



Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

Kerjaya dalam Keselamatan Siber

Gambaran Keseluruhan

Keselamatan Siber ialah sesuatu yang kita baca di dalam berita hampir setiap hari lebih-lebih lagi organisasi dan agensi kerajaan serata dunia digodam secara berterusan. Justeru, terdapat permintaan yang tinggi untuk mereka yang dilatih dalam bidang keselamatan siber untuk membantu memberikan pertahanan terhadap ancaman ini yang kian membesar. Bahkan terdapat anggaran untuk hampir 3 juta kerja kosong dalam bidang ini di serata dunia. Pernahkah anda mempertimbangkan kerjaya sebagai seorang pakar dalam bidang keselamatan siber? Kerjaya dalam keselamatan siber merupakan kerjaya yang sedang berkembang pesat serta mempunyai bidang yang sangat dinamik dan mempunyai pelbagai bidang pengkhususan yang boleh dipilih, termasuk forensik, keselamatan titik akhir, infrastruktur genting, tindak balas insiden, jaminan pengekodan, serta kesedaran dan latihan. Tambahan pula, kerjaya dalam keselamatan siber membolehkan anda untuk bekerja di mana sahaja di serata dunia dengan faedah menarik dan peluang untuk membuat perubahan yang nyata.

Tetapi Perlukah Saya Mempunyai Ijazah Sains Komputer?

Tidak sama sekali. Sesetengah pakar terbaik dalam bidang keselamatan mempunyai latar belakang bukan teknikal, seperti Bahasa Inggeris, pra-Perubatan atau Sejarah, juga terdapat mekanik, seniman dan suri rumah. Perkara yang paling penting ialah keghairahan untuk belajar – keselamatan siber adalah mempelajari bagaimana sesuatu perkara berfungsi. Apabila anda mempunyai pemahaman mengenai bagaimana teknologi berfungsi, anda boleh menjamin keselamatannya. Perkara yang menarik mengenai keselamatan siber ialah anda boleh mempelajari cara teknologi berfungsi mengikut tahap diri sendiri sambil berada di rumah.

Bagaimana untuk Bermula

Berikut Tidak pasti daripada mana anda patut bermula? Anda boleh mula meneroka sebarang teknologi yang berlainan dan lihat subjek yang menarik minat anda.



Pengekodan: Belajar asas pengaturcaraan, bagus untuk memulakan pembelajaran dengan Python, HTML atau Javascript. Tidak pasti daripada mana anda patut mula belajar? Anda boleh mempertimbangkan laman latihan dalam talian atau dapatkan mana-mana buku pengaturcaraan untuk mereka yang baru belajar.



Sistem: Belajar asas pentadbiran sistem operasi seperti Linux atau Windows. Jika anda berminat belajar dengan lebih mendalam, mulakan dengan Linux. Sekiranya anda dapat mempelajari cara untuk mentadbir sistem Linux menggunakan garis perintah dengan mahir, kemahiran tersebut akan membantu anda dalam sebarang bidang yang anda pilih.



Aplikasi: Belajar cara untuk membuat tatarajah, janaan dan menyenggara aplikasi seperti pelayan web atau pelayan DNS.



Rangkaian: Belajar cara rangkaian berfungsi, termasuk cara komputer dan peranti berkomunikasi dengan menangkap dan menghuraikan trafik rangkaian. Subjek ini boleh menjadi sangat menyeronokkan kerana rumah anda berkemungkinan besar adalah persekitaran rangkaian dengan pelbagai peranti yang saling berhubung.

Cara yang terbaik untuk belajar adalah dengan menyediakan makmal anda sendiri di rumah. Makmal tersebut mudah untuk disediakan kerana anda boleh mencipta beberapa sistem operasi maya pada komputer fizikal yang sama, ataupun anda boleh membuat persediaan menggunakan sumber Cloud seperti Amazon AWS atau Microsoft Azure. Setelah sistem operasi anda tersedia dan berjalan, mulakan interaksi dan anda boleh mengkajinya dengan lebih mendalam. Anda juga boleh membuat pilihan lain iaitu dengan bertemu dan bekerja dengan mereka di dalam keselamatan siber. Hadiri persidangan keselamatan siber tempatan (acapkali digelar sebagai 'con') berdekatan anda. Hampir kesemua bandar utama mengacarakan beberapa acara setiap tahun. Salah satu siri acara keselamatan siber terkenal yang direka untuk membantu orang yang baru bermula dalam bidang keselamatan siber digelar Bsid.es. Bahagian paling sukar adalah untuk mencari acara dan pertemuan pertama. Setelah anda menyertai acara yang pertama, hubungan dan peluang anda dalam keselamatan siber akan berkembang. Cara lain untuk anda mempelajari keselamatan siber ialah melalui video Youtube, forum dalam talian, langganan blog sama ada pakar keselamatan siber atau dengan menyertai acara Capture The Flags (CTF) dalam talian. Akhir sekali, terdapat banyak program yang boleh membantu anda memulakan kerjaya anda, termasuk CyberTalent Immersion Academies, Cyber Aces, dan program Cyber Patriot.

Pada dasarnya, jangan benarkan latar belakang pendidikan anda menjadi penghalang. Tidak kira apa sahaja latarbelakang anda, ianya akan membawa sesuatu yang unik dan istimewa yang sangat diperlukan dalam keselamatan siber. Perkara yang paling penting ialah keghairahan untuk belajar. Apabila anda mula membentuk kemahiran dan mula bertemu mereka yang lain dalam bidang ini, peluang anda untuk bekerja dalam bidang ini akan tiba.

Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: <http://snsk.skmm.gov.my/>.

Editor Jemputan

Heather Mahalik (@heathermahalik) ialah seorang Pengarah, Kejuruteraan Forensik di ManTech CARD dan seorang tenaga Pengajar/Pengarang Kanan untuk kursus Forensik Digital dan Tindak Balas Insiden (DFIR) di SANS. Beliau telah berkecimpung dalam bidang keselamatan siber selama hampir 17 tahun dan sangat menyukai kerja beliau. Beliau menulis dalam blog www.smarterforensics.com.



Sumber

Bsid.es: <http://www.securitybsides.com>
CyberTalent Immersion Academies: <https://www.sans.org/cybertalent/cybersecurity-career/seekers>
Cyber Aces: <https://www.cyberaces.org>
Cyber Patriot: <https://www.uscyberpatriot.org/>
Code Academy: www.codeacademy.com

OUCH! diterbitkan oleh program SANS Security Awareness dan diedarkan di bawah lesen [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). Kebenaran diberikan untuk mengedarkan surat berita ini atau menggunakannya dalam mana mana program kesedaran selagi tiada perubahan dibuat kepada kandungan asal. Untuk edisi lepas atau versi diterjemahkan, lawati www.sans.org/security-awareness/ouch-newsletter. Editor: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Translated by: Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie