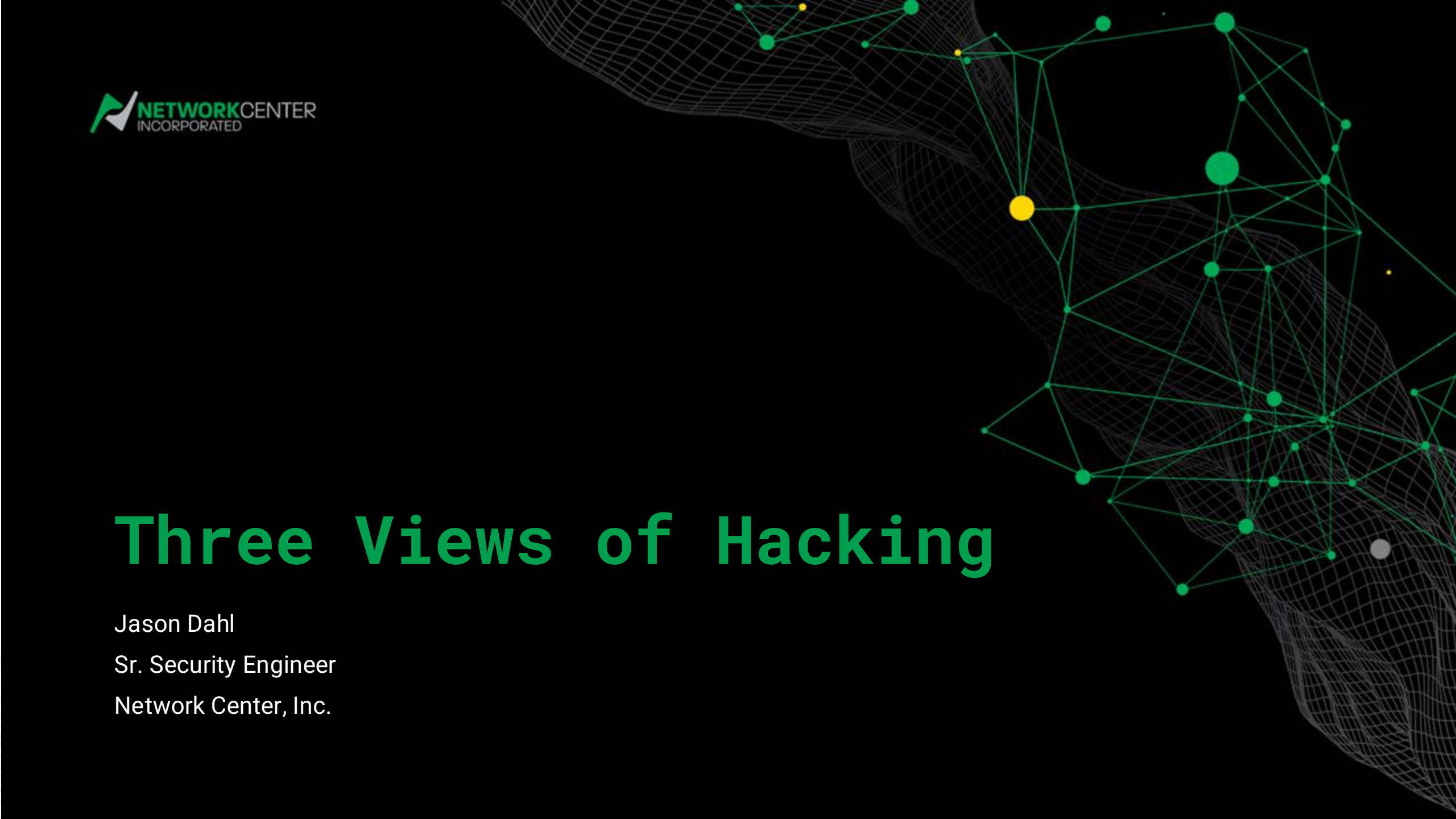
FLEXCARE FACT

If you are a FlexCare Budgeted customer, you now have the option to have up to 4 monthly tickets to help you make sure your AV and patching is at acceptable levels. This can free up some of your time and make sure your devices are protected. Your Account Rep has more details on each of these tickets. Please reach out to him for more information.

NETWORKCENTER
INCORPORATED



Three Views of Hacking

Jason Dahl

Sr. Security Engineer

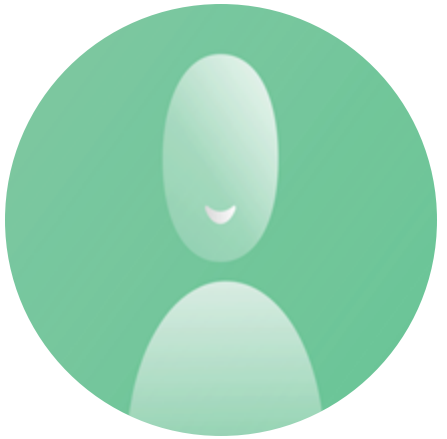
Network Center, Inc.

Disclaimer:

- The use of these tools without the approval of your organization is against the law
- All the tools are being used are in a control environment

The Hacker

- Motivation
  - Money, activism, nation-state or corporate espionage
- Just like your workplace, hackers specialize in certain areas
  - Initial access, malware, etc.



Different Types of Hackers:

White Hat – Researchers, MSPs, assist in securing your network

Grey Hat – Sometimes good, sometimes bad…

Black Hat – Elite for profit individuals, teams, or nation-state

OSINT (How a hacker finds you)

- OSINT or Open-Source Intelligence.
  - What can a Hacker find out about YOU:
    - EVERYTHING – Social Security Number, birthdate, kids' names, pets, old passwords (which you probably still use)
  - The information that is gathered is used to attack you (phishing)
  - Most information is from massive breaches of many different organizations
    - National Public Data Breach (Were you affected? Yes!)
      - https://npdbreach.com – You can see if your personal records were part of the 2.9 billion personal records breach.

The Payload

- Tools are open source and all available on Kali Linux or other hacker forums
- Many open-source programs can assist in creating a payload
  - You do need to have some experience on how to create the payload, so it evades anti-virus or intrusion detection system
- Payloads are customized to you and your organization

Initial Connection

- The first item in the attack is gaining a persistent connection to your O365 or network
- After gaining access, the attacker needs to discover the network, so they will make internal noise
  - If you are running an IDS system, it can detect when a computer is making those requests

The User

- User interaction is needed for **94%** of all attacks
  - Someone must click on something to start the hack
- Delivered via web site, email, or combination of both
- **HELP YOUR USERS**
  - Provide a minimum yearly training
- Invest in intrusion detection system monitoring
  - The faster you are notified, the faster we can stop the attack
- We can not stop every attack, but we can slow down the attacker
  - We can alert when certain events happen

The User

- What should YOU (the user) look for:
  - If something feels off, it probably is: ***trust yourself***
  - Your system becoming sluggish
    - You use your system everyday, you should have an idea of its natural baseline
- Patch **EVERYTHING**
  - It’s difficult to patch/remediate all vulnerabilities but it's a goal to work toward
- Update out-of-date equipment and software
  - If a computer is 7 years old and it seems like it’s still working, it’s not

The Security Engineer

Most important when researching a breach, a compromise, or anything else is:

LOGS • LOGS • LOGS

Logs tell us the whole story, and it's multiple locations we need to see

- Firewall
- Microsoft Sysmon
- IDS Systems
- O365
- Entra ID

Recommendation For ALL

Encrypted Backups	Veeam
Patch Management	Automate, PowerShell, WinGet, Intune
Log Management	Arctic Wolf, OSSIM, QRadar
Host IDS	Cisco AMP, ESET, Defender with MDR
Training	KnowBe4, Arctic Wolf
Implement OS Security Hardening Guidance	Application Control, Firewall, ASLR, Credential Guard
Install and configure Sysmon on all systems	

Success from recommendation

- According to several studies, training can reduce your overall risk from **60%** to as low as **10%**
- ***Early warning systems,*** if monitored and implemented correctly, can reduce your overall risk and reaction time substantially
- Implementing ***security hardening guidance*** will reduce your overall attack surface by 75% or more
  - Firewall
  - Application Control
  - BitLocker
  - Attack Surface Reduction (Works with MS Defender)

NETWORKCENTER INCORPORATED

Thank you!

info@netcenter.net
www.netcenter.net