TANIUM

Unifying Operations & Security in the Face of Advanced Threats

Landon Tholen

Director, Solution Engineering

30 September 2024

“The defining threat of our generation”

-FBI Director Christopher Wray

OSINT

Threat Actor Profile

Targets - IT & OT within the following sectors:

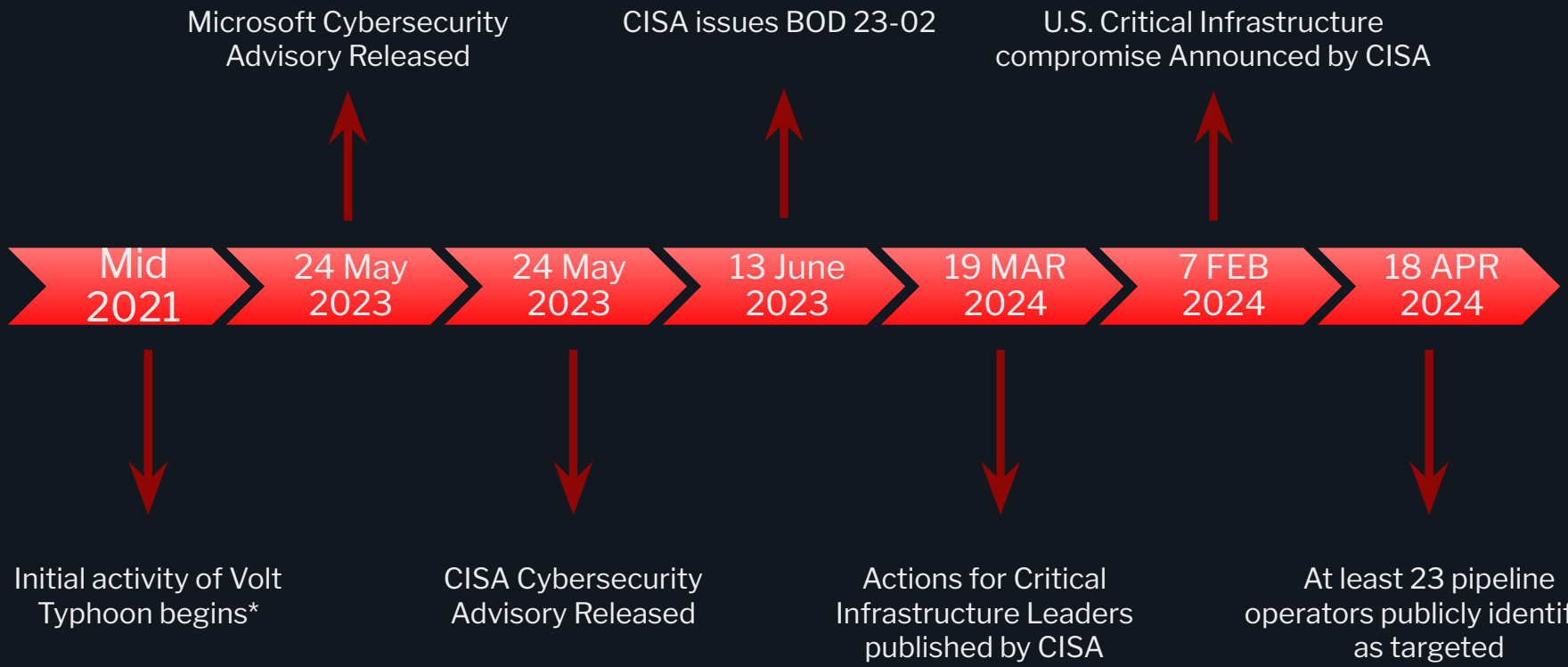
- Transportation
- Communication
- Construction
- Maritime
- Education
- IT Companies
- Manufacturing plants
- Water treatment facilities
- Government agencies
- Power Plants

Objective:
Pre-positioning for destructive attacks

Attack Characteristics

- External network mapping & exploitation
- Credential collecting
- Internal movement
- Limited movement
- LOTL - Living off the land
- Strategic coordination with geopolitical events
- XZ

TIMELINE



*As reported by Microsoft – other sources indicate it may have been earlier

Now what?

The Challenge

- Shortage of skilled cybersecurity professionals
  - More with less
  - Ever changing hybrid work environments
- Complexity of modern IT environments
  - Tools sprawl
  - Exponential amounts of amounts of data produced each year
  - Siloed organizations
- Rapidly changing landscape
  - Growth – M&A
  - Cloud

58%

”Say that staffing shortages put their organizations at significant risk”

-2024 ISC2 Cybersecurity WorkForce Study

Building Your Cybersecurity Ecosystem

- No single vendor does it all
  - Interoperability
  - Open standards
  - Multi-platform support
- Scalability
  - WFH
  - VPN
  - Off-domain
  - Semi-isolated
- Cross platform

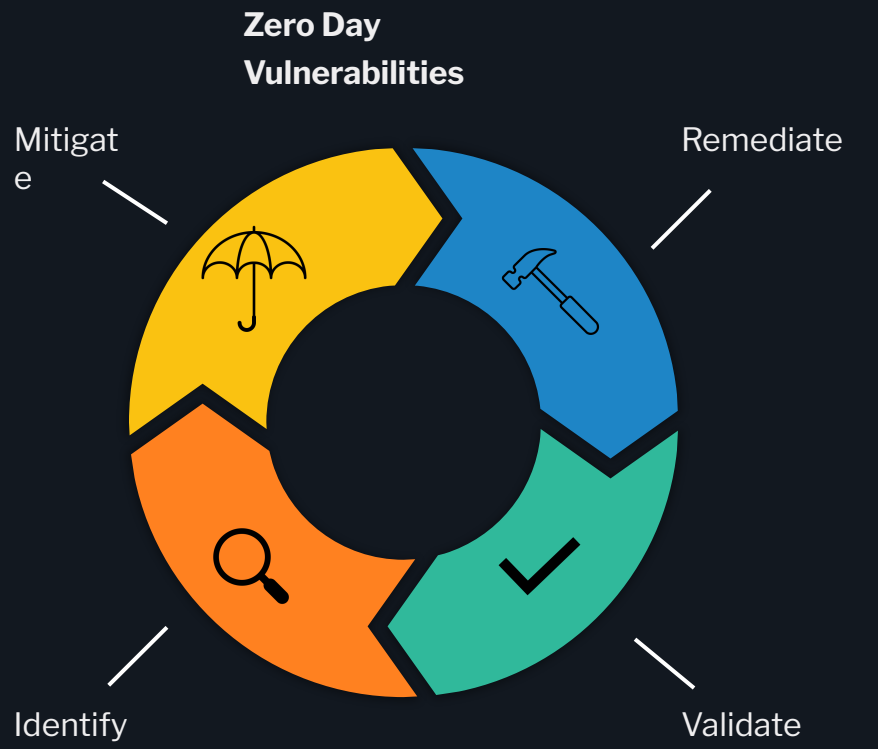
"Minimum effective toolset"
-Gartner

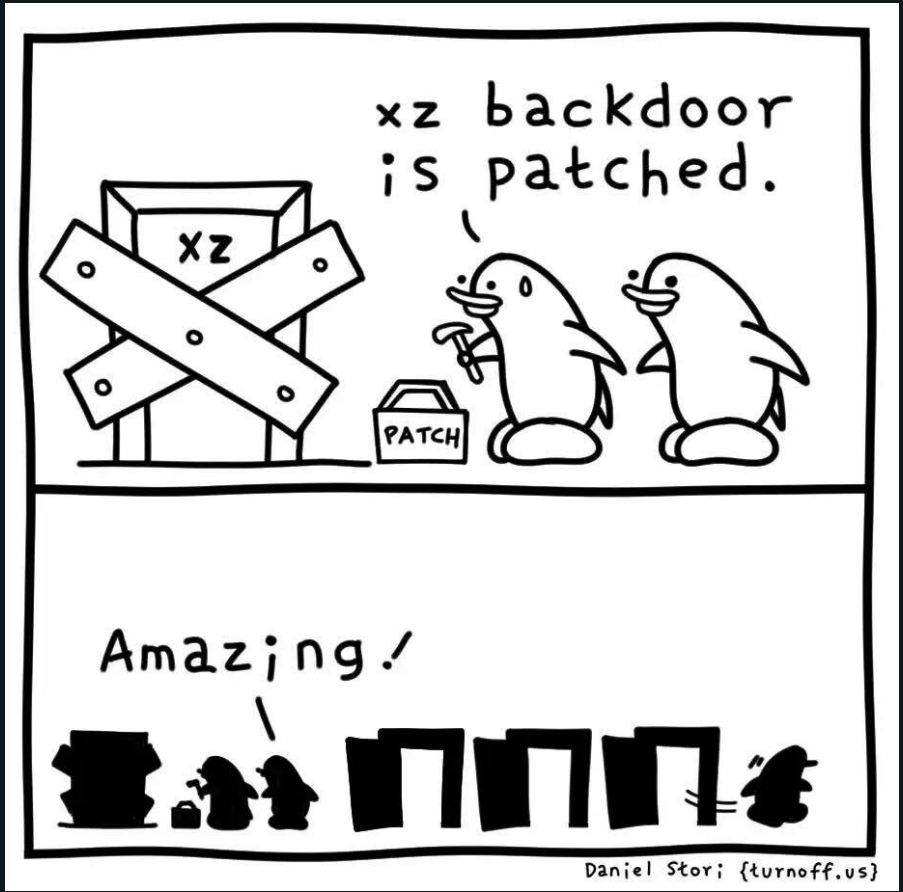
Convergence

- Breaking Down Silos
  - Improved visibility
  - Faster detection & response times
  - Enhanced collaboration
- Reporting
  - Align reporting using real-time information in dashboards and reports
  - Automate reporting – send out
  - Tailored reporting
- Meet & exceed regulatory compliance requirements

Building the Flywheel

- Vuln ID -> Remediation
  - Real-time data
  - Unify the process
  - Rinse & repeat
- Automate to the max extent possible
  - Reduce human error
  - Increase efficiency
  - Reallocate time towards high value activities





Autonomous Endpoint Management

Gartner

“Autonomous endpoint management (AEM) is the convergence of UEM, DEX, VM, and potentially other endpoint domains where the use of data and AI will be used to autonomously handle the majority of common endpoint management tasks.

AEM seeks to significantly reduce IT administration and enable reallocation of resources toward employee enablement and innovation activities.”

- *How many environments have applied this change?*
- *What is the success rate and impact of the change on the endpoints?*
- *How is each stage of the change performing?*
- *Any emerging patterns on failure? Causality?*
- *What are any indirect observations?*

Journey to get there

Target AEM State

Unlocking the answers to YOUR key questions

- What are others doing right now to secure their IT environment?
- How successful has the action been? And if applied to my environment?
- What is my platform doing right now – and why?

Governance at the Core

- See the impact of all actions over time
- Manage the flow of autonomous behaviours
- Compare action benefit, relative impact, and risk

Full Enterprise Control

- Deployment options automatically chosen based on risk threshold
- Can be determined by corporate policy
- Round-trip change request support for ServiceNow

Customize by Policy or by Action

- Details available on-demand with every element auditable
- Controlled by corporate policy and granular RBAC
- Every aspect of the plan can be inspected, modified, and stopped

Key Takeaways

Tools that work together

Breaking down silos

Consolidated Reporting

Automation

Sources

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
- https://www.cisa.gov/news-events/alerts/2024/03/19/cisa-and-partners-release-joint-fact-sheet-leaders-prc-sponsored-volt-typhoon-cyber-activity
- https://malicious.life/volt-typhoon/
- https://beerswithtalos.talosintelligence.com/2033817/14552585
- Mitigating LOTL attacks https://www.cisa.gov/sites/default/files/2024-02/Joint-Guidance-Identifying-and-Mitigating-LOTL_V3508c.pdf
- Initial Volt Typhoon Cyber Security Advorisory (CSA) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
- 24 MAY 2023 Microsoft announcement https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
- https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastructure-2024-04-18/ Christopher Ray Quotes
- https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF

Thank you

Seamless Workflows For IT And Security Operations

Comprehensive visibility & control + advanced threat intelligence, analytics & orchestration.

Real-time, high-fidelity data, action and remediation.

Microsoft

- Defender
- Intune
- Sentinel
- Entra ID
- Security Copilot

servicenow

- HR
- SPM
- Risk
- SecOps
- ESG
- ITOM
- ITSM

Converged Endpoint Management (XEM)

Questions

- What do you do to facilitate cross-organizational collaboration in your company?
- How many different tools or point solutions do you have in your environment?

Converged Endpoint Management (XEM)

Visibility, control, and remediation for all endpoints