Understanding Dynamic Cybersecurity Threats: Insights from the North Carolina National Guard Cyber Security Response Force

MAJ Brian Glish, Cyber and Mission Command Division Chief, NCNG
Ms. Kahmi Crocker, Cyber Hygiene Branch Chief, NCNG

Agenda

- Joint Cyber Security Task Force Overview
- Cyber Security Response Force Overview
- Cyber Threats
- Prevention Steps
- Open Forum

JOINT CYBER SECURITY TASK FORCE (JCTF)

Formal Partnership Executive Order (EO 254) - (March 16, 2022)

- **Members include:**
  - NC Division of Emergency Management (Cyber Unit & Intelligence Function)
  - NC National Guard (Cyber Security Response Force)
  - NC Department of Information Technology Enterprise Security Risk Management Office (ESRMO)
  - NC Local Government Information Systems Association (Cybersecurity Strike Team)
- **Partners include:**
  - NC Fusion Center (NC Information Sharing and Analysis Center – NC ISAAC)
  - Federal Bureau of Investigation
  - United States Secret Service
  - Department of Homeland Security
  - Other federal agencies, NC state agencies, or other stakeholders as needed

The JCTF has existed informally for several years, will continue to offer resource support, incident coordination and technical assistance to various entities, including state and local government agencies and schools and universities impacted by cybersecurity incidents. The Governor's order formalizes this

NC JCTF

Upon receiving a report of a significant cyber incident, the NC JCTF will establish a scoping call with the impacted entity to address the following high-level activities:

- Incident Response. This includes conducting forensics to identify root-cause, damage assessment and mitigation, and coordination with law enforcement activities as needed. Lastly information sharing of indicators of compromise.

- Recovery Response. This effort could include establishing best practice recovery methods, system hardening, restoration of services and infrastructure rebuild.

CYBER SECURITY RESPONSE FORCE (CSRF)

Mission

Conduct Defensive Cyberspace operations to support mission requirements as directed by The Adjutant General or Governor.

Federal Mission: Provide Defensive Cyberspace Operations capabilities on DODIN and supporting Critical Infrastructure

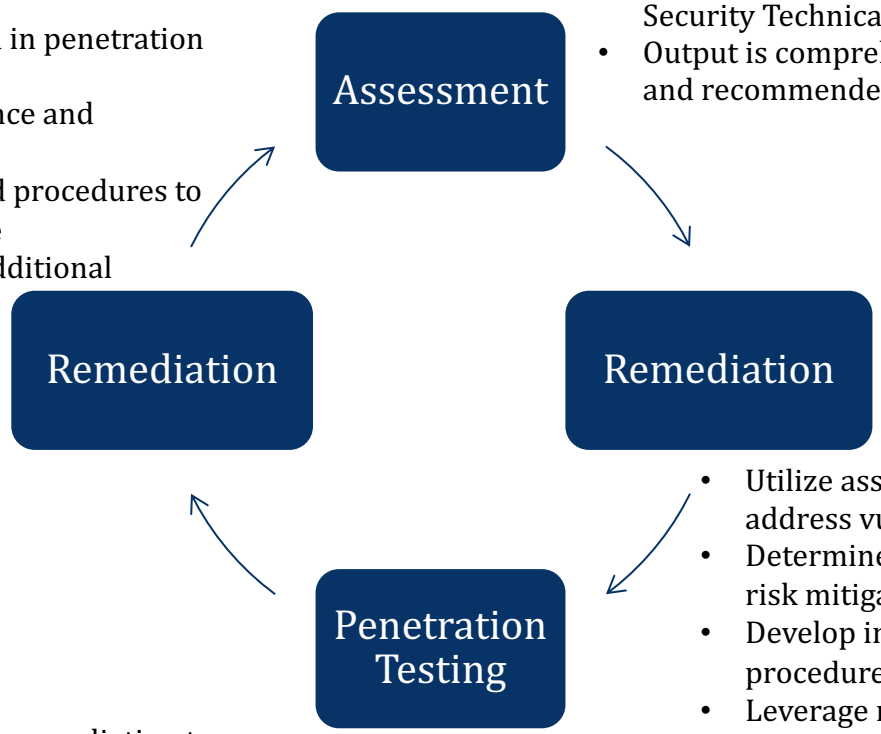
State Mission: Provide cybersecurity assistance to state local and critical infrastructure partners

NCNG CSRF - Lines of Effort

- **Cyber Hygiene Assessment** → Prevention
- **Penetration Testing** → Prevention
- **Continuous Monitoring** → Actively Monitoring Threats
- **Training and Outreach** → Education and Exercises
- **Quick Reaction Support (Cyber QRF)** → Cyber 911
- **Forensics Support and Malware Analysis** → How did it happen & preventing it from happening again

Strategy - Cyber Hygiene Cycle

- Assessment of information security program, environmental factors, and technical area review
- Purpose is to identify potential gaps in coverage as well as provide baseline of improvement recommendations
- Conducted using industry best practices and DOD Security Technical Implementation Guidelines (STIGs)
- Output is comprehensive report outlining vulnerabilities and recommended solutions



- Address vulnerabilities outlined in penetration testing report
- Identify additional risk acceptance and document mitigation strategy
- Evaluate processes, policies, and procedures to ensure comprehensive coverage
- Leverage report to determine additional resource requirements

- Utilize assessment report to prioritize and address vulnerabilities
- Determine acceptable risk levels and document risk mitigation strategy
- Develop internal processes, policies and procedures to improve security posture
- Leverage report to determine additional resource requirements

- Validate the steps taken during remediation to ensure appropriate resolution
- Identify additional areas of concern including user awareness and network monitoring capability
- Output is comprehensive report detailing actions taken and recommended solutions

Cybersecurity Hygiene - Audits/Assessments

The Assessment Team conducts thorough evaluations of networks and infrastructure to ensure they are following good cybersecurity practices. They review the technology and environment to identify any weaknesses, vulnerabilities, or gaps in security.

- Collaboration with Agencies
- Comprehensive Evaluation
- Utilization of Industry Best Practices
- Vulnerability and Security Gap Identification
- Recommendations for Improvement

Cybersecurity Hygiene - Penetration Testing

Goes a step further than cybersecurity hygiene audits/assessments. While the assessments focus on identifying weaknesses and vulnerabilities in a more general sense, penetration testing involves simulating actual cyberattacks to uncover specific vulnerabilities that could be exploited by malicious hackers.

- Simulating Real Attacks
- Exploiting Weaknesses
- Assessing Response
- Mitigation Recommendations
- Risk Prioritization

Continuous Monitoring

The Team provides monitoring for more than 150 agencies including state partners, county governments, and community colleges.

- Continuous oversight and early warning notifications
- Alert agencies to potential changes in their security posture in real time
- Technical expertise to resolve the issue as soon as its identified
- Reducing downtime and spread of attack vectors
- Ability to look across numerous platforms to research threats
- Notify agencies targeted by malicious actors

Training and Outreach

The Team conducts in person and virtual regular training and table-top exercises with state partners across a variety of cyber security related matters.

- Example subjects: Cyber Hygiene Best practices, Election Security, Web Security, Continuity of Operations Planning, Incident Response Plan Development, and Vulnerability Management
- Ransomware tabletop exercises and full scale exercises open to state partners that allows them to see how an incident develops from start to finish, and the steps to take to contain.

Quick Reaction Support (Cyber QRF)

The QRF has trained Incident Responders who can lead agencies into initial triage and through the completed process

- Scoping call in minutes
- On scene of the cyber attack anywhere in the state within hours
- Contain the incident
- Provide technical expertise to restore services as quickly as possible
- Past 12 months completed more than 20 Incident Responses

Forensics Support

Identify the attack vectors and root cause of the incident, as well as indicators of compromise to help prevent the attack from reoccurring.

- Threat hunting and reach back forensic analysis
- Utilize processes approved by Law Enforcement including Secret Service, FBI, and CISA
- Shared between agencies that will help mitigate future attacks

CY 2022 Totals

- 57 Cyber Hygiene Assessments
- 12 Penetration Tests

Through these the NCAAT identified Top 10 fixes that cost little to no money to fix, but they do require time and effort.

- 19 Incident Response Missions
- 3 Statewide elections
- 17 Outreach Events
- 759 Sites Monitored
- 56 Devices Triaged
- 100+ Indicators of Compromise Discovered and Shared

IR Totals Since 2019

- 22 – State Agency
- 16- County Government
- 14 – K-12 School System
- 12 – Community College/University
- 10- Municipal Government
- 8 – County/Tribal (1 associated with SolarWinds hack)
- 7 – City
- 2 – County/County Sheriff's Office
- 2 – Local Agency
- 2- SCADA/ICS
- 1- County Rescue Squad
- 1- Regional Airport
- 1 -City Utility Provider

CYBER THREATS

Ransomware gangs targeted 3 different US water treatment plants in 2021 in previously unreported attacks

- Three US water treatment plants were hit with ransomware attacks in 2021
- The previously unreported incidents came after a widely publicized attack on a Florida plant.
- In all three attacks, cybercriminals took over the water treatment plants' supervisory control and data acquisition systems, also known as SCADA, which lets administrators remotely monitor the facilities.

Prospect Medical Holdings: Hospitals, health care disrupted in 5 states August 2023

- Hospital cyberattacks in the US are a persistent cybersecurity problem.
- Operates 16 hospitals and over 165 clinics and outpatient centers in Connecticut, Pennsylvania, Rhode Island, and Southern California, shut down its clinical operation services and took its IT systems offline due to ransomware, forcing clinicians to revert to paper processes.
- In a recent ransomware research report from Barracuda, ransomware attacks on healthcare increased from 12% to 18% in 2023.

Who is the Real Target?

- Targets of opportunity
- Open-source tools make finding vulnerabilities and exploits easier and easier
- Cyber gangs can be sophisticated organizations with interpreters, lawyers, and coders
- Criminal gangs use Ransomware-as-a-Service to rent software and infrastructure for attacks
- Attacks are scripted and often are “fire and forget” until they gain access

Cyber Crime Impact

- The FBI received more than 800,000 cybercrime-related complaints in 2022
- FBI reports American losses in 2020 exceeding $10 billion - $4.1 billion in 2020
- A cyberattack occurs every 39 seconds
- Over 50% of devices that got infected were re-infected in the same year
- Average Ransomware demand rose to $338,669 in 2020
- Average ransomware attack cost company $1.5M
- 2020 survey of 5000 IT Managers found 51% had been impacted by Ransomware
  - Criminals succeeded in encrypting data in 73% of the attacks
- On average, it takes 212 days to identify cyber breach

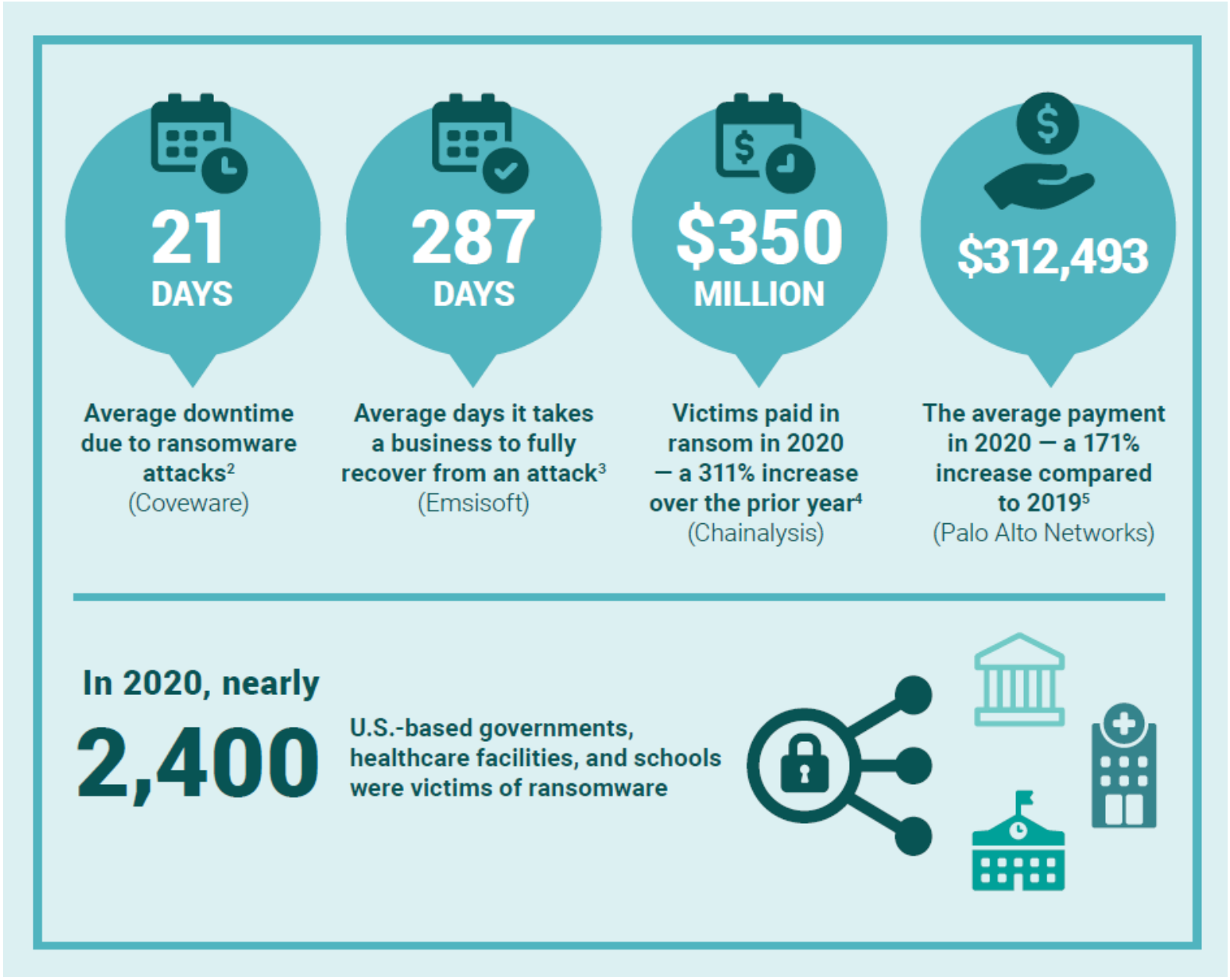
Cyber Threats

- Cyber crime is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them
  - Ransomware
  - Business E-mail Compromise
  - Phishing/Spoofing
  - Denial of Service
  - Malware/Scareware

Ransomware

- 39% of global data breaches caused by malware attributed to ransomware
- Malware that encrypts data or threatens to publish data unless ransom is paid
- Ransomware usually is the last step in a larger breach
  - First step is usually a credential theft process
  - Second step is to spread malware throughout network
  - Third step is to exfiltrate data/information
  - Fourth step is to encrypt systems
- Should you pay the ransom?
  - Attackers will almost always send the decryption key once they receive money
  - They still have access to the system, administrator accounts, networks
  - The only real way to ensure attackers are gone is to rebuild the systems

Ransomware


21
DAYS
Average downtime due to ransomware attacks[2]
(Coveware)
287
DAYS
Average days it takes a business to fully recover from an attack[3]
(Emsisoft)
$350
MILLION
Victims paid in ransom in 2020 — a 311% increase over the prior year[4]
(Chainalysis)
$312,493
The average payment in 2020 — a 171% increase compared to 2019[5]
(Palo Alto Networks)
In 2020, nearly
2,400
U.S.-based governments, healthcare facilities, and schools were victims of ransomware

Agency X

Assessment and Monitoring

Identified Cyber Vulnerabilities

- Bad logon attempts configuration
- Remote Desktop Protocol (RDP) being enabled
- Use of outdated/insecure protocols
- Use of end-of-life technologies
- Vulnerability/patch management concerns

Incident

2021 – Phobos Ransomware Attack

- 30,000 Brute force RDP attempts by malicious actors over two days
- Malicious actors completed lateral movement throughout the network utilizing RDP
- Attackers obtained access to an End-Of-Life Server 2003 R2 machine
- Machine had service pack 2 out of 4 installed

Impact

- Unmitigated identified vulnerabilities resulted in successful ransomware attack on county
- Average ransom demand $338,669
- Average cost of remediation is $622,596.18.

Ransomware in NC

- All attacks have had indicators of compromise in their logs weeks to months prior to attack
- Uptick in 3rd party or contractor account compromise
- Known vulnerabilities/end of life equipment
- Underfunded agencies usually the target
- House Bill 813 bans NC State Entities from paying ransomware

Business Email Compromise

- 2020 BEC losses exceed $1.8B
- In 2020, the FBI received 19,369 Business Email Compromise (BEC)/ Email Account Compromise (EAC) complaints
- Carried out by large criminal organizations
- Target is finances of companies
- Scam tries to get companies to perform wire transfers using existing partnerships
- Sophisticated attacks employ lawyers, social engineers, hackers
- CEO impersonator attacks
- Malware utilized through spear-phishing

Business Email Compromise Steps

Unnamed NC County

- County was working with a real vendor for road repairs
- County was communicating and sending invoices to real email address (i.e. jim@wolfpackpaving.com)
- At some point in the transaction, a new email appears for jim@wolfpackspaving.com
- New bank details and ACH transfer routing were sent to county from that email
- More than $200k was sent to the cyber criminal's account
- Only discovered when real vendor called about unpaid invoices

Phishing/Spoofing

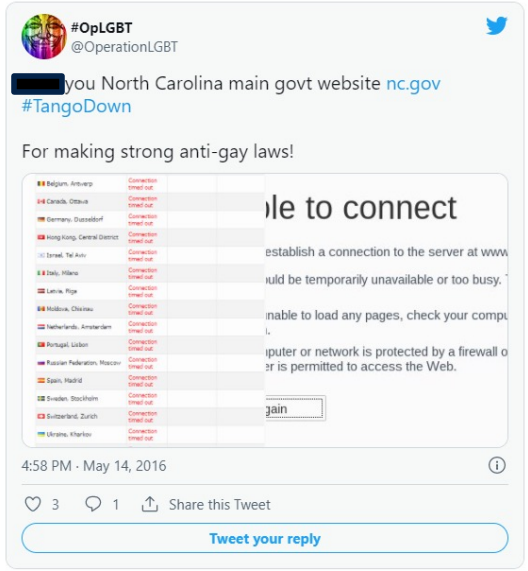
- Email or instant message that tries to obtain sensitive information
- Social engineering process that can appear to be from trusted sites or senders
- Multiple types
  - Spear phishing targets specific individuals
  - Whaling targets senior executives or high-profile targets
  - Clone phishing uses a previous email to make malicious identical email
  - Link manipulation changes the URL just enough to appear legitimate
  - Website forgery uses code to appear to be the correct website

Denial of Service

- Attack prevents users from being able to access systems, services, devices, or network
- Most common attack is a flood of network server to the point of overload
- DDOS increased as COVID 19 forced more people online
- Distributed Denial of Service (DDOS) uses multiple machines to attack a target
  - Usually hijacked machines
  - Makes finding source very difficult
  - Can be traded between hackers
  - 12.5 million variations of DDOS attacks on the web

Anonymous attack North Carolina

- In response to House Bill 2, the hacktivist group Anonymous targeted NC government domains
- Main target was governor Pat McCrory
- Goal was to disrupt traffic to NC government sites



Malware/Scareware

- Malware is short for malicious software
- Designed to gain access to or damage a computer
- Multiple types
  - Spyware-monitor activities
  - Viruses-usually harmful activities such as data destruction
  - Backdoors-allows for unauthorized access to systems
  - Trojan horse-hidden software that looks normal that can be destructive or provide access
  - Adware-installs forced advertising or additional browsers
- Scareware tries to trick you into buying fake or unnecessary software such as antivirus which will then install additional malware

Stuxnet

- Worm that targeted Programmable Logic Controllers built by Siemens
- Iran used the PLCs in their nuclear centrifuges
- Worm designed to speed up centrifuges past tolerance, causing them to shatter
- Worm had three parts
  - Execute payload
  - Spread the worm
  - Hide all evidence
- Introduced via USB to bridge Air Gap
- Accidentally spread outside of Natanz facilities

PREVENTION STEPS

Prevention Steps

- Employee Training
- System patching and maintenance
- Defense in Depth
- Security Policies
- Incident Response Plan
- Use your tools correctly

Common Vulnerabilities and best practices to remediate the vulnerabilities
North Carolina Joint Cyber Security Task Force

Vulnerability	Risk Assumed	Mitigation Measures
Insecure Network Design / vulnerable LEGACY equipment.	When a network is compromised a threat actor has access to compromise all network resources.	Implement network segmentation and enforce network topology changes to include a Demilitarized Zone (DMZ) and a layered defense model.
Insecure Remote Desktop Protocol (RDP) practices	Exposed RDP can allow a threat actor initial access to an organization's network	Place a limit on failed password attempts; limit access to RDP.
Unpatched Network Devices	Cyber Criminals scan for unpatched network devices with known vulnerabilities to target.	Apply aggressive patching methodologies to protect SLTT infrastructure.
Lack of offsite "air-gapped" back ups IAW security baseline and NIST SP 800-53.	Cyber Criminals target backups for encryption in ransomware attacks. If backups are connected to a network they are vulnerable	Maintain offsite backups that can be used in your business continuity plan.
Lack of 802.1x Network Port Control Solution	Devices not managed by the organization can join the network and gain unauthorized access or introduce malicious code to the network	Enable this port control solution for network devices.
Anonymous enumeration of shares must be restricted.	Allowing anonymous logon users (null session connections) to list all account names and enumerate all shared resources can provide a map of potential points to attack the system.	Disable this functionality for all managed assets.
Critical Assets such as domain controllers must be blocked from direct internet access	Domain controllers provide access to highly privileged areas of a domain. Such systems with Internet access may be exposed to numerous attacks and compromise the domain. Restricting Internet access for domain controllers will aid in protecting these privileged areas from being compromised.	Adjust system architecture and implement industry best practices.
The default AutoRun behavior must be configured to prevent AutoRun commands.	Allowing Autorun commands to execute may introduce malicious code to a system. Configuring this setting prevents Autorun commands from executing.	Disable this functionality for all managed assets.
AutoPlay must be disabled for all drives.	Allowing AutoPlay to execute may introduce malicious code to a system.	Disable this functionality for all managed assets.
The Windows Installer Always install with elevated privileges must be disabled.	Enabling Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain full control of a system.	Disable this functionality for all managed assets.
The use of default or shared administrator accounts	When ever users share accounts or use administrator accounts for routine uses they risk those credentials being compromised. It also limits network defender's ability to conduct investigations	Disable accounts no longer in use; use unique administrative accounts and unique user accounts for each individual.

OPEN FORUM