CENTARIS

Cyber Threat Brief and What You Can Do

CONNECTWISE

Speaker Intro

Jason McNew, CISSP

Principal Solutions Advisor

- Veteran, United States Air Force
- White House Communications Agency, 2003-2014. Camp David Special Missions Command, 2005-2014. Held Presidential Access clearance (Yankee White)
- Founded Stronghold Cyber Security 2017 – NIST & CMMC consulting – 50+ DoD Contractors. Cybersecurity consulting with finance, legal, medical, manufacturing, hospitality, logistics, etc.
- Master of Professional Studies (MPS) – Information Sciences, Cybersecurity & Information Assurance, Penn State
- CISSP

CONNECTWISE™


1998:
Don't get into strangers' cars
Don't meet people from the internet
2017:
Literally summon strangers from the internet to get into their car

What is Cybersecurity?

Cyber security is the body of technologies, processes and practices designed to protect computers, handheld and other Internet connected devices, networks, programs and data from attack, damage, or unauthorized access.

CENTARIS™

What is Cybersecurity?

~~*Cyber security is the body of technologies, processes and practices designed to protect computers, handheld and other Internet connected devices, networks, programs and data from attack, damage, or unauthorized access.*~~

Cyber security is about managing risk. For most businesses, security is a cost center, so security only makes sense to the extent that it reduces business risk or saves money.

CENTARIS™

Agenda

- Top Security Concerns for SMB's
- SIEM & MDR: What You Need to Know
- Benefits from Managed Threat Detection & Response (MDR)
- MDR Solutions – Compliance & Regulations
- Security Risk Assessments

SMB Security Concerns

SMB's & Cybersec

CENTARIS™

SMBs Are Targets

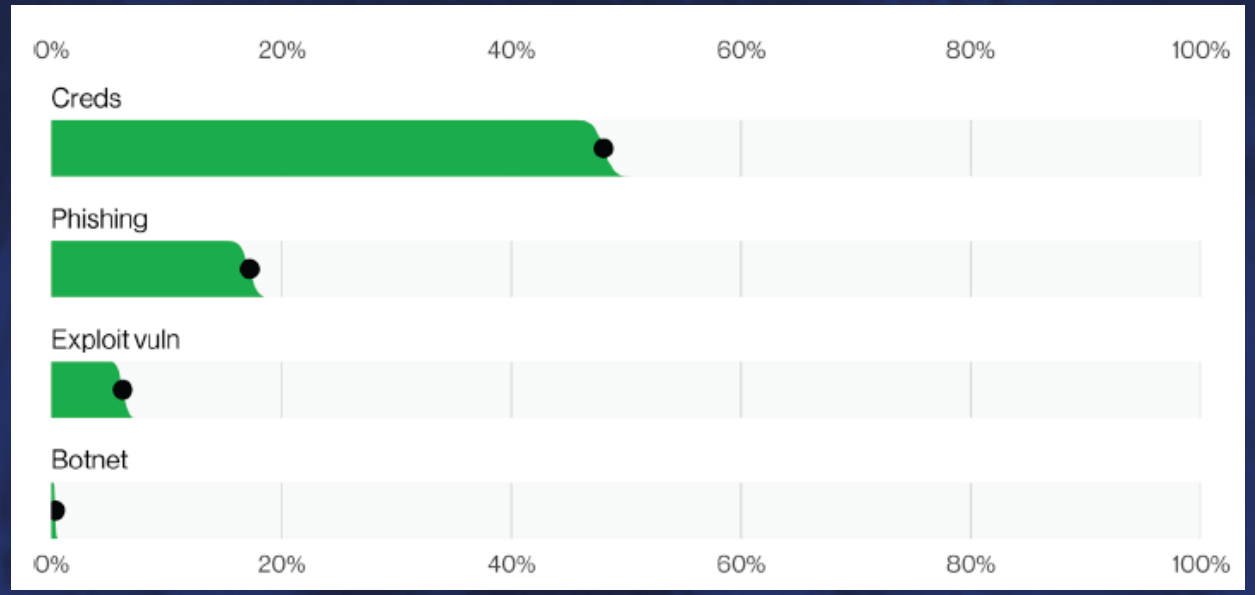
The gap between the number of breaches seen by small and large organizations has become much less pronounced over the past two years.

All organizations are being targeted by financially motivated organized crime actors !!

Source: Verizon 2022 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

CENTARIS™

Verizon 2022 DBIR Report



There are four key paths leading to compromise of your estate:

- Credentials
- Phishing
- Exploit vulnerabilities
- Botnets

No organization is safe without a plan to handle them all.

Source: Verizon 2022 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/dbir/#segment-reports

CENTARIS™

Threat Report Security Concepts

- **Assets** – Has value in a company
- **Threats** – Has potential to damage asset
- **Threat Actors** – Person or organization carrying out a threat
- **Vulnerability** – Openings, or weakness to a system
- **Exploit** – Process of taking advantage of a vulnerability to attack
- **Ransomware as a Service (RaaS)** – A subscription-based model that enables affiliates to use already-developed ransomware tools to execute ransomware attacks

CENTARIS™

2021 Top Threat Actor Profiles

Top 5 groups

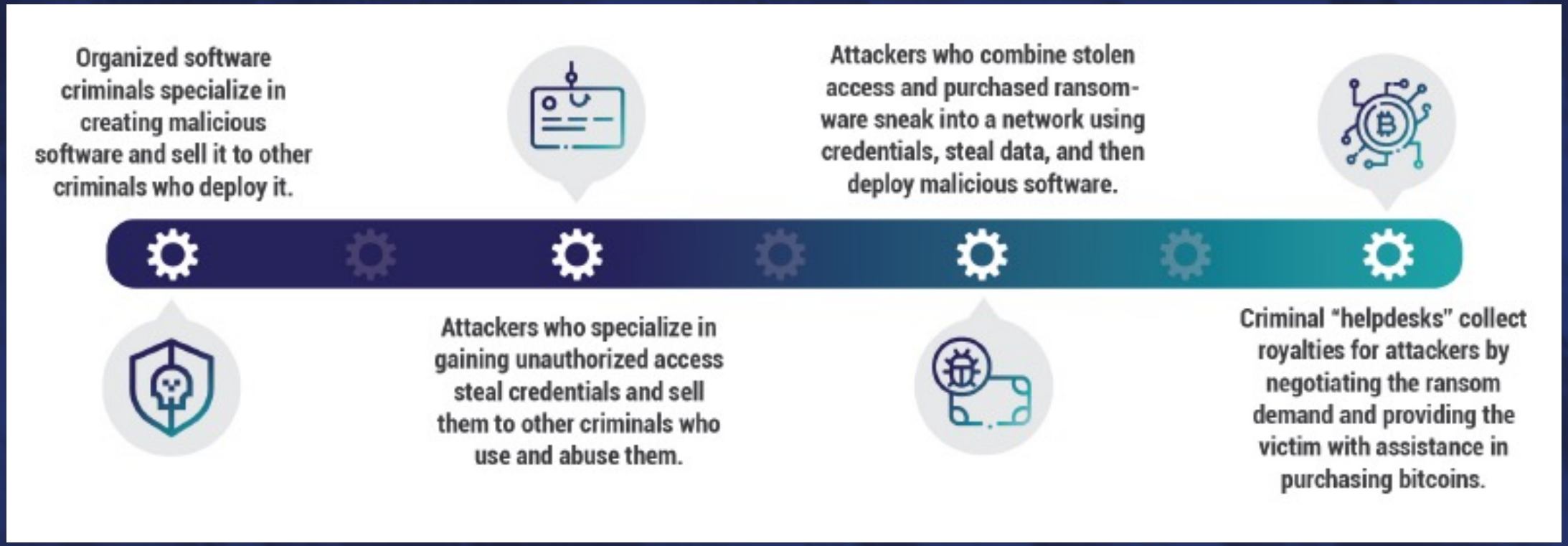
- **LockBit/LuckyDay/LockBit 2.0/ ABCD**
- **Conti**
- **Avaddon**
- **Hive**
- **REvil/Sodin/Sodinokibi**

TTPs shared by all 5 groups:

- Initial Access (TA0001)
  - Phishing (T1566)
- Execution (TA0002)
  - Command and Scripting Interpreter (T1059)
  - Windows Management Instrumentation (T1047)
- Defense Evasion (TA0005)
  - Obfuscated Files or Information (T1027)
- Impact (TA0040)
  - Data Encrypted for Impact (T1486)
  - Inhibit System Recovery (T1490)
  - Service Stop (T1489)

CENTARIS™

Ransomware-as-a-Service:
A production line of organized crime



Source: https://delinea.com/blog/ransomware-as-a-service-new-ransomware-model

Paying Ransom Rarely Works

On average:

- 8% - of affected companies recovered all data after paying a ransom
- 29% - of affected companies recovered no more than half their data after paying a ransom

Sophos – State of Ransomware 2021

More Than Ransom

2020	2021
0.76M	1.85M

Average approximate cost to organizations to rectify the impacts of the most recent ransomware attack

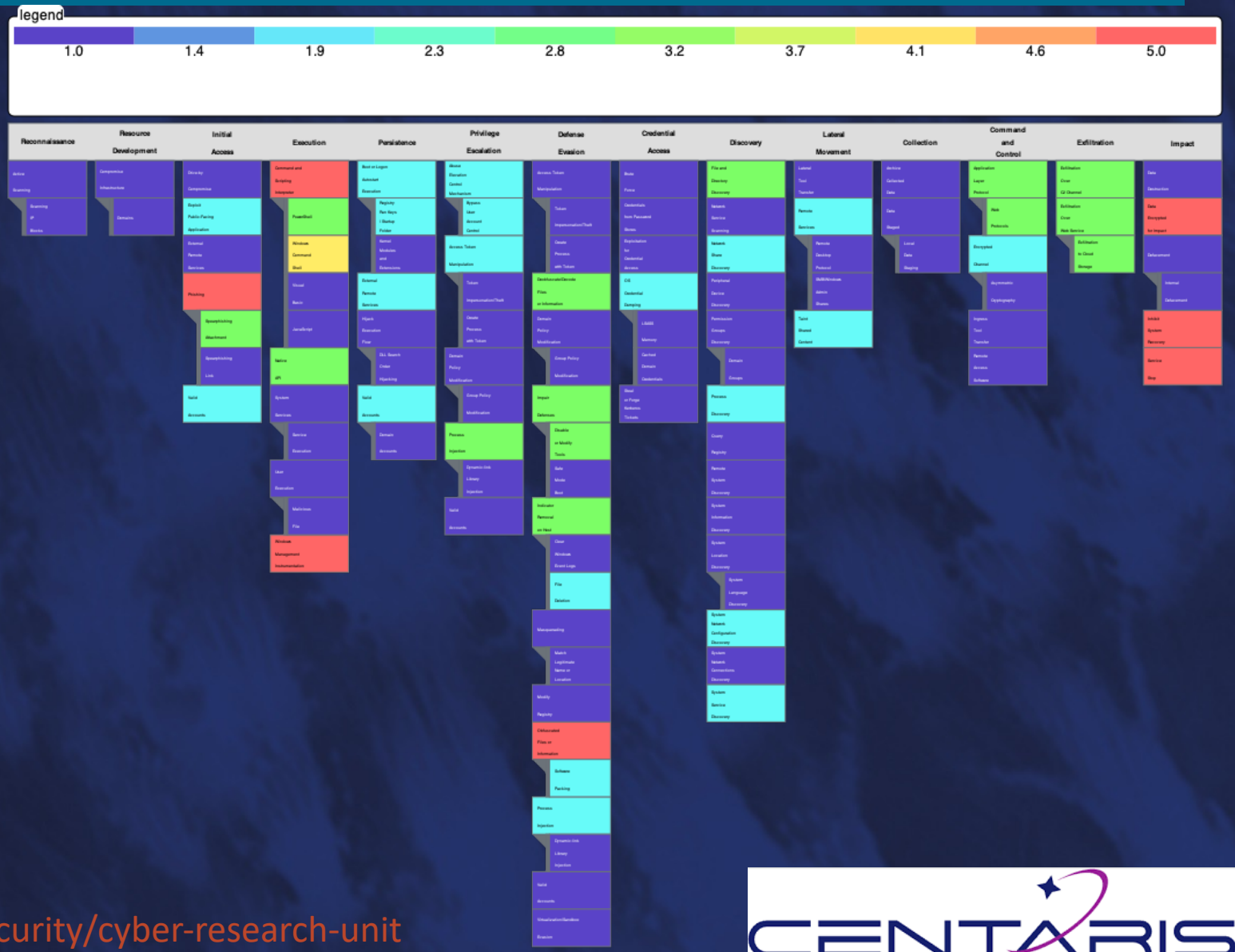
Sophos – State of Ransomware 2021

Everyday Challenges for SMBs

- Cybersecurity confusion (IT challenge vs. Business Challenge)
- Difficult to manage cybersecurity with competing priorities
- Complexity of shifting to a remote workforce
- Poor communications between organizations & their managed IT service providers about cybersecurity needs
- Poor cybersecurity skill sets within the organization
- Ad hoc business continuity & disaster recovery (BCDR) efforts
- Increased costs to respond & recover from an incident

CENTARIS™

2021 Top Threat Actor Profiles



https://www.connectwise.com/cybersecurity/cyber-research-unit

We Are Only Human

A person is involved at the center of most security events

- 82% of breaches result from human elements
- 66% of breaches involve phishing or stolen credentials
- 2.9% of employees may click on phishing emails

SMBs can significantly reduce their attack surface by focusing on controls to mitigate the likelihood of phishing techniques and stolen account credentials

- Adopt email filters and provide user training to combat phishing attacks
- Practice good password hygiene
- Use multi-factor authentication (MFA) everywhere

Source: Verizon 2022 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

CENTARIS™

Threat Landscape for MSPs, TSPs & SMBs

Most data thieves are organized professional criminals deliberately trying to steal information they can turn into financial gain.

- 13% increase in ransomware breaches
- 40% of ransomware incidents involve Desktop sharing software (RDP)
- 35% of ransomware incidents involve the use of email with links to droppers or attachments
- 62% of system intrusion incidents involve threat actors compromising business partners

Source: Verizon 2022 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

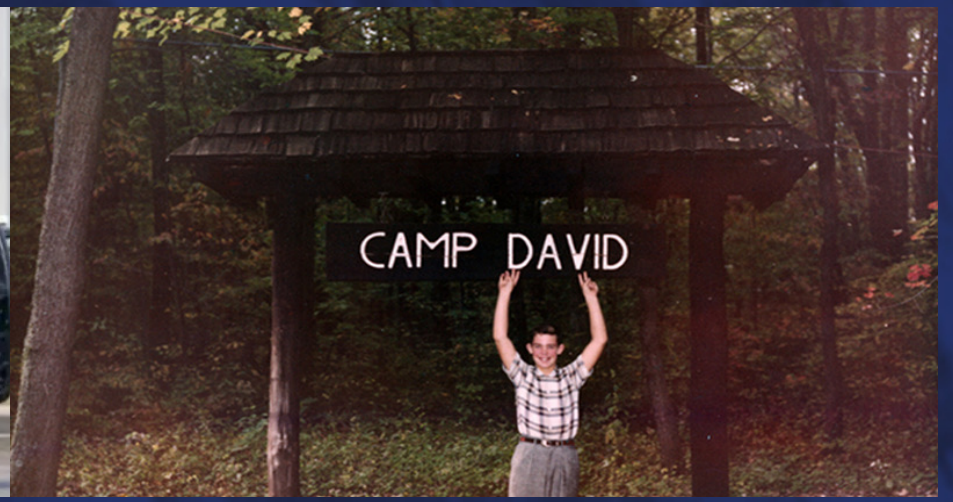
CENTARIS™

Other Considerations to Consider

- Study the NIST Cybersecurity Framework
- Create (and practice) an incident response plan
- Regularly review security procedures
- Keep your software up to date
- Review CISA's Ransomware Notice
- Review the ConnectWise Security Trust and Compliance site

CENTARIS™

Story time!! – Tales from WHCA and Camp David



WHITE HOUSE COMMUNICATIONS AGENCY

SIEM & MDR

Understanding how they work & complement each other

What is a SIEM?

Security Information and Event Management

A SIEM works by collecting log and event data generated by an organization's systems, devices, and applications and brings them into the centralized platform for analysis and reporting.

When the SIEM identifies a threat through a set of predetermined rules, an alert is generated for human review.

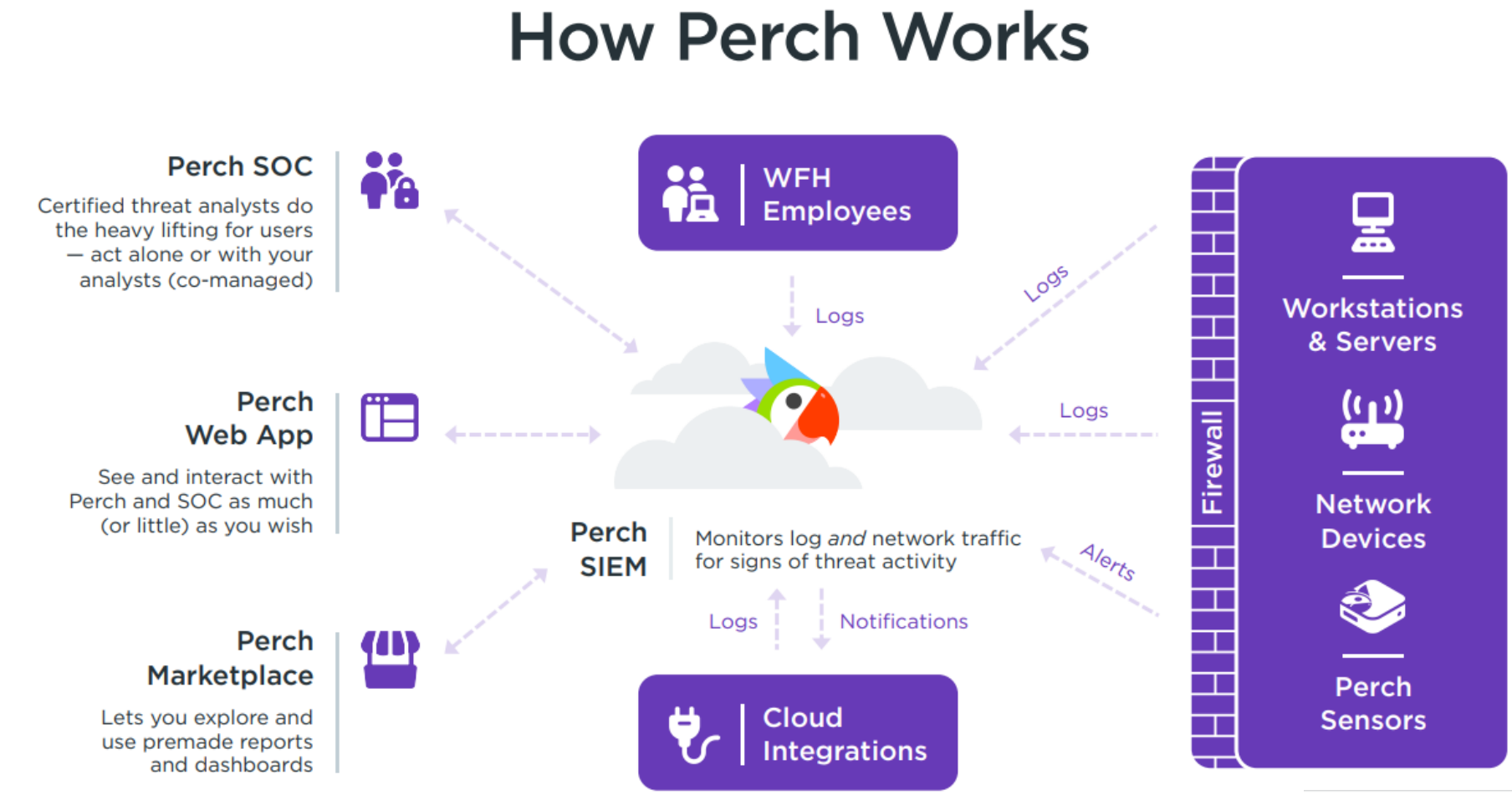
Why do I need it?

- Auditing and Compliance Requirements
- Full Visibility of Everything Happening Within the Network
- Dramatically Decreases the Time it Takes to Identify Threats
- Detailed Forensic Analysis in the Event of Major Security Breaches

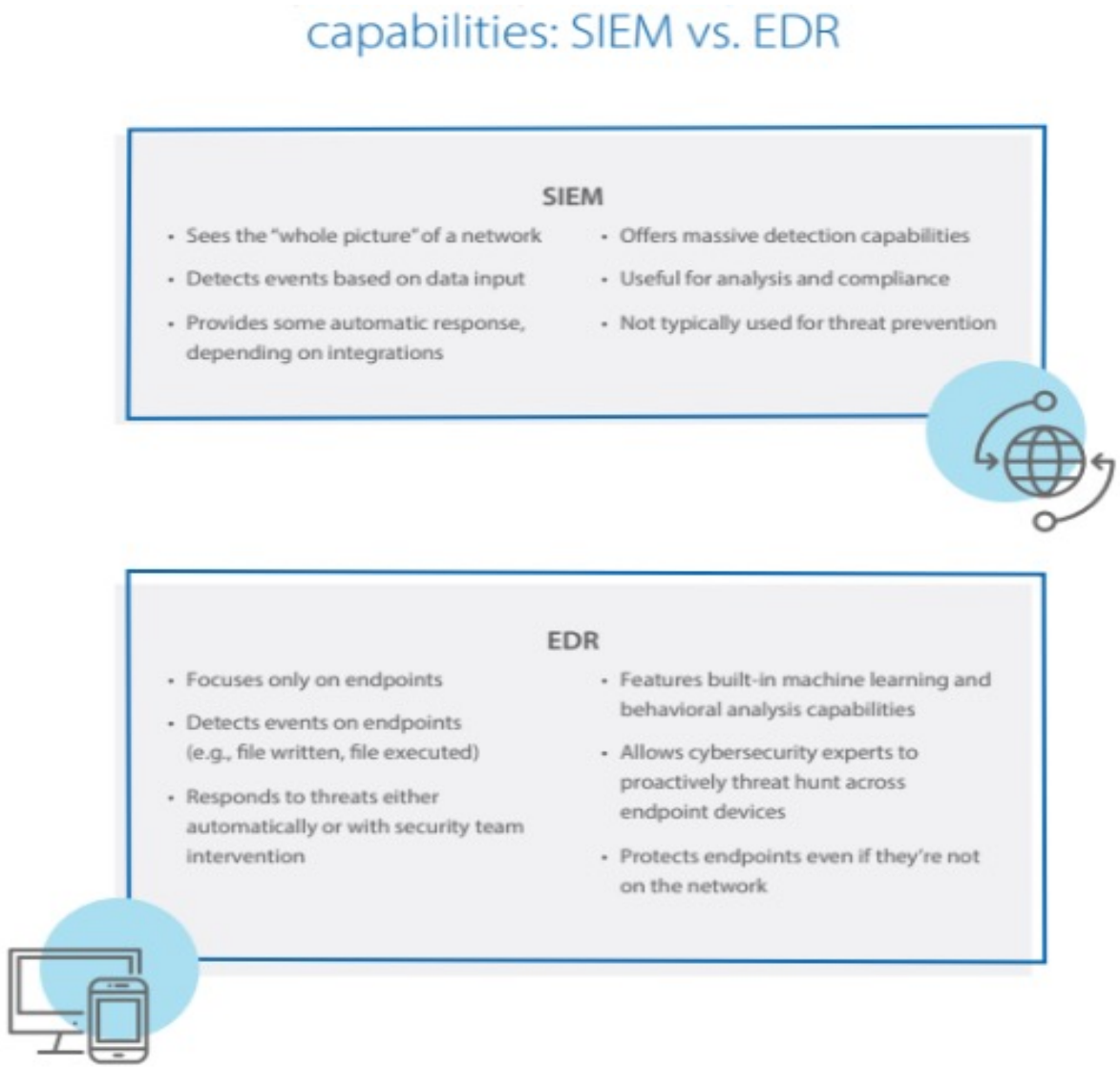
CENTARIS™

The problem with SIEM

How a SIEM Works



Differences in SIEM & EDR (MDR)



Traditional AV vs MDR/EDR

Traditional Anti-virus

- Antivirus is signature based, so it only recognizes threats that are known.
- Can utilize Heuristics – predictions based on normal behavior
- AV can include scheduled or regular scanning of protected devices to detect known threats
- Assists in removal of more basic viruses (worms, trojans, malware, adware, spyware, etc.)
- Warnings about possibly malicious sites

Managed Detection & Response (MDR)

- MDR includes real-time monitoring and detection of threats – including those that may not be easily recognized or defined by standard antivirus.
- MDR is behavior based, so it can detect unknown threats based on a behavior that isn't normal.
- Data collection and analysis determines threat patterns and alerts organizations to threats
- Forensic capabilities can assist in determining what has happened during a security event
- MDR can isolate and quarantine suspicious or infected items.
- MDR can include automated remediation or removal of certain threats

Legacy Anti-virus is No Match For the New Threat Landscape

Malware

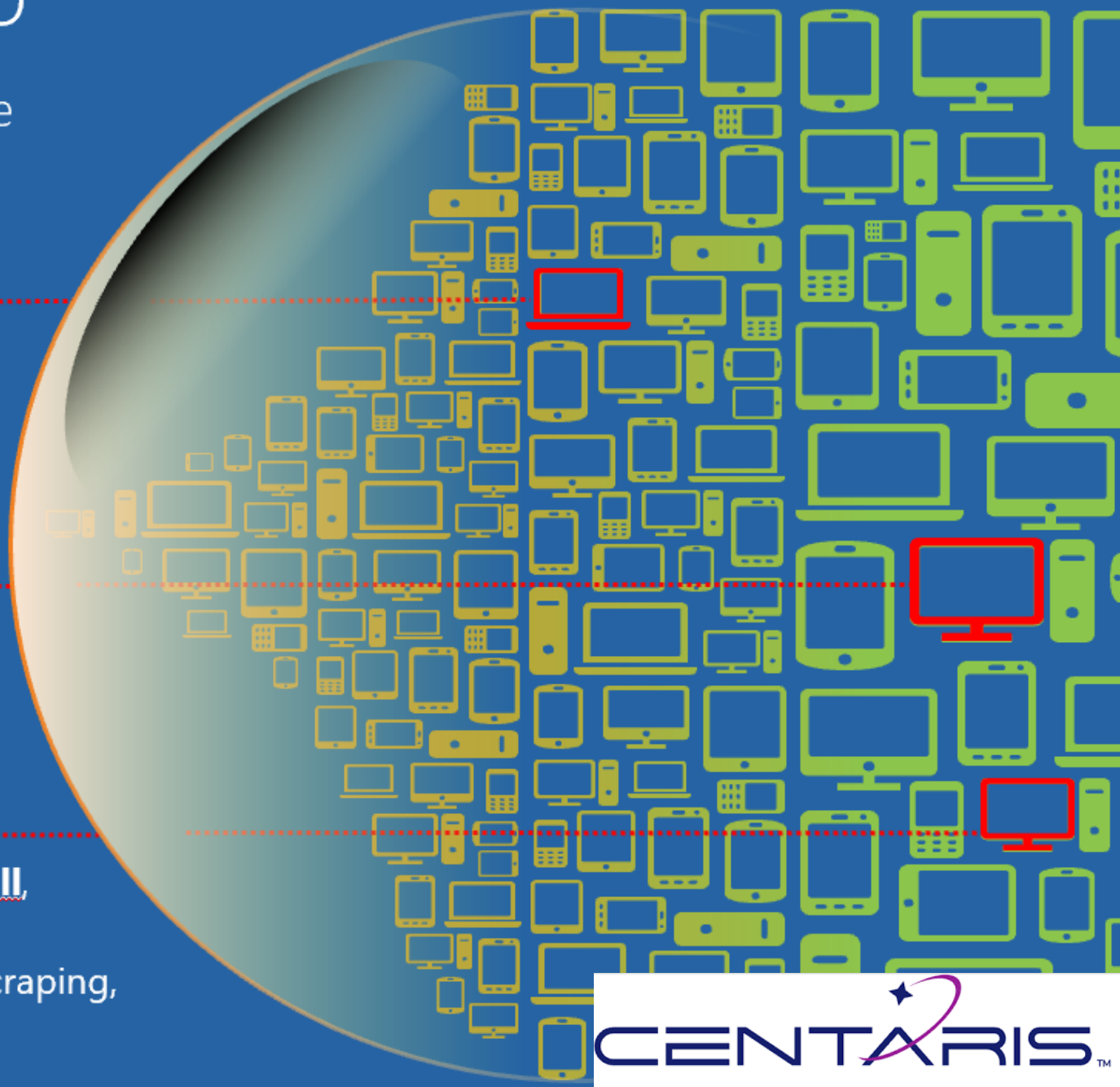
- Ransomware, trojans, worms, backdoors
- **File-less / Memory-based malware**

Exploits

- Document-based exploits
- Browser-based exploits

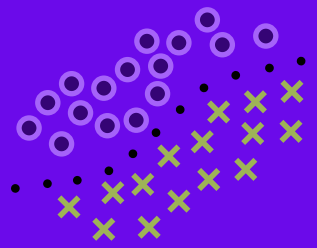
Live Attacks

- **Script-based: Powershell, Powersploit**, WMI, **VBS**
- Credentials: credential-scraping, Mimikatz, Tokens



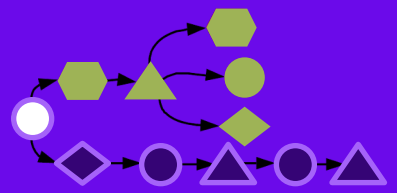
CENTARIS™

Real Time File Analysis



AI Static File Models

ActiveEDR™ Code Analysis



AI Dynamic Behavioral Models

Remediation

- Kill & Quarantine
- One-click Cleanup
- One-click Rollback
- Disconnect from Network
- Local firewall control
- Anti-tamper

Deep Visibility Response

- Threat hunting / Watchlists
- Fast queries. Highly scalable.
- Single pivot storyline built with Storyline™
- Mark entire story as threat
- MITRE ATT&CK™ TTP hunt

REAL TIME PREVENTION + REMEDIATION & RECOVERY | DETECTION & RESPONSE

SentinelOne

CENTARIS™

Cyber Research Unit

Security Content

All the latest in security news. The CRU identifies new vulnerabilities, researches them, and shares what they find with all to see.

Automation

The CRU has developed automated tools to perform basic analysis on security incidents to help automatically make decisions on escalation and remediation.

Research

With "research" in the name, it only makes sense that research is involved. They dig deep into automated and manual malware analysis, vulnerabilities, and more.

Intelligence

The CRU monitors ransom leak sites and malicious botnets for new threats, uses OSINT resources, and utilizes data from the Perch platform to help create content and complete research.

Threat Hunting

With the CRU, cyber threat hunting involves building visualizations to highlight abnormal activity, searching through data for new indicators of compromise (IoCs), or testing various queries and reviewing the results.

CTFs

The CRU is a big fan of hosting CTFs, and for good reason. From their eyes, cybersecurity capture the flag events are a great way to dip your toes into cybersecurity or build upon expert skills.

https://github.com/PerchSecurity/PerchLabs

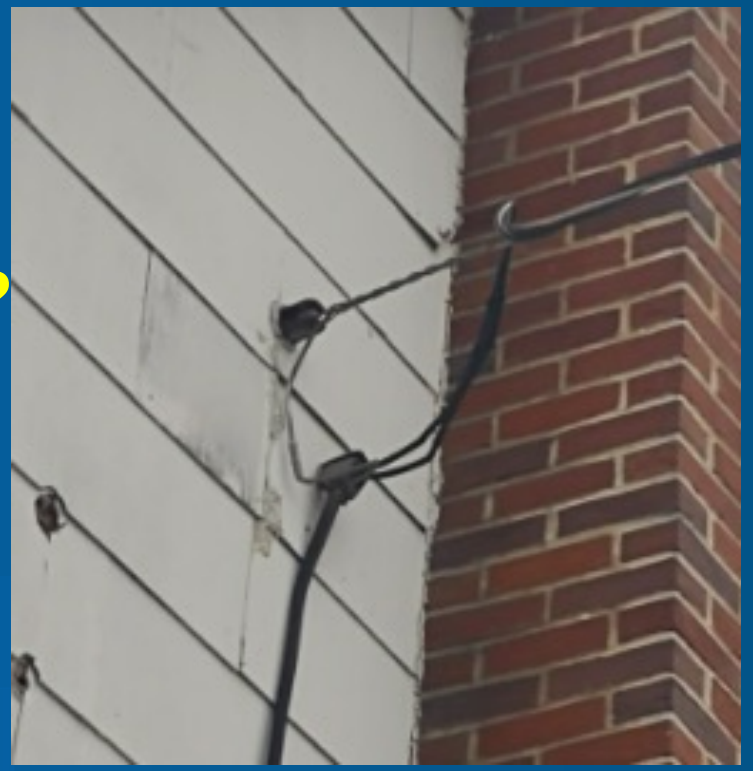
Security & Risk Assessments

Because "You don't know, what you don't know."

CENTARIS™

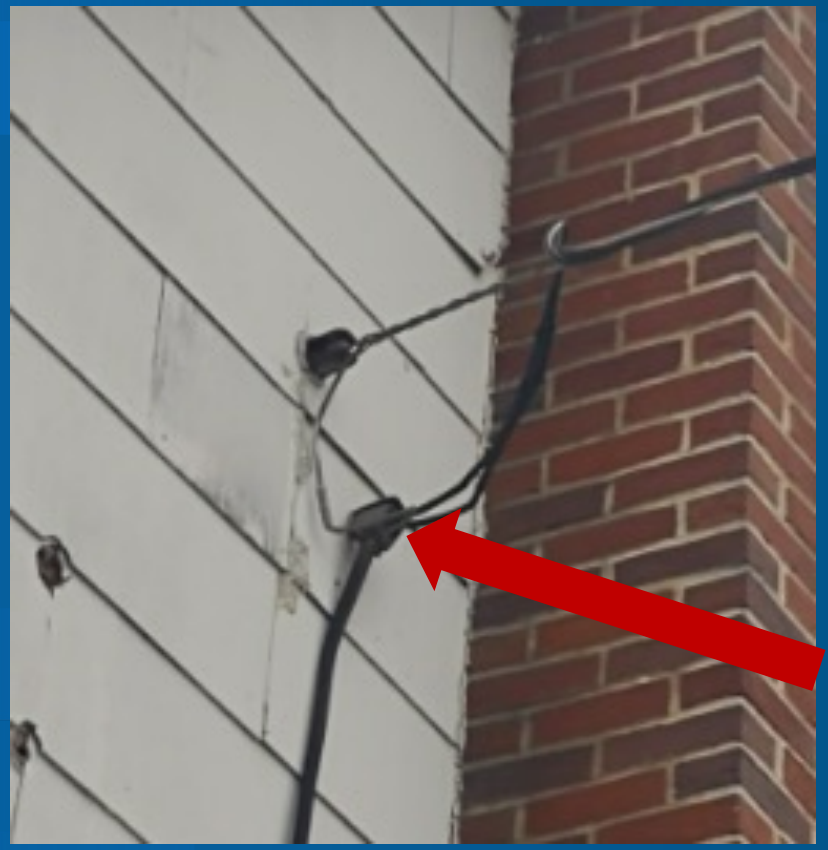
Because “You don’t know, what you don’t know.”

See anything wrong here?

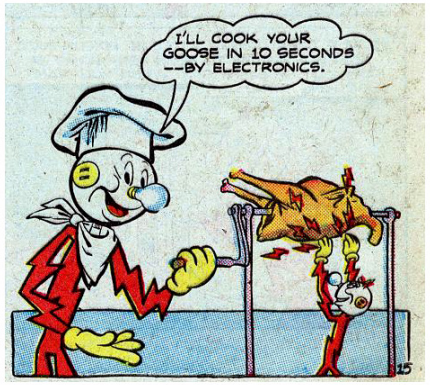


Because “You don’t know, what you don’t know.”

RIGHT!!!



Wrong!!!



Components of a Well-Designed Cybersecurity Solution for Your Business

Security Assessment

Security Awareness

Passwords

DNS Protection

Mobile Device Security

Advanced Endpoint Detection & Response

SIEM / Log Management

Dark Web Research

Backup

Computer Updates

Spam Email

Multi-Factor Authentication

Encryption

Firewall

Cyber Insurance

CENTARIS™

‘The Right’ Cybersecurity

Identify	Protect	Detect	Respond	Recover
Family / Pets	Doors Windows	Alarm	Dog	Cyber Incident Response Plan
Collectibles	Locks	Motion Sensor	Insurance	Backup Systems
Documents / Valuables	Education	Doorbell Camera	Police	Insurance
Electronics / Computers	Yard Signs	Neighborhood Watch	Baseball Bat	Emergency Equipment

CENTARIS™

Compliance

How MDR can help you meet compliance needs

CENTARIS™

Considerations

Compliance

- CMMC
- HIPAA
- ITAR
- SOX
- GLBA
- Contractual Requirements
- Other

Policy

- AUP
- BYOD
- Cloud
- WFH
- Encryption
- Other

Process

- Incident Response
- BC/DR
- Change Mgmt.
- ROI
- Other

Technology

- SAT
- MFA
- EDR / MDR
- SIEM
- Backups
- Network Flow
- Other

CENTARIS™

Q & A

Closing Remarks &
Thank you!

Jason.mcnew@ConnectWise.com

CENTARIS™