Thwarting Nation-State Cyberthreats

Bob Flores

bob.flores@applicology.com

How can you defend critical infrastructure and sensitive systems against sophisticated state-sponsored cyber operations?

CornCon 11

Who is This Guy and Why Should I Listen to Him?

- 30+ years at the Central Intelligence Agency
- CIA Deputy Director of Information Technology
- CIA Chief Technology Officer
- vCISO at General Radar Corp
- vCISO at Thesus Health
- Several Advisory Boards and Boards of Directors
- Boardroom Qualified Technology Executive (QTE)
- Dad
- Grandpa
- All-around nice guy

Nation-State Cyber Actors

Nation-state cyber actors are government-sponsored groups that engage in cyber operations. They leverage technology to achieve political, economic, or military goals, often targeting critical infrastructure, government institutions, or private companies.

State-Sponsored Groups

Well-funded and highly skilled, these groups are often motivated by political or economic gain.

Advanced Persistent Threats (APTs)

APT groups engage in long-term, stealthy campaigns, often targeting specific organizations or individuals.

Espionage and Intelligence Gathering

Nation states often seek to steal sensitive data, intellectual property, or military secrets.

Disinformation and Propaganda

Some nation states may use cyberattacks to spread propaganda, influence public opinion, or sow discord.

Common Penetration Techniques

All Require a Human in the Loop

1

Spear Phishing

Highly tailored messages targeting specific individuals or organizations.

2

Social Engineering

Convincing narratives designed to manipulate targets into action.

3

Malicious Links

Disguised URLs leading to credential theft or malware installation.

4

Credential Harvesting

Tricking users into revealing sensitive data or access credentials.

Exploitation of Vulnerabilities

Known Vulnerabilities

Nation-state actors exploit publicly disclosed security flaws, often targeting organizations slow to patch. They leverage comprehensive vulnerability databases and automated scanning tools to identify potential entry points across vast networks.

Zero-Day Exploits

These actors invest heavily in discovering and weaponizing unknown vulnerabilities. Zero-days provide a critical advantage, allowing attackers to breach even well-maintained systems. Nation-states may hoard these exploits, using them sparingly to maintain their effectiveness.

Nation-states can afford to allocate significant resources to vulnerability research, often employing teams of elite hackers and security researchers specifically to discover new attack vectors before they become public knowledge.

Long-Term Persistence Strategies

Extended Dwell Time

Maintaining access for months or years, patiently gathering intelligence and avoiding detection.

- Average APT dwell time: 200+ days before detection
- Some advanced actors remain undetected for 2+ years
- Tactical patience to achieve strategic objectives

Network Mapping

Gradually building comprehensive maps of target infrastructure for future operations.

- Discovery of critical assets and data repositories
- Identification of security controls and defensive gaps
- Documenting admin privileges and access patterns

Credential Caching

Storing and rotating stolen credentials to ensure continued access even if some are discovered.

- Harvesting from multiple privilege levels
- Creating backdoor accounts with legitimate-looking names
- Maintaining separate access pathways

Adaptive Tactics

Continuously evolving techniques to counter improving defensive measures.

- Monitoring security tool deployments
- Adjusting C2 infrastructure to avoid detection
- Developing customized tools for specific environments

Targeting Critical Infrastructure

Energy Sector

Compromising power grids, nuclear facilities, and oil/gas infrastructure to potentially cause widespread disruption.

- Remote manipulation of industrial control systems
- Disruption of power generation and distribution
- Pipeline monitoring and control system compromise

Transportation Systems

Infiltrating air traffic control, railway networks, and maritime operations to gather intelligence or prepare for kinetic attacks.

- Manipulation of traffic management systems
- Disruption of automated logistics operations
- Compromise of GPS and navigation systems

Water Treatment Facilities

Accessing control systems of water treatment plants, posing risks to public health and safety.

- Manipulation of chemical dosing systems
- Disruption of filtration and purification processes
- Tampering with monitoring and reporting systems

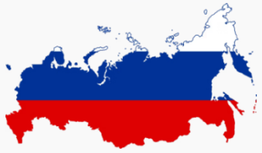
Financial Networks

Breaching banking systems and stock exchanges to gather economic intelligence or cause financial instability.

- Manipulation of transaction processing systems
- Disruption of inter-bank settlement mechanisms
- Theft of financial market intelligence

Compromising critical infrastructure would cause mass chaos and severely impact force protection.

Recent Nation State Attacks



SolarWinds Attack (2020)

A sophisticated supply chain attack compromised the SolarWinds Orion software, affecting numerous U.S. government agencies and private sector organizations. The breach is attributed to **Russia's** Foreign Intelligence Service (SVR), demonstrating the far-reaching impact of compromising widely-used software.

- 9 federal agencies compromised
- 100+ private companies affected
- 18,000 organizations downloaded the backdoored update

3CX Supply Chain Attack (2023)

The 3CX Phone System, a popular voice and video chat app, was compromised, potentially impacting hundreds of thousands of users globally. This attack, linked to the **North Korean** cybercrime group Lazarus, highlighted the ongoing vulnerability of software supply chains.

- 600,000+ customers potentially affected
- Sophisticated two-stage malware deployment
- Data theft and espionage objectives

Microsoft Exchange Server Breach (2023)

Chinese state-sponsored hackers targeted the U.S. Department of State by exploiting vulnerabilities in Microsoft Exchange Server. This breach compromised email accounts and allowed access to sensitive information, underscoring the persistent threat to critical communication infrastructure.

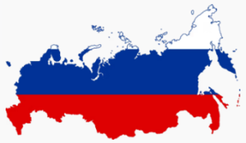
- Tens of thousands of Exchange servers affected
- Zero-day vulnerabilities exploited
- Diplomatic communications potentially
- compromised

And . . .

Colonial Pipeline Ransomware Attack (2021)

The largest cyberattack on U.S. energy infrastructure led to a temporary shutdown of the Colonial Pipeline. A ransomware payment of $5 million was made. Attributed to Russian-backed actors.

- 45% of East Coast fuel supply disrupted
- Six-day operational shutdown
- Gas prices rose by 8.6% in affected regions



Russian Cyberattacks on Ukraine and NATO (2024)

Russia conducted widespread cyberattacks on Ukrainian critical infrastructure and several NATO member states.

- Power grid disruptions
- Telecommunications outages
- Government services compromised
- Coordinated with kinetic military operations

Salt Typhoon (2024)

Chinese state-sponsored hackers conducted extensive cyber operations targeting U.S. critical infrastructure, including military bases and communication networks.

- Multi-year espionage campaign
- Defense industrial base compromised
- Telecommunications providers targeted

Iranian Cyber Operations (2023)

An Iranian hacker group managed to breach multiple American organizations, including a small municipal water authority in Aliquippa, Pennsylvania.

- Industrial control systems targeted
- Water treatment facilities accessed
- Critical infrastructure reconnaissance

Ukraine Power Grid Attacks

2015 Attack

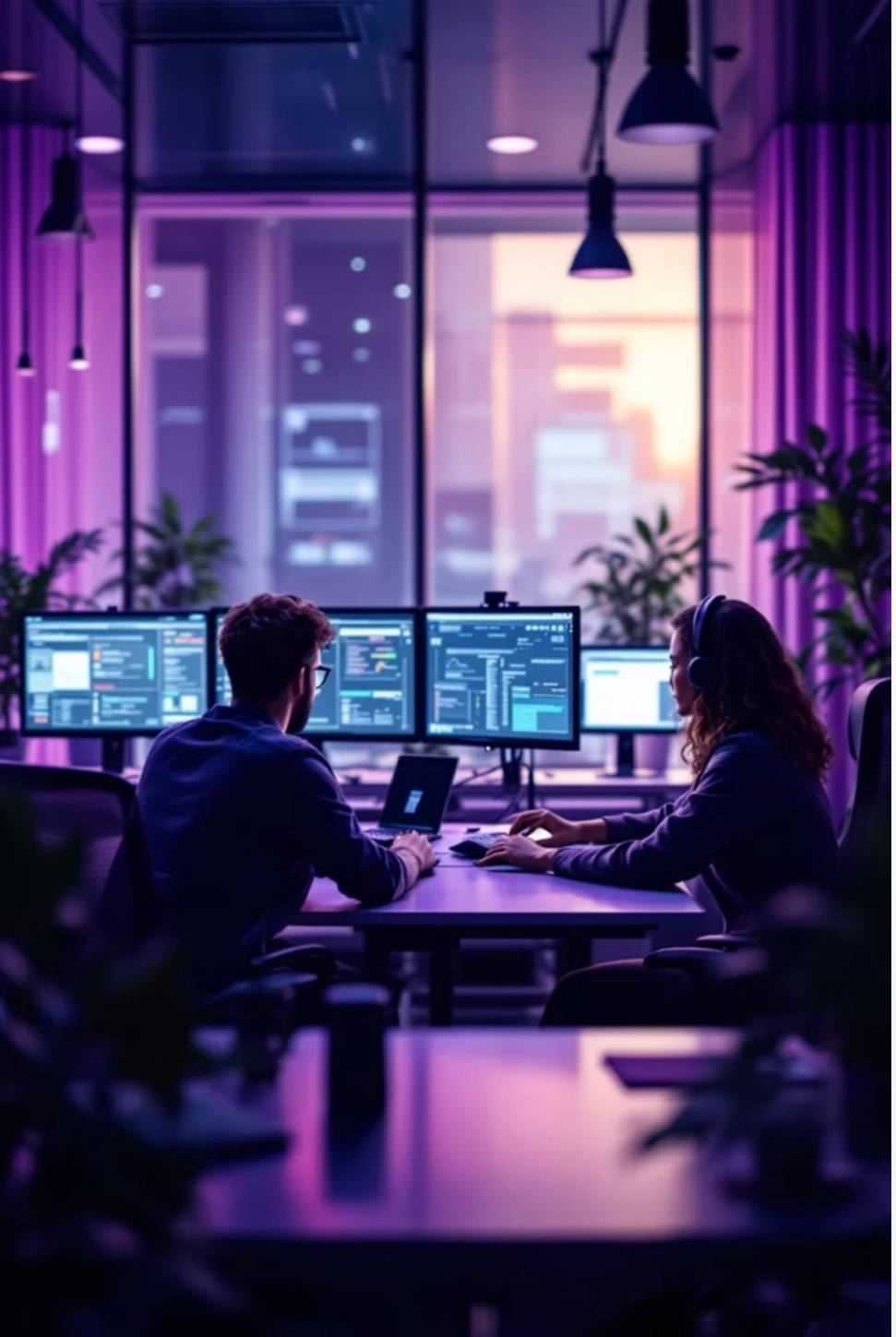
Attributed to Russian hackers, this attack caused power outages for 230,000 residents. Attackers used phishing emails to deploy BlackEnergy 3 malware and gain access to SCADA systems. They remotely opened circuit breakers to disconnect power and deployed KillDisk malware to hinder recovery efforts.

- First confirmed cyberattack to cause power outage
- Six-hour blackout in freezing winter conditions
- Operators forced to manual control for months

2022 Attack

Linked to the Russian hacker group 'Sandworm', this attack targeted a Ukrainian critical infrastructure organization. It caused unplanned power outages across four regions. The initial intrusion began in June 2022, culminating in disruptive events in October 2022, showcasing the persistent nature of these threats.

- Deployed Industroyer2 malware specifically designed for industrial control systems
- Coordinated with physical military operations
- Demonstrated evolution of ICS attack techniques



December 2024

Chinese State Hackers Breach US Treasury

Chinese-backed hackers breached the US Department of the Treasury via cyber vendor BeyondTrust. This attack allowed adversaries to access Treasury workstations and steal unclassified data, potentially revealing sensitive financial data.

⚠ Critical Intelligence Impact

The breach may have exposed financial intelligence data, diplomatic economic strategies, and sanctions enforcement information. Access to this data could inform Chinese economic policy, sanctions evasion techniques, and counter-intelligence operations.

The intrusion was part of a larger campaign targeting multiple government agencies through third-party supply chain vulnerabilities, demonstrating the persistent threat of nation-state actors to critical financial infrastructure.

March 2025

Ghost in the [Juniper] Router

Initial Compromise

A sophisticated Chinese state-sponsored group exploited zero-day vulnerabilities in widely used network routers, establishing a covert presence deep within critical infrastructure networks.

The affected Juniper MX routers were running end-of-life hardware and software

Long-Term Persistence

The attackers maintained persistent access for over a year, conducting extensive reconnaissance and data exfiltration from government agencies and private sector organizations.

July 2025

CISA Issues Urgent SharePoint Advisory

The Cybersecurity and Infrastructure Security Agency (CISA) ordered urgent patching after Chinese hackers were discovered exploiting SharePoint vulnerabilities in live attacks.

Critical Vulnerability

Active exploitation of SharePoint flaws by Chinese threat actors required immediate attention from organizations using this platform.

Mandatory Patching

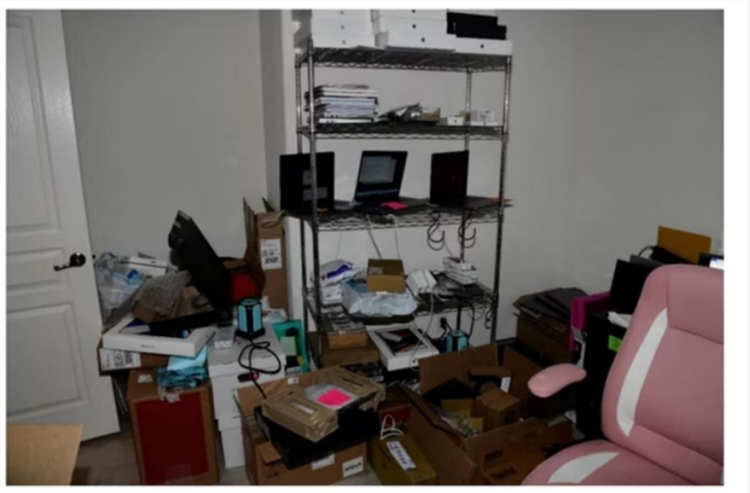
CISA issued a directive requiring federal agencies and recommending that all organizations apply security patches without delay.

Ongoing Threat

These attacks represent part of a broader campaign targeting vulnerable infrastructure across multiple sectors.

July 2025

The North Korea Laptop Farm Operation



When clients got hired, she would receive their corporate laptops in the mail. She kept more than 90 machines at her Arizona home, while re-shipping others to "a city in China on the border with North Korea."

Arizona Woman Sentenced for $17M Information Technology Worker Fraud Scheme that Generated Revenue for North Korea

The Technical Setup

- Used proxies, VPNs, and remote-access software like Anydesk
- North Koreans logged in from afar appearing as normal US-based employees
- Attended Zoom meetings and collected paychecks
- Occasionally exfiltrated data or installed ransomware

July 2025

Chinese Spies Impersonated US Lawmaker to Deliver Malware

US trade groups, law firms and government agencies received an email purporting to come from Rep. John Moolenaar, chairman of the House Committee on the Chinese Communist Party.

The messages, coming from a non-government email address, urged recipients to provide feedback on proposed sanctions against China, telling them that their “insights are essential”.

The email contained an attachment that appeared to be a draft of the legislation. However, it turned out to be a piece of malware that has been linked to the threat group tracked as APT41, which has long been believed to be sponsored by the Chinese government, specifically the Ministry of State Security.

Mitigation Strategy

What Can You Do?

Building a comprehensive defensive posture against nation-state threats requires a multi-layered approach combining technical controls, operational processes, and organizational awareness.

.

Use a Security Framework

1

NIST Cybersecurity Framework

A comprehensive framework for managing cybersecurity risks across an organization.

- Five core functions: Identify, Protect, Detect, Respond, Recover
- Adaptable to organizations of all sizes and sectors
- Maps to regulatory requirements and industry standards
- Enables risk-based approach to cybersecurity

2

ISO 27001

An internationally recognized standard for information security management systems.

- Systematic approach to managing sensitive information
- Risk assessment methodology for identifying threats
- Controls spanning organizational, physical, and technical domains
- Certification process demonstrates compliance

3

CIS Controls

A prioritized set of cybersecurity best practices for organizations of all sizes.

- Implementation groups based on organizational maturity
- Proven effective against known attack vectors
- Focused on operational cybersecurity actions
- Regularly updated based on evolving threats

Security frameworks provide a structured approach to cybersecurity, ensuring comprehensive coverage of defense measures and establishing a common language for security professionals across organizations.

Implement Zero Trust

Never Trust, Always Verify

No user or device is automatically granted access to network resources, even if they are already inside the organization's network.

Instead, all users and devices are required to authenticate and authorize their access before they are granted access to any resources.

Continuous Verification

Authenticate and authorize every access request regardless of source location

Least Privilege Access

Limit user access rights to only what's necessary for their role

Assume Breach

Operate as if your network is already compromised

Zero Trust is a culture, a belief system. It's not a tool or a control.

Build a Culture of Security

Training Programs

Regular security awareness training for employees.

- Mandatory quarterly security refreshers
- Role-specific security training
- Simulated attack scenarios
- Security awareness gamification

Phishing Simulations

Testing employee vigilance against phishing attacks

- Randomized campaigns targeting all levels
- Customized scenarios mimicking real threats
- Immediate feedback and education
- Targeted training for repeat failures

Security Policies

Clear and concise security policies for employees.

- Accessible language and format
- Regular updates reflecting new threats
- Enforcement mechanisms with accountability
- Integration with HR processes

Reporting Mechanisms

Encouraging employees to report suspicious activity.

- Simple reporting tools and procedures
- Non-punitive reporting culture
- Recognition for valuable reports
- Feedback loop on report outcomes

Identity and Access Management

Multi-Factor Authentication (MFA)

Require multiple forms of authentication, like passwords, one-time codes, or biometrics, to verify user identities.

- Implement MFA for all remote access and sensitive systems
- Use phishing-resistant methods like FIDO2 keys
- Enforce contextual authentication based on risk
- Eliminate SMS-based authentication where possible

Least Privilege Principle

Grant users only the access they need to perform their job duties, limiting their ability to access sensitive data.

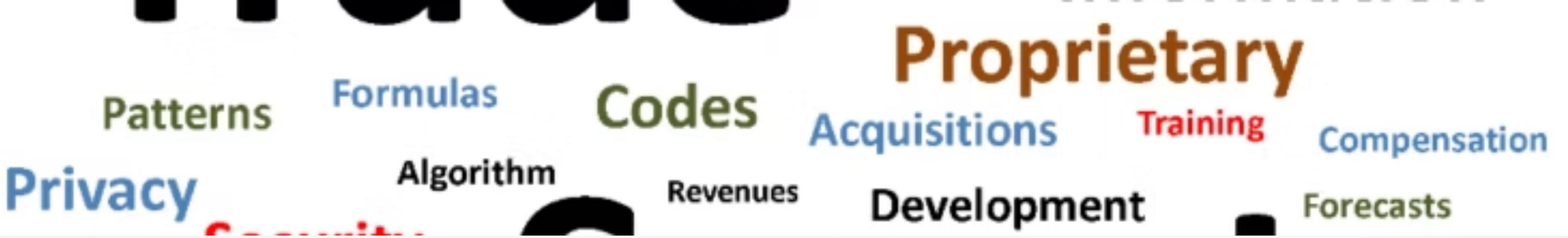
- Implement role-based access control (RBAC)
- Regularly review and right-size permissions
- Employ time-limited privileged access
- Implement workflow-based approval for privileged operations

User Access Reviews and Auditing

Regularly review user access permissions and audit system logs to identify any unauthorized access attempts or suspicious activity.

- Conduct quarterly access certification campaigns
- Implement centralized logging of all authentication events
- Use automated tools to identify access anomalies
- Maintain separation of duties for critical functions

Use a Dedicated Host in Azure or AWS for Active Directory



Sensitive Corporate Database Access

No Token-based Access

Avoid allowing access via SAML, SSO, etc. for sensitive corporate databases. Users must access these databases using account and passwords, biometrics, or passkeys.

Direct Authentication Only

Require dedicated credentials specifically for database access, separate from network authentication.

Biometric Verification

Implement fingerprint or facial recognition as an additional layer for database access authorization.

Hardware-Based Keys

Utilize physical security keys (FIDO2) for database authentication to prevent credential theft.

⚠ Token-based methods like SSO and SAML can create a single point of failure. If an attacker compromises the identity provider, they could potentially gain access to all connected systems, including sensitive databases.

Asset Inventory

You can't protect what you don't know about. A comprehensive asset inventory forms the foundation of effective security by ensuring visibility into all components of your technology environment.

Network Visibility

Maintain a real-time inventory of all IT assets, including hardware and software.

- Automated discovery and tracking of all connected devices
- Continuous monitoring of network endpoints
- Shadow IT detection and management
- IoT and operational technology asset mapping

Risk Assessment

Continuously evaluate the security status of each asset on your network.

- Automated vulnerability scanning
- Security rating for each asset
- Patch status monitoring
- End-of-life/support tracking

Cloud Integration

Extend asset management to cloud environments for comprehensive coverage.

- Cloud resource discovery and tracking
- Container and serverless function inventory
- Multi-cloud visibility
- API endpoint management

Automated Vulnerability Management

Proactive identification, rapid remediation, and continuous monitoring are essential to minimize exposure to nation-state threats.

Utilize automated scanning and CVE monitoring

- Rapid Detection and Continuous Coverage
- Efficient Prioritization
- Compliance Support
- Scalability

Implement Windows Hotpatching

Instead of replacing entire executable files, hotpatching modifies the code within a process's memory space while it's running.

- Available for servers and clients
- Fastest way to patch
- No rebooting required
- Removes the customer and IT bureaucrats (mostly) from the patch process

Restrict Personal Hardware

No BYOD

Strictly prohibit personally-owned computers and devices on the corporate network. You can't secure what you can't manage.

- Enforce through network access control
- Implement device authentication
- Maintain clear policies with consequences
- Provide corporate alternatives for all use cases

Access Control

Use 802.1X authentication to ensure only authorized devices connect.

- Certificate-based device authentication
- MAC address filtering as secondary control
- Integrate with asset management system
- Automatic quarantine for unauthorized devices

Personal devices represent an uncontrolled attack surface that can bypass your security controls. Maintaining strict device policies creates a more defensible environment against sophisticated threats.

Application Control

Application control is one of the most effective defenses against malware, ransomware, and nation-state attacks. It prevents the execution of unauthorized code, dramatically reducing the attack surface.

Implement Strict Application Controls

Deploy App Control for Business (aka WDAC).

- Enforce code integrity policies
- Block unsigned or unauthorized code
- Create multiple policy levels based on risk profile

Allowlist Approved Apps

Create a comprehensive list of permitted applications and scripts.

- Catalog all business-critical applications
- Document required file paths and hash values
- Include legitimate system utilities and admin tools

Monitor Execution

Track all application launches and flag unauthorized attempts.

- Log all execution attempts
- Alert on blocked execution events
- Analyze patterns of blocked attempts

Regular Review

Periodically audit and update the application whitelist.

- Review policy effectiveness monthly
- Adjust based on emerging business needs
- Test updates in controlled environments

Memory Protection

Runtime Protection

Deploy similar memory protection software on all devices (**Morphisec, Virsec**)

- Prevent code injection attacks
- Detect in-memory manipulation
- Protect against fileless malware

Exploit Mitigation

Prevent memory-based attacks like buffer overflows and code injection.

- Data Execution Prevention (DEP)
- Address Space Layout Randomization (ASLR)
- Control Flow Integrity (CFI)

Virtualization-Based Security

VBS uses hardware virtualization and the Windows hypervisor to isolate sensitive security services.

- Protects Windows kernel mode/drivers from memory-based malware attacks
- Restricts kernel memory allocations
- Requires hardware virtualization support (64-bit CPU, SLAT, Secure Boot, TPM 2.0)

Nation-state attackers frequently use sophisticated memory-based techniques to evade traditional security controls. Memory protection technologies specifically target these advanced techniques, providing protection even against zero-day exploits.

Ransomware Defense

Protect

Deploy a dedicated ransomware protection tool (**Halcyon, RansomSnare**).

- Block known ransomware behaviors
- Prevent encryption attempts
- Monitor file system for suspicious activity

Detect

Utilize behavioral analysis to identify ransomware activities.

- Monitor for high volumes of file changes
- Detect unusual encryption patterns
- Identify suspicious process behaviors

Respond

Implement automated containment and rollback capabilities.

- Isolate affected systems automatically
- Kill suspicious processes
- Block outbound communication

Recover

Maintain secure, offline backups for rapid restoration.

- Implement 3-2-1 backup strategy
- Test recovery procedures regularly
- Maintain offline golden images

Nation-state actors increasingly use ransomware as a smokescreen for espionage or disruption operations. Effective ransomware defenses not only protect against criminal groups but also raise the cost for nation-state actors to conduct disruptive operations.

Neutralize File-Based Threats

File-Based Attacks

Many malicious attacks exploit vulnerabilities in files, leveraging techniques like fileless attacks and file manipulation to gain unauthorized access.

- Weaponized documents with macros
- Embedded shellcode in legitimate file formats
- Zero-day exploits in document parsers
- Hidden payloads in complex file structures

Content Disarming and Reconstruction

Deploy a CDR solution. Scan and sanitize all incoming and outgoing files (**Votiro, Glasswall**).

- Deconstruct files to their core components
- Remove active content and embedded objects
- Validate against file format specifications
- Rebuild clean files from verified components

Unlike traditional scanning, CDR doesn't rely on signatures or behavioral analysis. It transforms potentially malicious files into safe versions by rebuilding them according to known-good specifications.

Data Encryption

1 Implement Homomorphic Encryption

Deploy HE for all sensitive databases (**EnVeil, Duality, ShieldIO**).

- Enables computation on encrypted data without decryption
- Prevents clear-text exposure during processing
- Maintains confidentiality throughout data lifecycle
- Protects against both external threats and insider risks

2 Secure Processing

Enable data analysis without decryption, maintaining confidentiality.

- Perform queries on encrypted databases
- Run analytics while preserving privacy
- Share encrypted data with third parties safely
- Protect sensitive information from unauthorized access

3 Key Management

Establish robust key management processes for encryption.

- Implement secure key generation and storage
- Rotate encryption keys regularly
- Apply strong access controls to key repositories
- Create key recovery procedures for business continuity

4 Performance Optimization

Fine-tune HE deployment for minimal impact on system performance.

- Select appropriate HE schemes for specific use cases
- Optimize query patterns for encrypted data
- Balance security requirements with performance needs
- Implement caching strategies where appropriate

Mitigate Web-Based Threats

Browser Isolation

Implement browser isolation technology (**Kasm, EverFox, LayerX**).

- Execute web content in isolated environments
- Render only safe visual output to end-users
- Prevent direct code execution on endpoints
- Create disposable browsing sessions

Isolate Web Traffic

Run all web browsing in isolated containers.

- Physical or logical separation from core systems
- Containerized browsing environments
- Virtual machine isolation techniques
- Remote browser isolation (RBI) deployment

Prevent Downloads

Block direct file downloads to endpoint devices.

- Sanitize files through CDR before delivery
- Implement strict file type filtering
- Apply download quotas and restrictions
- Use isolated file viewers for untrusted content

Monitor Activity

Log and analyze isolated browsing sessions for threats.

- Record all browsing activity for forensic purposes
- Implement behavioral analysis for session activities
- Flag unusual patterns or risky websites
- Generate reports on browsing trends and risks

Network Segmentation and Micro-Segmentation

Restrict Lateral Movement

Prevent attackers from moving freely across the network.

- Implement granular east-west traffic controls
- Create security zones based on data sensitivity
- Enforce strict access controls between segments
- Monitor inter-segment communication for anomalies

Isolate Critical Assets

Protect sensitive data and applications.

- Place crown jewels in highly restricted segments
- Implement dedicated security controls for critical assets
- Apply enhanced monitoring for sensitive zones
- Create airgapped environments for most sensitive systems

Reduce Attack Surface

Limit the number of potential targets.

- Minimize network pathways to critical systems
- Implement least-privilege network access
- Create choke points for enhanced monitoring
- Remove unnecessary services and protocols

Identity-Based Segmentation

Use user and application identity for access decisions.

- Implement software-defined perimeter
- Apply dynamic access policies based on identity
- Create contextual access controls
- Ensure consistent policy enforcement across environments

Restrict Third-Party Access

No Direct Access

Prohibit third-parties from directly accessing your network.

- Eliminate VPN access for vendors
- Remove standing access privileges
- Prevent direct connection to internal systems

Security Proxy

Implement a secure proxy for controlled third-party interactions.

- Deploy privileged access workstations
- Record all third-party sessions
- Implement time-limited access windows

Cloud Isolation

Utilize cloud-based isolation platforms for external collaborations.

- Implement secure virtual environments
- Create data transfer controls
- Enable granular activity monitoring

Third-party access represents one of the most significant attack vectors for nation-state actors. The SolarWinds and 3CX breaches both leveraged trusted vendor relationships to compromise targets. Implementing strict third-party controls is essential for defense against sophisticated threats.

Secure the Supply Chain

Vendor Due Diligence

Thorough vetting of suppliers to assess their security practices and controls.

- Comprehensive security questionnaires
- Third-party security rating services
- On-site security assessments for critical vendors
- Review of security certifications and audit reports

Secure Software Development

Implement secure coding practices and vulnerability management throughout the software development lifecycle.

- Code signing requirements
- Software composition analysis (SCA)
- Static and dynamic application security testing
- Binary analysis for third-party software

Third-Party Risk Management

Establish ongoing monitoring and assessment of third-party vendors and service providers.

- Continuous monitoring of vendor security posture
- Regular reassessment of critical suppliers
- Contractual security requirements and SLAs
- Incident response coordination planning

Supply chain compromises like SolarWinds represent some of the most sophisticated and damaging nation-state attacks. A robust supply chain security program is essential for organizations with sensitive information or critical infrastructure responsibilities.

Secure Privileged Access

Isolate Workstations

Provide domain admins with dedicated PCs located outside the organization forest.

- Physically secured administrative workstations
- Hardened operating systems with minimal attack surface
- Restricted network connectivity
- Enhanced monitoring and logging

Air-Gapped Systems

Ensure admin workstations have no internet access.

- Physical network separation
- Dedicated administrative networks
- Jump server architecture
- Controlled file transfer mechanisms

Strict Access Controls

Implement rigorous authentication for admin activities.

- Multi-factor authentication for all privileged access
- Just-in-time privilege elevation
- Time-limited administrative sessions
- Biometric verification for critical operations

Administrative credentials are primary targets for nation-state actors. Once compromised, these credentials provide extensive access across the environment. Implementing secure administrative workstations significantly reduces the risk of credential theft and misuse.

Remote Administration: Just Say “NO!”

No Remote Admin

You can't secure a remote location.

- Remote connections create uncontrollable attack vectors
- Home networks and public Wi-Fi present significant risks
- Physical security cannot be verified for remote administrators

On-Site Only

Require all admin work to be performed on-premises.

- Establish physical security controls for admin areas
- Implement clean desk policies and screen privacy
- Enable camera monitoring of administrative activities

Secure Infrastructure

Establish dedicated, secure environments for administrative tasks, including sign-ons.

- Privileged Access Workstations (PAWs)
- Physically secured administration rooms
- Network isolation for administrative functions

⚠ **Remote administration significantly expands the attack surface for critical systems. The inability to control the physical environment, network path, and potential device compromise creates unacceptable risks when dealing with nation-state adversaries.**

Continuous Monitoring and Improvement

Vulnerability Scanning

Regular automated scanning of all systems to identify security weaknesses.

- Daily vulnerability scans
- Prioritized remediation based on risk
- Coverage verification

Security Event Monitoring

Real-time analysis of security logs and events to detect potential threats.

- 24/7 SOC operations
- Configure Advanced Auditing (now part of Purview Audit)
- Behavior analytics

Incident Response Testing

Regular drills and tabletop exercises to practice responding to security incidents.

- Quarterly tabletop exercises
- Annual full-scale simulations
- Red team assessments

Security Audits

Independent assessments of security controls and processes.

- Internal audit program
- Third-party assessments
- Penetration testing

Policy Updates and Training

Regular review and improvement of security policies and training programs.

- Quarterly policy reviews
- Continuous awareness training
- Lessons learned implementation

By following a security framework and ruthlessly implementing security controls, you can go a long way toward thwarting most Nation-State attacks.

Defense in Depth

Implement multiple layers of controls so that if one fails, others will still provide protection.

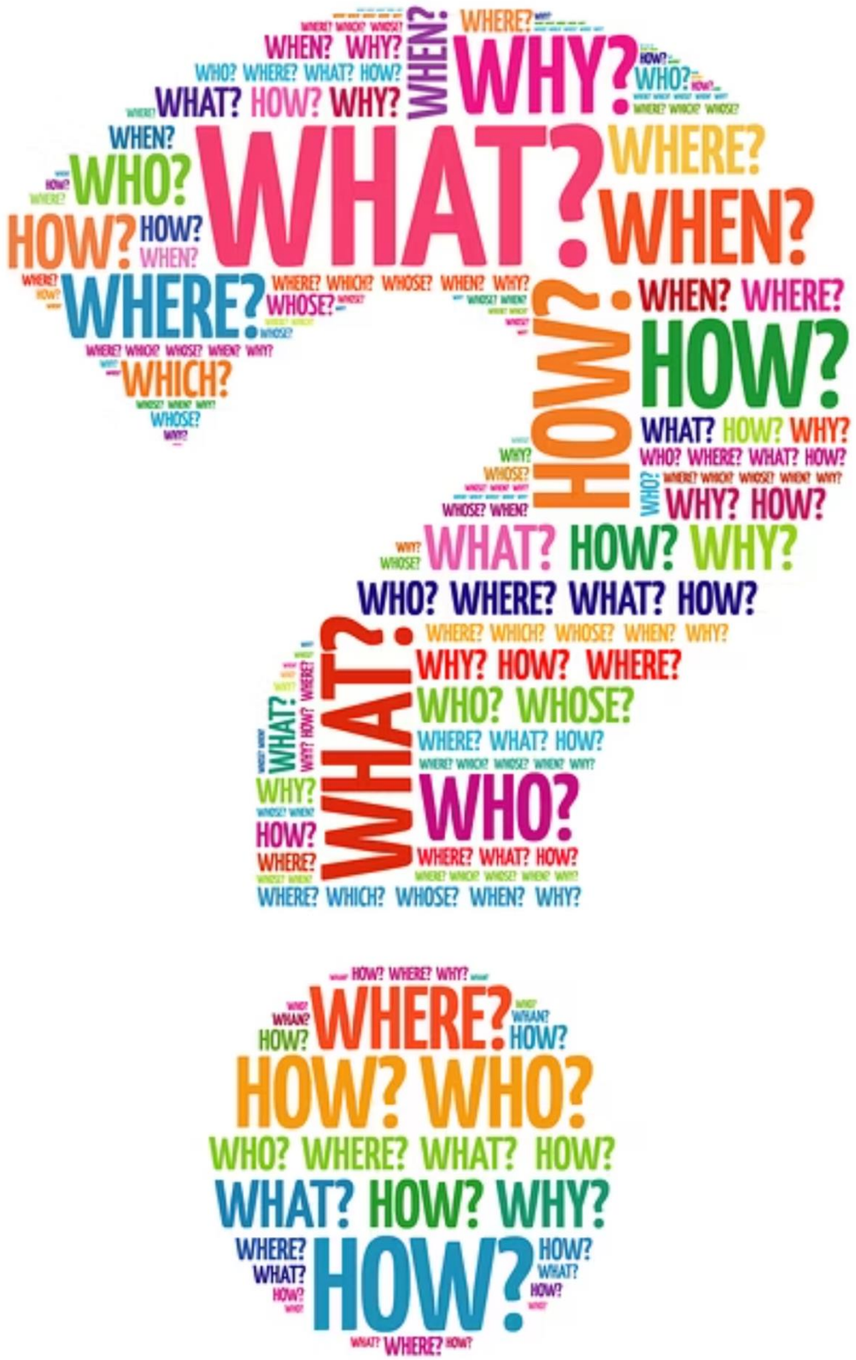
Assume Breach

Design security architectures with the assumption that some controls will be compromised.

The goal is not perfect security, but rather to make your organization a hardened target that requires nation-state actors to expend significant resources, potentially causing them to seek easier targets elsewhere.

Remember

- **Security is not a static goal, but a continuous process.**
- **Nation-state actors constantly evolve their techniques, requiring organizations to maintain vigilant monitoring and continuous improvement of defenses.**
- **Regular assessment, testing, and refinement of security controls is essential to maintaining an effective defense against sophisticated threats.**



Thank You!

For further information or consultation on implementing nation-state threat defenses:

Bob Flores

bob.flores@applicology.com