nccgroup

Life of a Security Consultant

UT ISSS Security Day

11/5/2021

Making the world safer and more secure

Introductions

Tony Cargile

- Regional Vice President at NCC Group
- UT CS – Class of 2013

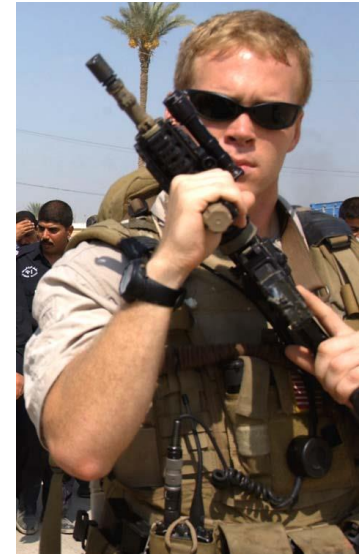## Kevin Chen

- Security Consultant at NCC Group
- UT BBA in Finance – 2015
- UT MS in CS - 2021

nccgroup

Agenda

- Choosing a Career in the Security Industry
- The Security Consultant Job Role
- Security Consultant Working Practices
- Consultancy Office Hierarchy
- Research & Development
- Industry & Community Interaction

Second hit on Google Image Search for 'Security Consultant' ☺

nccgroup

Choosing a Career in the Security Industry

What are my options? So many choices…

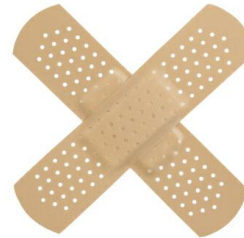nccgroup

Choosing a security career

- **Security Ethics**
  - Responsible Disclosure
  - Full Disclosure

- **Current Industry Debates**
  - Disclosure for Security
  - Selling Weapons

- These concepts may shape your career

nccgroup

Choosing a security career

- **Software Development**
  - Write (more) secure software; write security software
- **Academia**
  - Teach security concepts to others; security research
- **Internal Security**
  - Bug remediation; internal testing; compliance
- **Crime / BlackHat (!)**
  - It's an option – but don't do this! Hacks might be easy – getting away and making money is hard ☺
- **Security Consultant**
  - Penetration testing; red-teaming; exploit dev.; real-world work

nccgroup

The Security Consultant Job Role

Who are these guys?! This and other questions answered…

nccgroup

The Security Consultant Job Role

- In a nutshell - what does a security consultant do?

A Security Consultant provides advice and guidance to clients to help increase the level of security for that client. Typically this involves carrying out security tests against the client's products or assets and making recommendations for how better to secure them from attack. Products or assets could take any form – computer or non-computer based.

Eh?

The Security Consultant Job Role

- Okay, but what types or work do they do?
  - Potentially very diverse – depends on their specialism

  > Penetration testing; security assessment; fuzzing; source code review; wireless security tests; internal network compromises; web application tests; physical security breaches; war dialing; incident response; forensic analysis; build reviews; social engineering; mobile app security; write security tools / software; red-teaming; APT-simulation; IDS/IPS evasion; write reports; provide teaching & training…

- A consultant may do one, more or all of these things!

The Security Consultant Job Role

- Who are your clients? Anyone I've heard of?

- Trusted advisors to over 1,750 clients world wide

nccgroup

The Security Consultant Job Role

- What background does a Security Consultant have?

- We've seen almost any background you can think of
  - Graduates – Bachelors, Masters, Ph.D.
  - No degree – industry experience, or none
  - Not finished high school – 15 years old (long story)
  - Change in Focus – Sysadmin or Developer
  - No IT experience at all – just a creative thinker!
  - Anyone that likes to 'take things apart'

nccgroup

The Security Consultant Job Role

- But what makes a good Security Consultant?

- Definitely a mixture of things –don't have to have it all…
  - Deconstructive Thinking
  - Problem solving & analysis of complex systems
  - Enthusiasm and passion for the work and industry
  - A good balance between software and infrastructure
  - Basic coding skills to write your own tools
  - Good written and speaking skill – explain concepts well

nccgroup

Modes of Working as a Consultant

- Where do I go? What do I do?

- **Remote Working** – carrying out security assessment against client assets across the Internet (servers, web sites, VPN endpoints etc.)

- **Onsite Working** – visiting a client's place of business to carry out work against onsite assets (working directly with client staff)

- **Offline Working** – carrying out work that doesn't require a particular location or target (remote writing, source code review etc.)

- **Team Working** – collaborating with team members on projects and research activities either remotely or office based.

nccgroup

Typical Working Practices

- **Pre-Engagement**
  - Help Account Manager decide on technical scope for engagement
  - Prepare for technical aspects of the engagement
  - Take part in team planning & liaison prior to engagement start

- **Engagement**
  - Carry out testing activities as dictated by scope and team structure
  - Produce written evidence and commentary for client reporting
  - Maintain communication with the client in line with project goals

- **Post Engagement**
  - Provide client with agreed end-of-engagement deliverables
  - Carry out post-engagement clean up, data storage etc.
  - Support report contents with client; re-test; presentation

Consultancy Office Hierarchy

Your subordinates, peers, boss and boss' boss…

nccgroup

Consultant Office Heirarchy

- Consultancy Levels
  1. Associate Security Consultant
  2. Security Consultant
  3. Senior Security Consultant
  4. Principal Consultant
  5. Distinguished Consultant
- Directors and Above
  1. Technical Director
  2. Regional Director
  3. Research Director
  4. Regional Vice President
  5. Senior VP / C-Level
- Technical Areas
  1. Technical Services Consulting (Pentesting)
  2. Cyber Incident Response (Defensive Side)
  3. Specialty Practices (Crypto, Transport, HW)
  4. Risk Management & Governence
  5. Managed Services including Bug Bounty

Making the Wheels Go Round

- Operations + Managers
- Project/Program Managers
- HR / Payroll Administrators
- General Office Administrators
- IT & Technical Support Staff

Paid Interns can also be found in the majority of our offices!

nccgroup

Research & Development
When is a Consultant not a Consultant?

nccgroup

Research & Development

- **Consultancy** – Typically a client paid engagement with the focus on scrutiny and remediation advice for a specific system, application asset etc.

- **Research** – Typically not funded by a client, but instead undertaken by a consultant to further knowledge or capabilities within a certain key area of interest.

> Research projects of specific worth are funded and supported by NCC to achieve certain goals.

nccgroup

Research & Development

- **NCC Supported Research**

  1. Consultants submit research topic requests
  2. Research subjects are selected that have clear benefits
  3. NCC provides scheduled time for the consultant
  4. Monetary budget may be provided for equipment etc.
  5. Research results are compiled into a technical paper
  6. Supporting tools maybe written or exploits etc.
  7. NCC responsible disclosure policy is adhered to at all times
  8. Paper is used to gain access to key industry conferences
  9. Research findings are presented at industry conference
  10. Reputation increases for Researcher and NCC

nccgroup

Industry & Community Interaction

- Active participation in the security industry is actively encouraged! This can take many forms:

  - Attending or speaking at conferences
  - Teaching training courses at public events
  - Participation in regional groups such as OWASP, 2600 etc.
  - Volunteering for charities (linked to the industry or not)
  - Blogging or tool development
  - Continuing relationships with academia

nccgroup

Tony Cargile
Regional Vice President
E: tony.cargile@nccgroup.com

Kevin Chen
Security Consultant
E: kevin.chen@nccgroup.com

W: www.nccgroup.com

- https://www.nccgroup.com/us/about-us/newsroom-and-events/blog/2012/december/so-you-want-to-be-a-security-consultant/
- https://www.nccgroup.com/us/about-us/newsroom-and-events/blog/2017/september/employee-spotlight-tony-principal-security-consultant-ncc-group-north-america/
- https://www.linkedin.com/in/tony-cargile-7073b151/
- https://www.linkedin.com/in/cckevin/

nccgroup