည်။

၁၁။ Digital forensics tool, platform များ၏အခြေခံကိုနားလည်တတ်ကျွမ်းရမည်။

၁၂။ Open source security solution များကိုအခြေခံ၍ plug-in များ၊ module များကို ရေးသားနိုင်ရမည်။

၁၃။ တက္ကသိုလ်ဝင်တန်း အောင်မြင်ပြီးသူ ဖြစ်ရမည်။

တာဝန်

၁။ Network, server, web application, mobile application အစရှိသော ICT system များ၏ လုံခြုံရေးကို လေ့လာသုံးသပ်ရမည်။

၂။ ICT system များ၏ လုံခြုံရေးအားနည်းချက်များကို အခွင့်ကောင်းယူ၍ အသုံးပြုသူ၊ ဖွဲ့အစည်းနှင့် လူ့အဖွဲ့အစည်း ထိခိုက်နစ်နာအောင်လုပ်ဆောင်မှုကို တာဝန်ရှိရှိ သရုပ်ပြရမည်။

၃။ မသမာသူများ ဖောက်ထွင်းထားသော ICT system များကိုလေ့လာ၍ မသမာသူများ၏ လုပ်ဆောင်ချက်များနှင့် ၎င်းတို့ကြောင့် ဖြစ်ပေါ်လာသော အန္တရာယ်များကို လေ့လာသုံးသပ်ရမည်။

၄။ အဖွဲ့အစည်းများ၏ ICT system များသို့ မသမာသူများ ဝင်ရောက်နောက်ယှက်ခြင်းမှ တားဆီးနိုင်ရန် open source နှင့် commercial product များသုံး၍ cyber security များ တည်ဆောက် အကောင်အထည် ဖော်ရမည်။

၅။ လုပ်ငန်းအတွက် လိုအပ်သော tools, programs နှင့် scripts များ တီထွင်ဖန်တီး ရေးသားရမည်။

၆။ လုပ်ငန်းအတွက် လိုအပ်သော စာရွက်စာတမ်းများ၊ report နှင့် presentation များ ရေးသားတင်ပြရမည်။

၇။ Customer များ၏ လိုအပ်ချက်များကို နားထောင်ဖြည့်ဆည်း ညှိနှိုင်းဆောင်ရွက်ရမည်။

၈။ ရလာဒ်ကိုဦးတည်၍ စီမံကိန်းများကို အရည်အသွေးပြည့် အချိန်မှီ ဆောင်ရွက်ရမည်။

၉။ ပြည်တွင်း၊ ပြည်ပ cyber security ဖြစ်စဉ်များကို အဆက်မပြတ် လေ့လာသုံးသပ်ရမည်။

အလုပ်ချိန်

- တနလ်ာ မှ သောကြာ (မနက် ၉ နာရီ မှ ညနေ ၆ နာရီ)
- အလုပ်လိုအပ်ချက်ရှိသောအခါမှအပ စနေ၊ တနင်္ဂနွေ အလုပ်ဆင်းရန်မလို။