
go
cyber
COLLECTIVE

September Announcements

Serving Our Communities

Thank You, Technology First!

Cyber 101 for Law Enforcement SUCCESS!

HIPPA Workshop, Axis Experience Vehicle

LEADS Nov. 4

2025 GoCyber CTF Nov. 6

September GoCyber Collective Keynote Speaker

- Anna Blair
- Senior Systems Engineer – KBR Inc.
- University of Dayton Graduate (Bachelors and Masters)
- Shifting Your Cybersecurity Lens. Start System-wide.

By Slidesgo

Securing What Matters: A Systems Perspective on Cyber Risk

Anna Blair
Sr. Systems Engineer, KBR Inc.
Linkedin.com/in/anna-g-blair

Speaker Bio

- Education, University of Dayton
  - BS Biochemistry
  - MS Renewable & Clean Energy
- Educational Experience
  - Chaminade-Julienne High School
  - KBR Internship Program
  - AFIT/LS Continuing Education + more
- Customer Experience
  - AFLCMC program offices
  - AFRL
  - AFIT

Intro to System Safety

STPA and STPA-Sec

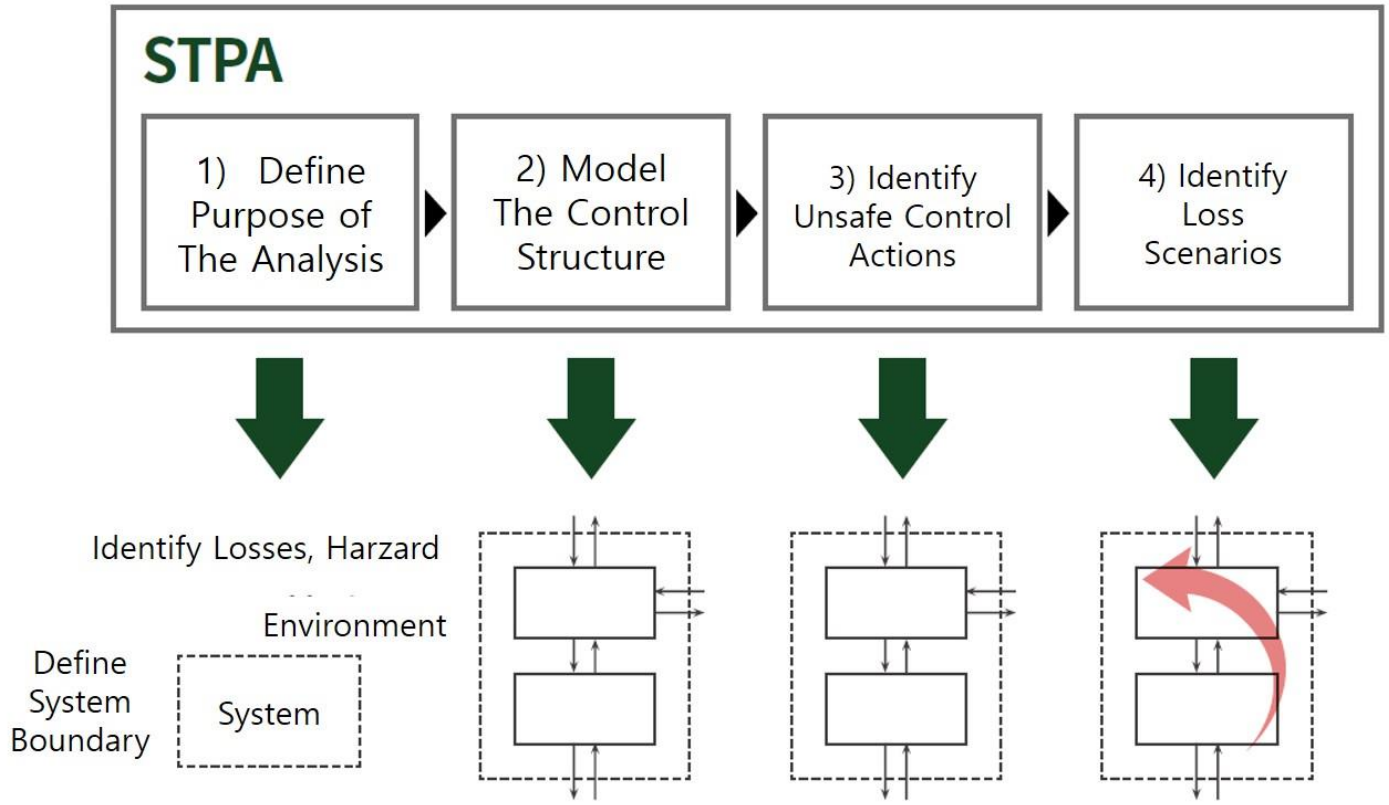
Intro to System Safety

- Technology changes faster than safety methods
- Not enough opportunity to learn from experience
- Changing nature of accidents: more involve software/digital components
- Increasing complexity & coupling in systems
- Decreasing tolerance for single accidents
- More complex relationships between humans and automation
- Changing regulatory & public views of safety

"Incremental improvements in traditional safety engineering approaches over time have not resulted in significant improvement in our ability to engineer safer systems."

- Nany Leveson, PhD, *Engineering a Safer World*

Systems-Theoretic Process Analysis



STPA for Safety and Security

Safety

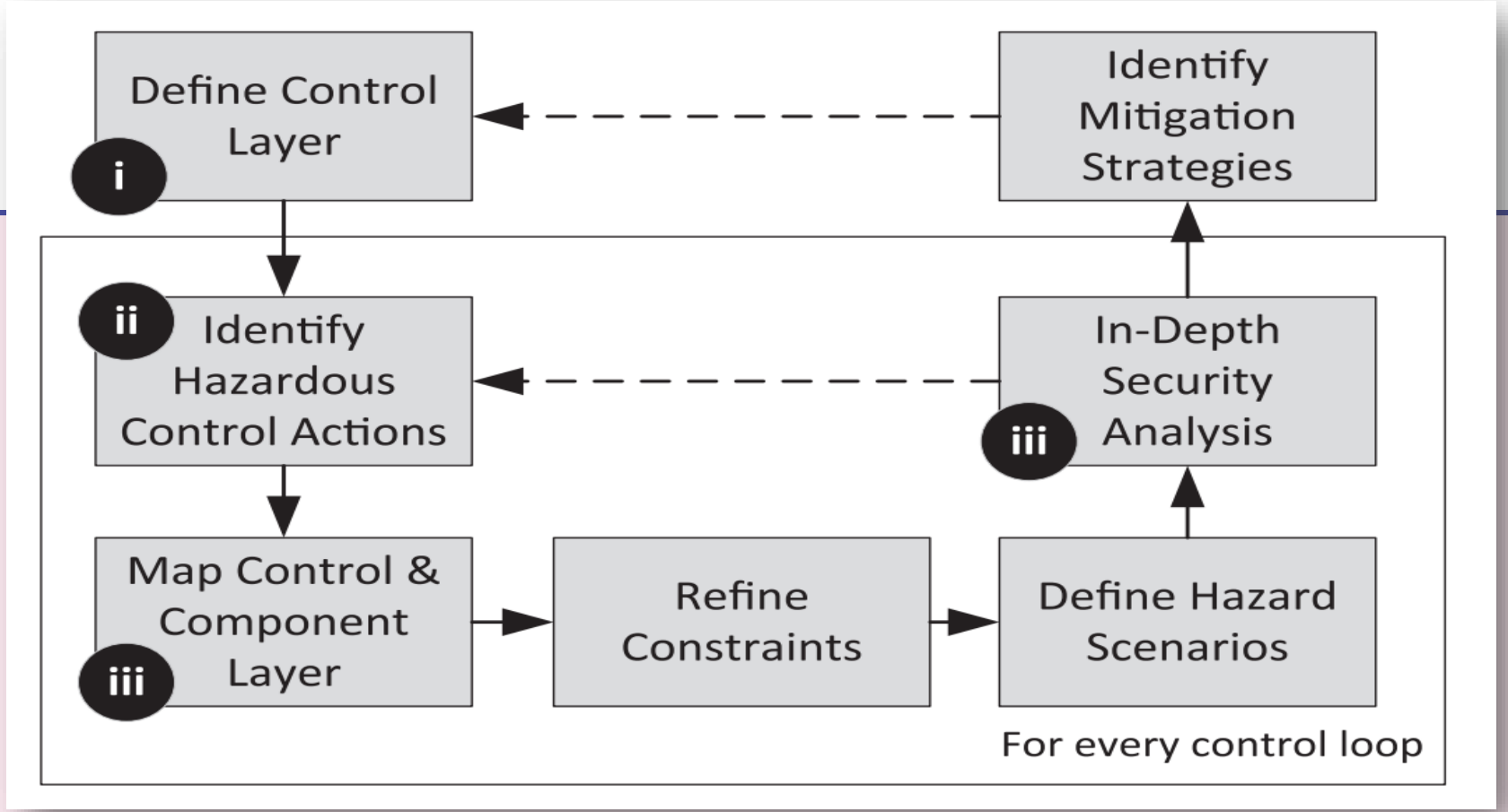
- **Hazards** lead to **safety incidents**
- Prevent **unintentional** losses from **benevolent** actors

Security

- **Vulnerabilities** lead to **security incidents**
- Prevent **intentional** losses from **malevolent** actors
- STPA must be extended to consider intentionally unsafe actions in **Step 4**

Shift security considerations from **tactics** (reactive) to **strategy** (proactive)

Systems-Theoretic Process Analysis for Security (STPA-Sec)



Let’s take a look!

Now that we know the theory, let’s apply it to a real-world cybersecurity issue, and observe the benefits.

I need an app...

I need an app to help turn our precious pets into **animal-influencers**! I want to design a platform for pet-related **lifestyle content, e-commerce,** and access to **pet-sitting services** all in one place!

01

Define the Analysis

Identify losses and hazards that could lead to a loss

1: Define the Purpose of Analysis

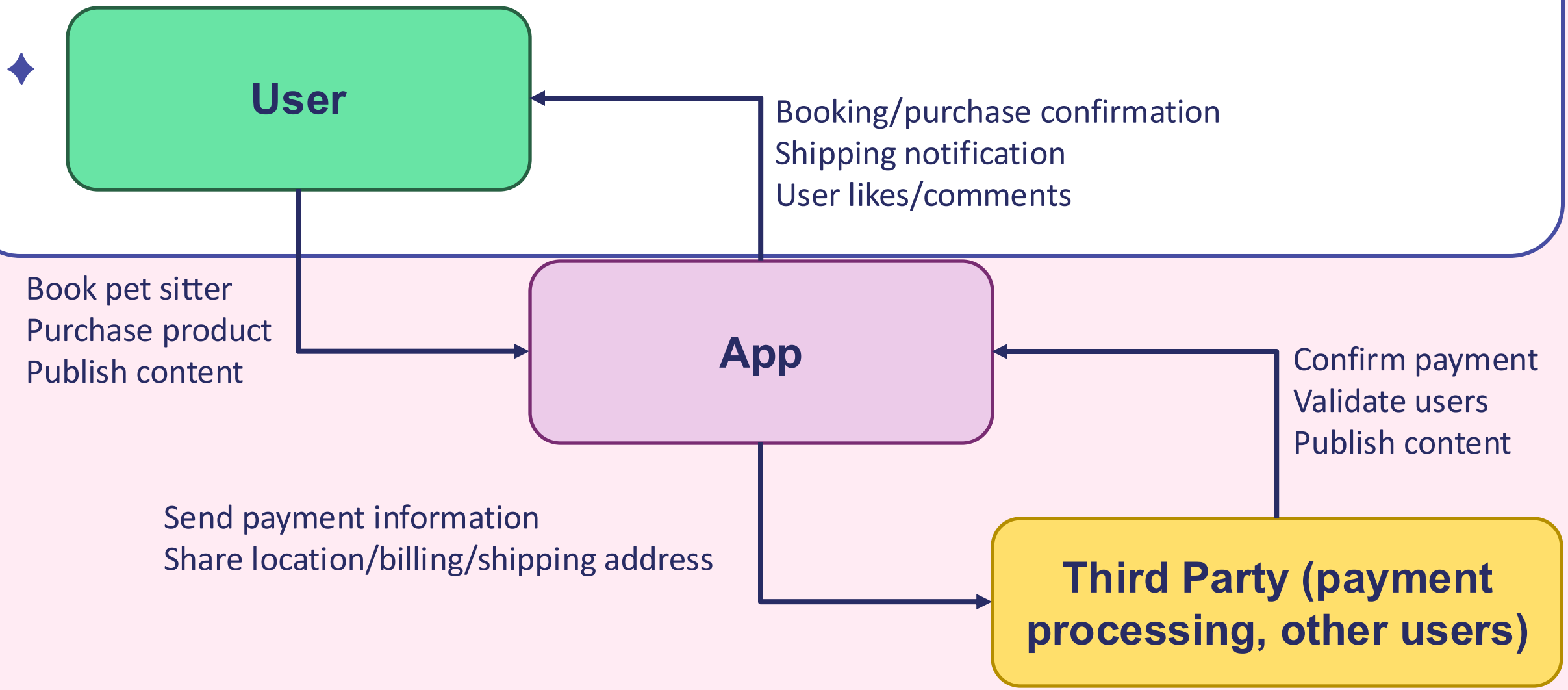
- Identify Losses
  - L1: Pet harm
  - L2: Financial loss
  - **L3: Privacy breach**
  - L4: Reputational damage
  - L5: Platform trust erosion
  - L6: Physical security risk
- Identify Hazards (under the right conditions, could lead to a loss)
  - H1: Unverified providers
  - H2: Weak authentication
  - **H3: Insecure payment handling**
  - H4: Overexposed location data
  - H5: Malicious content injection
  - H6: Unmoderated communication

02

Model the Control Structure

Identify the controller, system under control, and control actions

Model the Control Structure

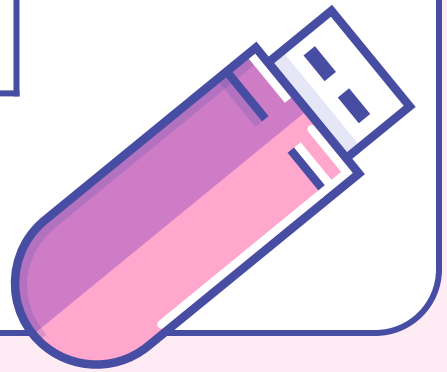


03

Identify Unsafe Control Actions

Unsafe Control Actions

UCA1: Provide	The app provides payment credentials to third parties without proper authorization
UCA2: Not Provide	The app fails to restrict access to sensitive data (keeps payment data visible or poorly protected)
UCA3: Incorrect Timing/Order	The app processes a transaction before verifying sitter/vendor identity, enabling fraud
UCA4: Stopped Too Soon/Applied Too Long	The app retains payment or personal data longer than necessary, increasing exposure in case of a breach



04

Identify Loss Scenarios

How unsafe control actions could arise

- **UCA1:** A poorly written API shares full payment details with their-party pet sitter services instead of using secure tokens
- **UCA2**: Developer debug logs accidentally store unencrypted credit card data, which is later exposed during a server misconfiguration
- **UCA3**: The app lets a sitter/walker accept bookings and charge users before their background check or payment account validation completes
- **UCA4**: The app keeps users' full billing information indefinitely, instead of deleting or anonymizing it after a transaction, so a breach years later still compromises old customers

Possible Mitigations/Safety Constraints

- SC1: Limit Exposure
  - The app shall tokenize all payment credentials and never share raw payment details outside the secure processor
- SC2: Protect Data Lifecycle
  - The app shall purge sensitive data (billing info, PII) after its intended use period
- SC3: Verify Before Transaction
  - The app shall complete vendor/sitter identity checks before enabling payment processing
- SC4: Audit & Monitor
  - The app shall log all payment access events securely and alert on anomalous activity

Thanks!

Do you have any questions?

Anna.blair@us.kbr.com

Linkedin.com/in/anna-g-blair

References

- Nancy Leveson, *Engineering a Safer World*
- Ivo Friedberg et al, *STPA-SafeSec: Safety and security analysis for cyber-physical systems*
- William Young, *Basic Introduction to STPA for Security (STPA-Sec)*
- William Young & Nancy Leveson, *An Integrated Approach to Safety and Security Based on Systems Theory*

September GoCyber Collective Spotlight

- David Sutherin
- Founder & Cyber Compliance Program Director – Triumvirate Cybersecurity Consulting
- CMMC for the Little Guy: January 27

TRIUMVIRATE CYBERSECURITY

NIST SP 800-171

News

DFARS 252.204-7021

September 17th, 2025 | Cybersecurity Compliance Updates

CMMC FINAL!

EFFECTIVE DATE: **NOVEMBER 10TH**

CYBER AB CMMC CERTIFICATION REGISTERED PRACTITIONER ORGANIZATION RPO

CMMC Finalized in Federal Register

- **DFARS Case 2019-D041** Final Rule published September 10th
- Allows enforcement of CMMC requirements as a condition of contract award effective **November 10, 2025**
- **Original phased implementation plan** would permit CMMC Level 1 and Level 2 self-assessments
- DoD memo from January specifies self-assessments are **not permitted** for contracts with CUI in the “Defense” category
- **Extreme shortage of C3PAOs**—booking 6+ months out

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Practical Implications

- If you handle CUI for defense work, expect **CMMC Level 2 certification** show up as a requirement in contracts beginning November 10th
- **Contact a C3PAO** to find out their lead time for assessment
- Be ready to provide self-attestation, **at minimum**, with evidence of intent to undergo an assessment ASAP (e.g., via attestation letter from C3PAO or RPO)

September GoCyber Collective Sponsor

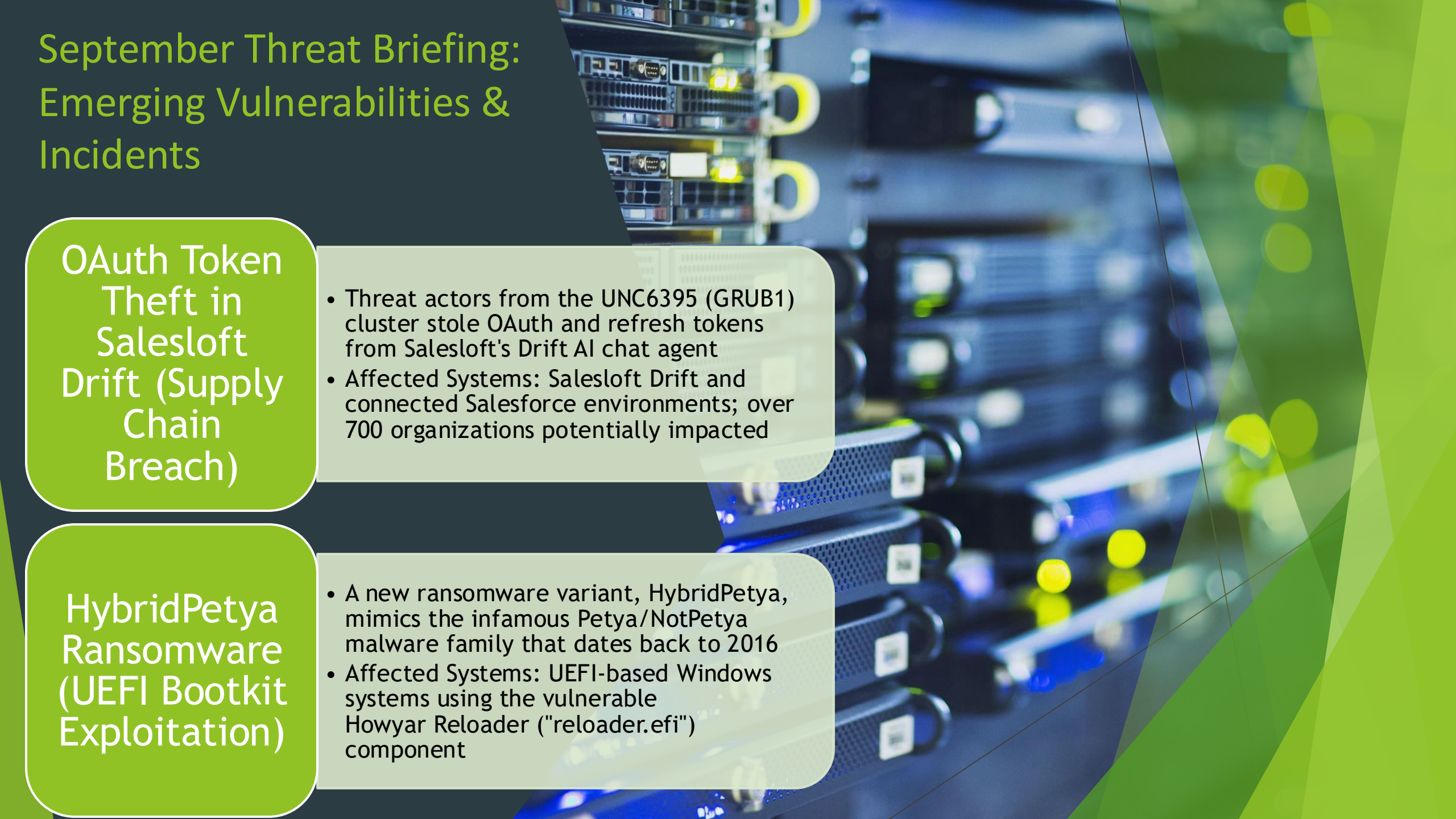
- Thank you, Technology First!
- Taste of IT
- November 12, 2025
- Three Free Tickets

TECHNOLOGY FIRST®

Threat Briefing

Charles Zugaro – Cybersecurity Analyst – Warren County Telecommunications

September Threat Briefing: Emerging Vulnerabilities & Incidents



OAuth Token Theft in Salesloft Drift (Supply Chain Breach)

- Threat actors from the UNC6395 (GRUB1) cluster stole OAuth and refresh tokens from Salesloft's Drift AI chat agent
- Affected Systems: Salesloft Drift and connected Salesforce environments; over 700 organizations potentially impacted

HybridPetya Ransomware (UEFI Bootkit Exploitation)

- A new ransomware variant, HybridPetya, mimics the infamous Petya/NotPetya malware family that dates back to 2016
- Affected Systems: UEFI-based Windows systems using the vulnerable Howyar Reloader ("reloader.efi") component

September Threat Briefing: Emerging Vulnerabilities & Incidents

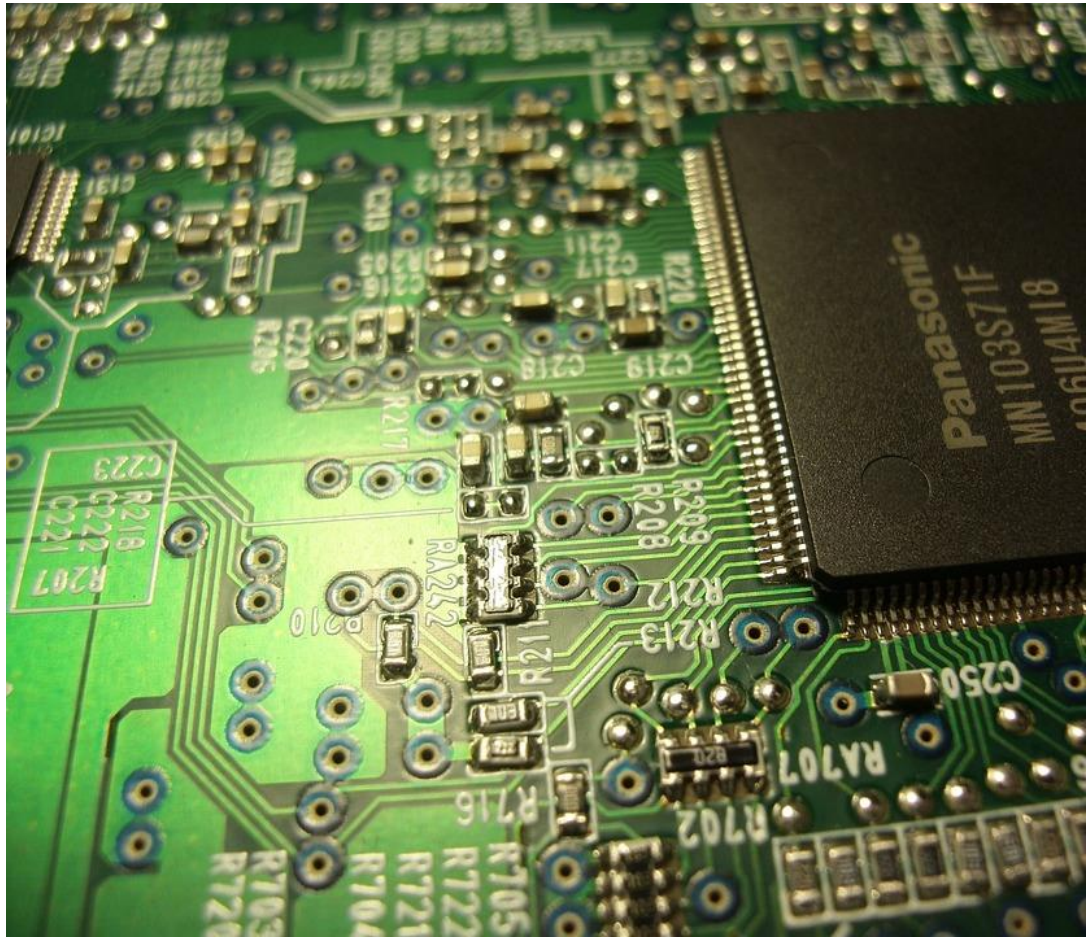
- CVE-2025-5086 in DELMIA Apriso (Remote Code Execution)
  - A critical deserialization vulnerability allows remote code execution via untrusted data in the FlexNetOperationsService endpoint. Exploits deliver a Base64-encoded, GZIP-compressed malicious DLL ("fwitxz01.dll") that acts as a Trojan for spying (keylogging, screenshots, app monitoring) and data exfiltration
  - Affected Systems: DELMIA Apriso Manufacturing Operations Management software (versions 2020–2025)

October Speakers: Zach Heck – Taft

- Cybersecurity Month
- Privacy
- Security
- Government Contracts
- Reducing Risk
- Ensuring Compliance
- Law

September Parting Shots

- Local Gov't/Public Safety SIG – Sun Watch Room
- Education SIG – Wright Patt Room
- Defense Contractor SIG – Hawthorn Room
- Register for CTF, Monthly Meetings and LEADS Workshop
- Turn in your lanyards at the desk



Information

Email me at john@GoCyberCollective.org.

If you have a suggestion on meeting topics, special interest groups, breakfast menu, or anything else we want to hear from you.

You can register for future breakfast meetings from the website.

- GoCyberCollective.org

Event Sponsors