CYBER SECURITY OPERATIONS ON THE FRONT LINES

KARL SCHEUERMAN
MANAGER, CROWDSTRIKE FALCON COMPLETE

KARL SCHEUERMAN

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

CROWDSTRIKE

AGENDA

- Thanks
- Pillars of defensive cyber operations
- Real world examples
- Career opportunities

©2022 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

CROWDSTRIKE

CYBER DEFENSE PILLARS

©2022 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

CROWDSTRIKE

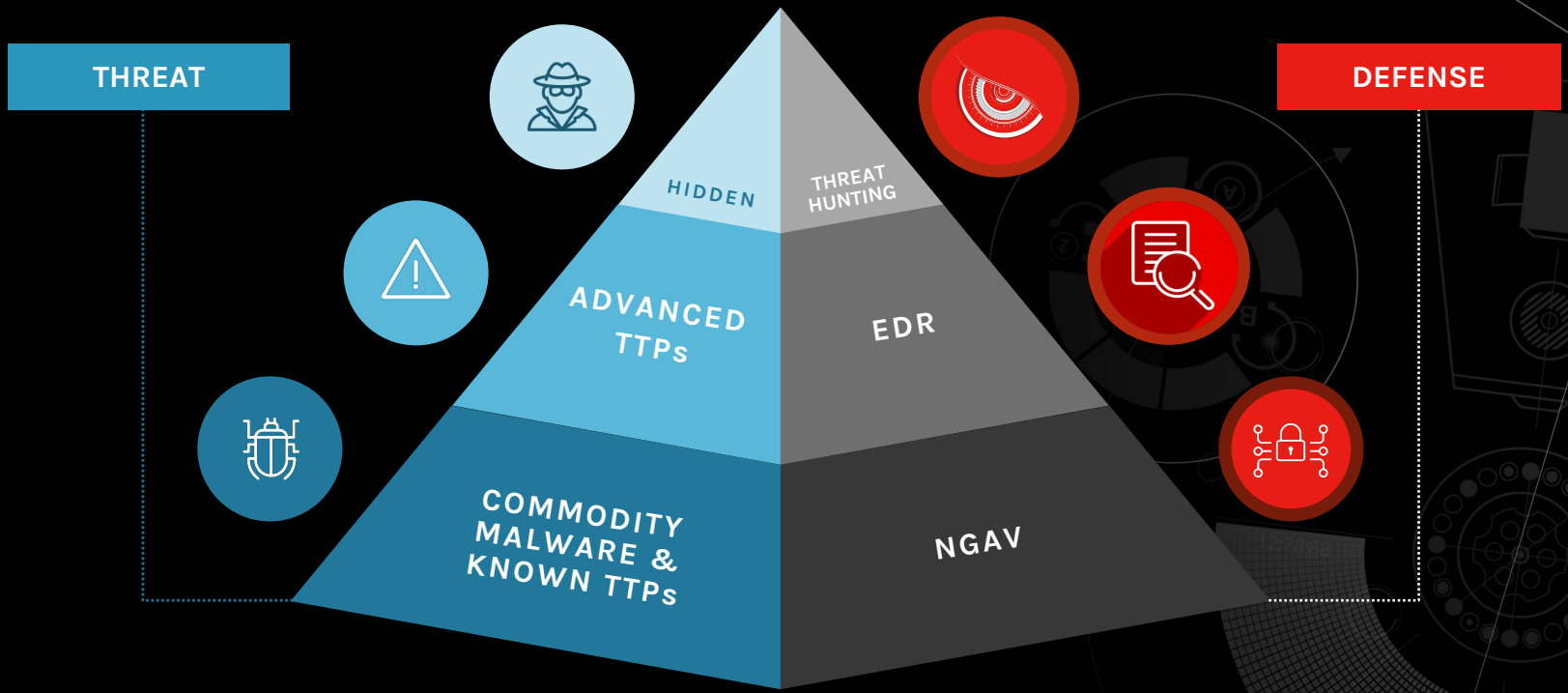
KEY PILLARS TO EFFECTIVE CYBER DEFENSE OPERATIONS
(NOT AN EXHAUSTIVE LIST)

- Threat detection/prevention
- Threat hunting
- Incident response and remediation
- Threat intelligence
- Pen testing
- Security architecture, engineering support, etc.

©2022 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

CROWDSTRIKE

KEY COMPONENTS TO EFFECTIVE DEFENSE



2022 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

CROWDSTRIKE

REAL WORLD EXAMPLES

©2022 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

Interactive Intrusion Activity Over Time

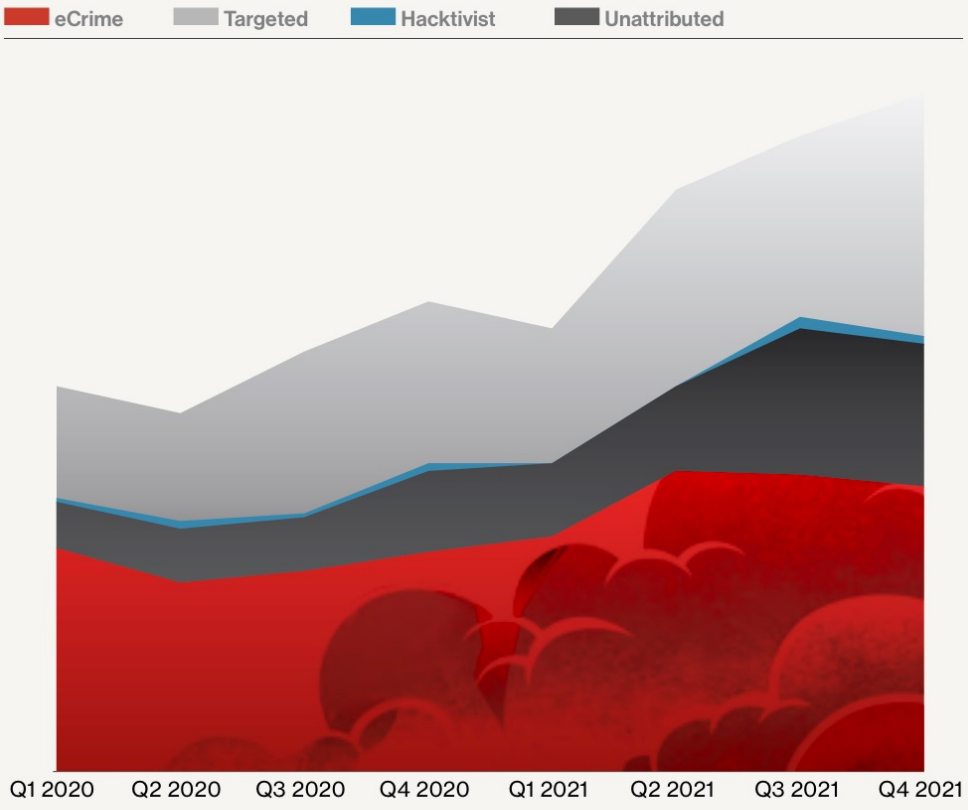
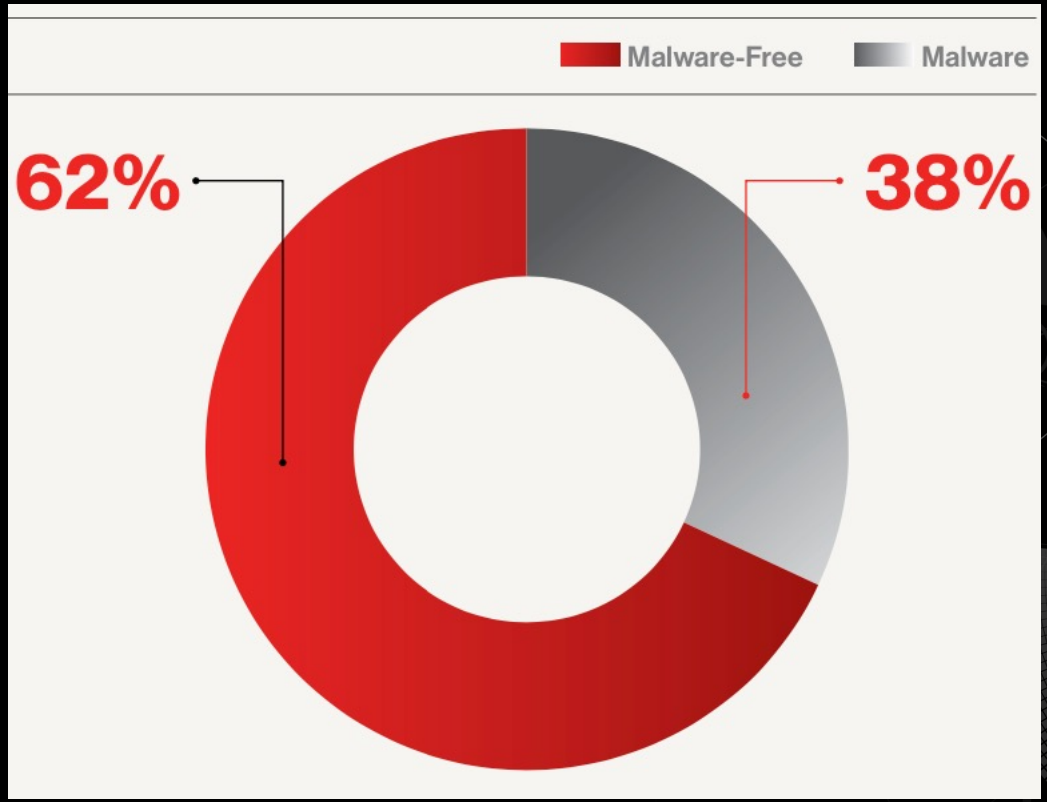


Figure 1. Quarterly Growth in Interactive Intrusion Campaigns by Threat Type, Q1 2020 to Q4 2021

2021 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

MALWARE VS. MALWARE-FREE ATTACKS

2021



2021 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

CROWDSTRIKE

CAREER OPPORTUNITIES

©2022 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

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=RrnVIbiMaBQ
  - 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

2021 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

256TH INTELLIGENCE SQUADRON
WASHINGTON AIR NATIONAL GUARD

- WA Air National Guard has 4 cyber units
  - 262nd and 143rd COS at JBLM/Camp Murray
  - 256th IS and 242nd 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).

CROWDSTRIKE

KARL SCHEUERMAN

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

CROWDSTRIKE

QUESTIONS?

©2022 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.