EMERGENCY COMMUNICATIONS COORDINATOR REPORT OCTOBER 2024

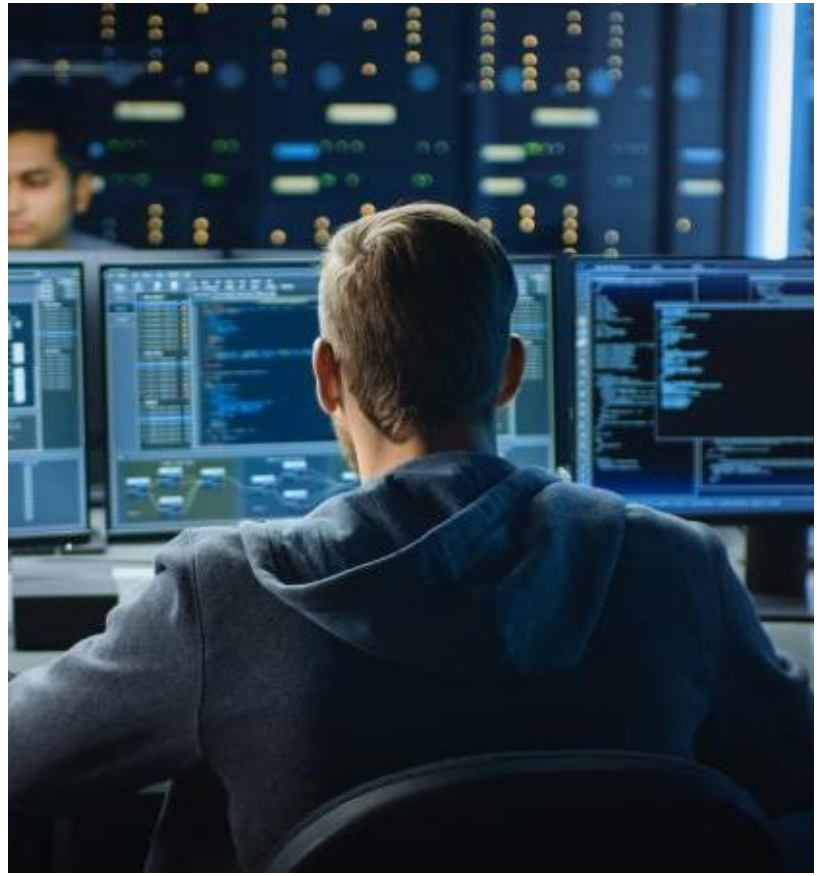
Chris Maiers
October 10, 2024

Cybersecurity Awareness Month 2024

- October is 21st Cybersecurity Awareness Month
- Government & Industry Collaboration
- Four simple steps to stay safe online:
  - Lock down your logins with strong passwords and a password manager.
  - Use multifactor authentication (MFA)
  - Recognize and avoid phishing attempts, scams or tricks. "Think before you click!"
  - Keep your devices safe by updating software regularly and enable automatic updates.
- Cybersecurity Awareness Month | CISA

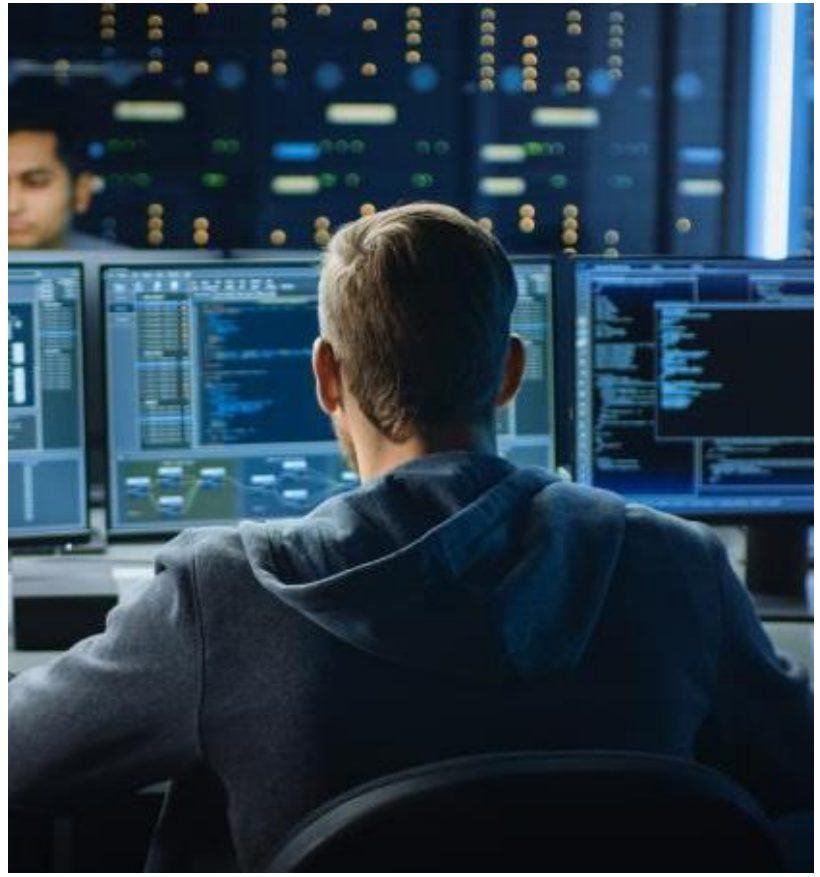
Advanced Persistent Threat – Salt Typhoon

- Appeared in Sept 25th news article and is linked to People's Republic of China.
  - Potentially similar to other threat actors such as Flax Typhoon, Volt Typhoon, and GhostEmperor.
- Indicators of compromise (IOCs) and tactics, techniques, procedures (TTPs) are still being investigated and aggregated.
- Open-source news articles suggest that targets of Salt Typhoon include communications systems for espionage, pre-positioning, and potential disruption.
  - Potential for threat actor to be deeply hidden in systems similar to Volt Typhoon.



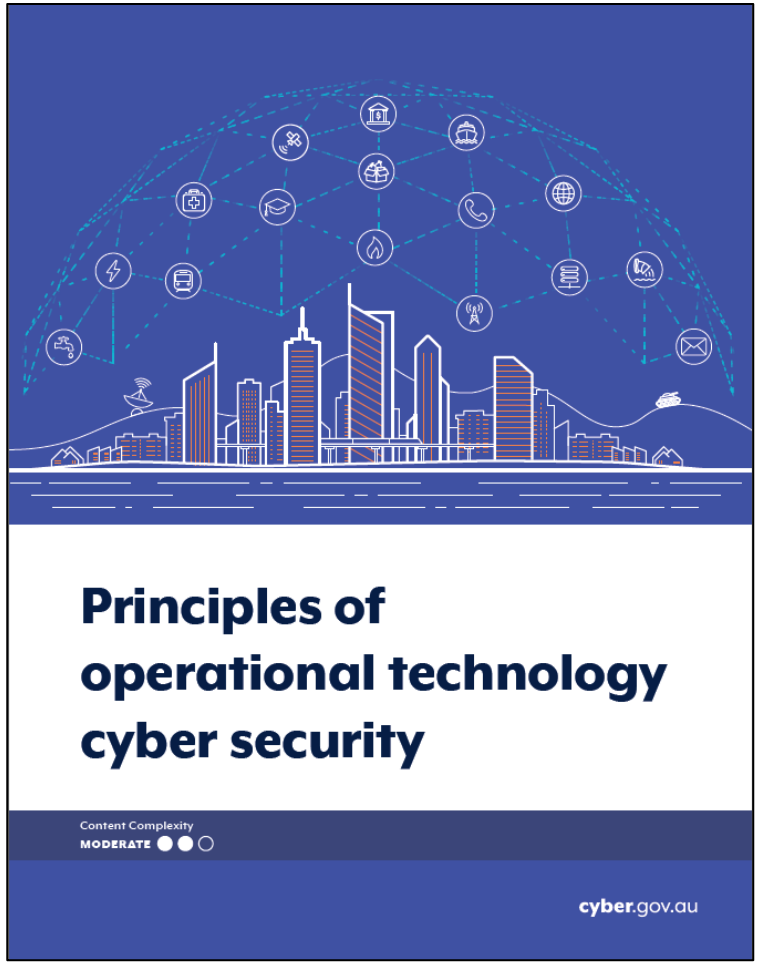
Salt Typhoon (continued)

- Common Vulnerabilities and Exposures (CVEs) that may be applicable for discerning IOCs and TTPs:
  - CVE-2020-0688
  - CVE-2021-26855
  - CVE-2021-4034
  - CVE-2021-40539
  - CVE-2023-46805
  - CVE-2023-4966
  - CVE-2024-21887



Principles of Operational Tech Cyber Security

- Released by CISA & the Australian Signals Directorate Australian Cyber Security Centre and other partners.
- Six principles that OT decision makers should examine closely and apply:
  - Safety is paramount
  - Knowledge of the business is crucial
  - OT data is extremely valuable and needs to be protected
  - Segment and segregate OT from all other networks
  - The supply chain must be secure
  - People are essential for OT cybersecurity
- Principles of Operational Technology Cyber Security



Voluntary Cyber Incident Reporting

- Voluntary cyber incident reporting moved to new CISA Services Portal
- Enhanced functionality: ability to save and update reports, share submitted reports with colleagues or clients for third-party reporting, and search and filter reports
- Guidance resource available: who, why, when, what, and how to report
- https://myservices.cisa.gov/irf
- https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia/voluntary-cyber-incident-reporting

Regional News of Note

- Technical Assistance Request Period – October 2024
  - States that have submitted:
    - Iowa
    - Kansas
    - Missouri
  - Other regional areas that have submitted:
    - Kansas City – FIFA 2026 Planning and Training endorsed by Kansas and Missouri SWICs
  - Will update states as requests are processed.
- Communications Unit Leader (COML) Course.
  - Olathe, KS the week of October 14, 2024.

For more information:

Chris Maiers
Christopher.Maiers@cisa.dhs.gov
202-701-3235