CYBER SECURITY OPERATIONS ON THE FRONT LINES

KARL SCHEUERMAN
MANAGER, CROWDSTRIKE FALCON COMPLETE
KARL SCHEUERMANN
Manager, Falcon Complete

- 14 years in intelligence and information security

Career
- Air Force/Air Nat’l Guard
- PNNL
- CrowdStrike OverWatch and Falcon Complete

LinkedIn:
https://www.linkedin.com/in/karlscheuerman/

Email: karl.scheuerman@crowdstrike.com
AGENDA

- Thanks
- Pillars of defensive cyber operations
- Real world examples
- Career opportunities
**KEY PILLARS TO EFFECTIVE CYBER DEFENSE OPERATIONS**
*(NOT AN EXHAUSTIVE LIST)*

<table>
<thead>
<tr>
<th>Threat detection/prevention</th>
<th>Threat intelligence</th>
<th>Incident response and remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat hunting</td>
<td>Pen testing</td>
<td>Security architecture, engineering support, etc.</td>
</tr>
</tbody>
</table>
KEY COMPONENTS TO EFFECTIVE DEFENSE

- **Threat**: Threat Hunting, EDR, NGAV
- **Defense**: Advanced TTPs, Commodity Malware & Known TTPs, Hidden

2022 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.
Interactive Intrusion Activity Over Time

<table>
<thead>
<tr>
<th>Q1 2020</th>
<th>Q2 2020</th>
<th>Q3 2020</th>
<th>Q4 2020</th>
<th>Q1 2021</th>
<th>Q2 2021</th>
<th>Q3 2021</th>
<th>Q4 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>eCrime</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Targeted</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacktivist</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unattributed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 1.** Quarterly Growth in Interactive Intrusion Campaigns by Threat Type, Q1 2020 to Q4 2021
MALWARE VS. MALWARE-FREE ATTACKS

2021

62% Malware-Free

38% Malware
CROWDSTRIKE INTERNSHIPS

- Expecting ~230 interns globally this year
- Most internships are 12-weeks during the summer
  - Some remote, some in-office
  - Some extend into the school year
  - Many interns eventually become full-time employees
- Internships are paid
  - No relocation or housing allowance
- Qualifications
  - Pursuing Bachelors or higher
  - Returning to school after summer

- More information:
  - University recruiting careers page: https://www.crowdstrike.com/careers/university-interns/
  - Internship experience video: https://www.youtube.com/watch?v=RNvIbiMaBQ
  - Talent community form if you want to stay in the loop for upcoming events and internship openings: https://forms.gle/eYspySfNc5MgNB3XA
  - Point of contact: university.recruiting@crowdstrike.com
W A Air National Guard has 4 cyber units
- 262\textsuperscript{nd} and 143\textsuperscript{rd} COS at JBLM/Camp Murray
- 256\textsuperscript{th} IS and 242\textsuperscript{nd} CBCS at Fairchild AFB

Obligations
- Up to 12-month initial training program (out-of-state)
- 1 weekend per month + ~15 days of annual training per year
- Maintain health and fitness standards

Benefits
- Real-world experience and skills training
- Unparalleled networking for civilian careers
- Health insurance
- Tuition assistance
- Security clearance
- Salary
- Retirement plan (up to 4% match) vested after just 2 years
- Serve your country, state, and communities

If interested, connect with me on LinkedIn and send me a direct message there. Or you can call Sergeant Loren at 509-247-7598 (Tues-Fri, 7am – 4pm).
KARL SCHEUERMAN

- LinkedIn: https://www.linkedin.com/in/karlscheuerman/
- Email: karl.scheuerman@crowdstrike.com
QUESTIONS?