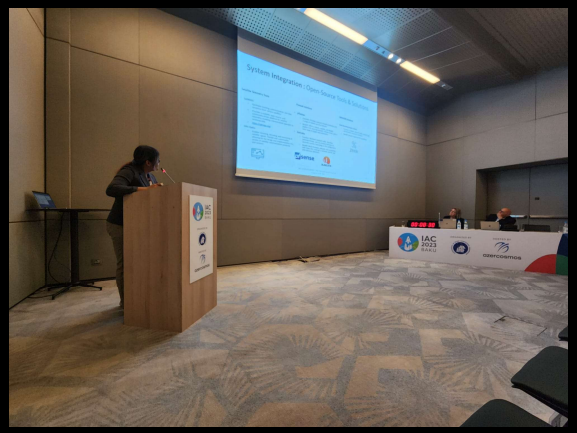
Cyberpunk Security: Refreshing your security mindset

Speaker: Alex Thach

Agenda

Introduction	Cybersecurity Today	AI and Machine Learning	Biometrics	Zero Trust Architecture
The Cybersecurity Market	Edge Technologies	Industries at the Forefront	The Role of IoT	Drone and UAS/UGV Security Concerns and Incidents
Robotics and Satellite Systems Security	The Cyberpunk Influence	The Human Element	Preparing for the Future	Q&A
Conclusion & Call to Action	References			



Introduction

- Today, we'll be diving deep into the evolving landscape of cybersecurity. We'll explore its current state, the technologies shaping it, and the challenges and opportunities that lie ahead. Quick intro: Alex Thach is the name and building edge tech, robots, drones and satellites is the game. Been in security for the last decade and recently in the past 3 months I've presented at DEFCON31, local conferences, published papers on satellite security and currently trying to get a robotics and drone security startup off the ground.

- https://infosec.exchange/@Lexicon101
- https://github.com/Lexicon421
- https://dl.iafastro.directory/event/IAC-2023/paper/80363/
- https://astradacyberlabs.com/

Cybersecurity Today

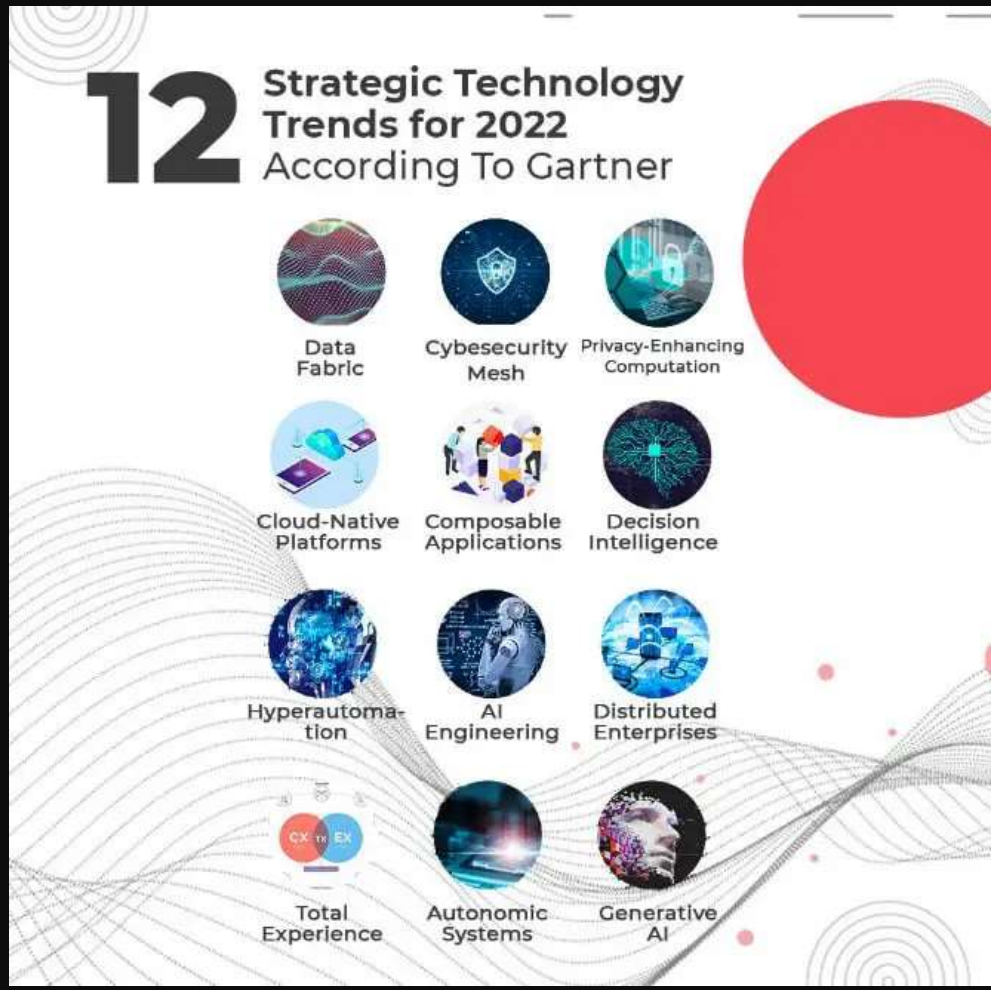
- The cybersecurity landscape is rapidly changing. A notable 48% of organizations reported an increase in cyberattacks this year compared to the last. However, this figure is the smallest reported increase in the past six years. This could be due to evolving defense mechanisms or under-reporting of cyberattacks. The pressing need for transparency and collaboration in the cybersecurity domain cannot be emphasized enough.

- [ISACA's 2023 State of Cybersecurity report]

AI and Machine Learning

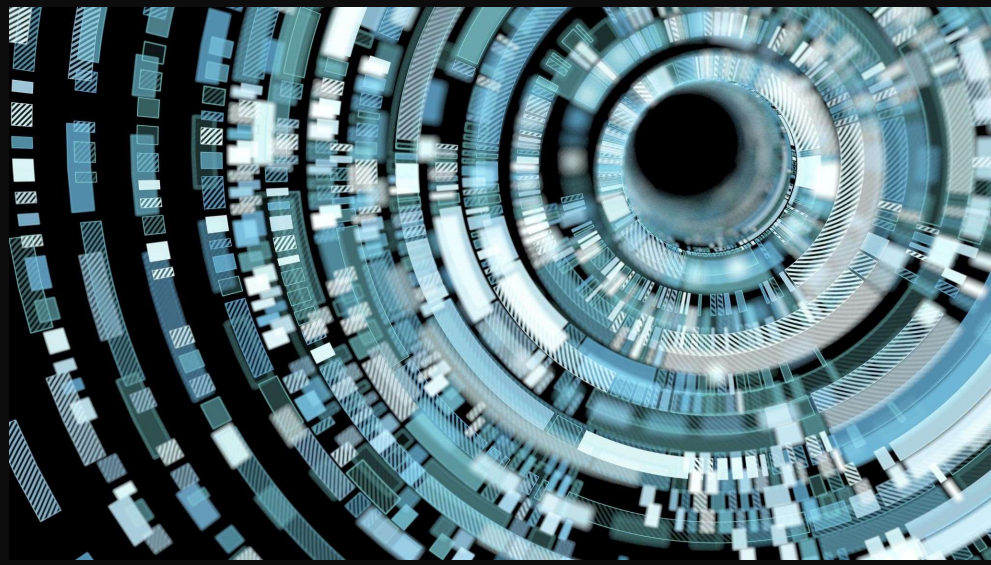
- Artificial Intelligence (AI) is reshaping the cybersecurity landscape. While AI-driven solutions offer enhanced threat detection and automated responses, they also introduce novel vulnerabilities. Adversarial attacks, data poisoning, and model inversion are just a few examples of how AI systems can be compromised. As AI becomes integral to cybersecurity, robust cloud security is indispensable. Furthermore, safeguarding the data AI learns from is paramount.

- ISACA's 2023 State of Cybersecurity report
- AI and Machine Learning in Cybersecurity



Biometrics

- Biometrics offer a new dimension to security. By using unique physical or behavioral attributes, biometrics can enhance identity verification. However, they come with challenges. The use of biometric data, especially in areas like counter-terrorism, raises concerns about privacy and civil liberties. It's essential to strike a balance between security and privacy.



- CSIS - Biometrics and Security

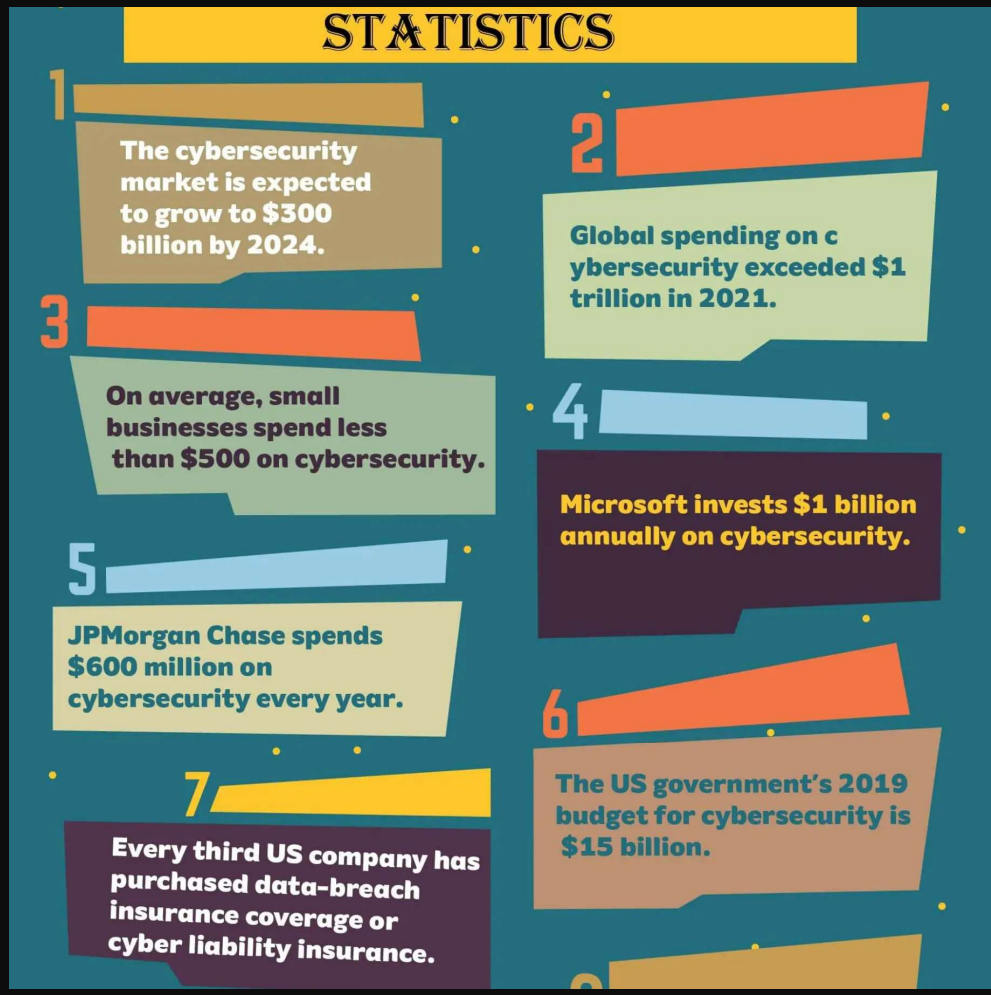
Zero Trust Architecture

- The Zero Trust model operates on the principle of 'never trust, always verify.' In today's complex digital environment, it's crucial to ensure that every user and device is authenticated and authorized before granting access. This approach minimizes the risk of insider threats and data breaches

- BeyondTrust Cybersecurity Trend Predictions 2023

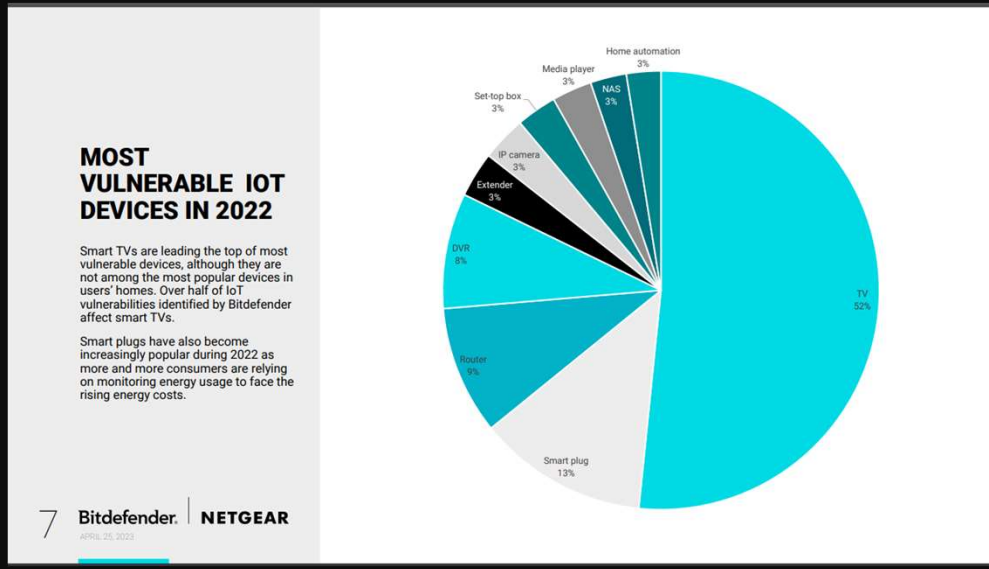
The Cybersecurity Market

- The cybersecurity market is booming. With the rise in cyber threats, there's an increasing demand for specialized services, from threat intelligence to incident response. Companies are investing heavily in cybersecurity solutions to protect their assets and data.



Edge Technologies

- Edge technologies are decentralizing our digital infrastructure. By processing data closer to its source, edge computing offers faster response times. However, this decentralization also presents new security challenges that we must address
  - Autonomous vehicles
  - Drones
  - AR/VR
  - Smart Cities
  - CDNs
  - Remote Healthcare equipment

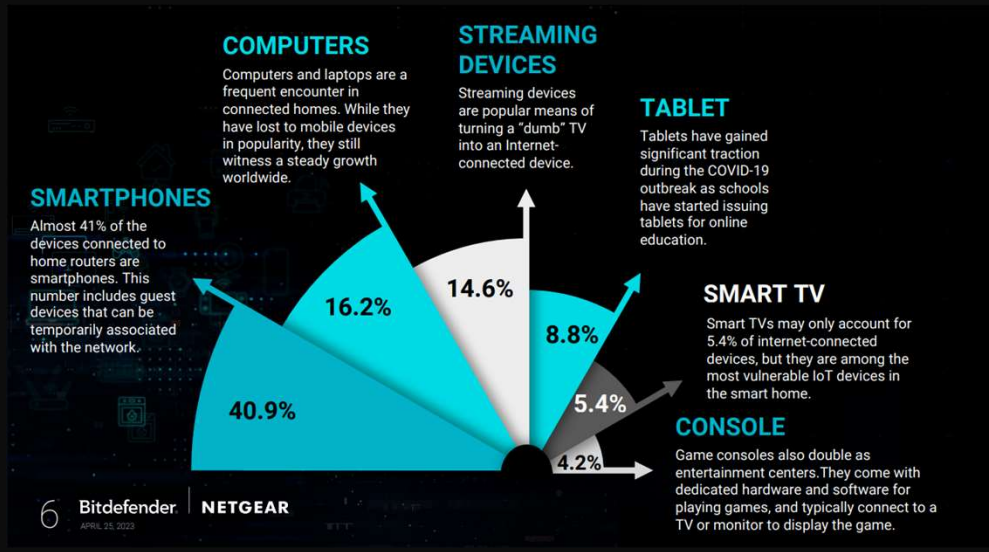


Industries at the Forefront

- Several industries are at the forefront of cybersecurity challenges. Healthcare, automotive, and smart cities, for instance, are grappling with unique threats. From medical device vulnerabilities to car hacking, these sectors need robust cybersecurity solutions

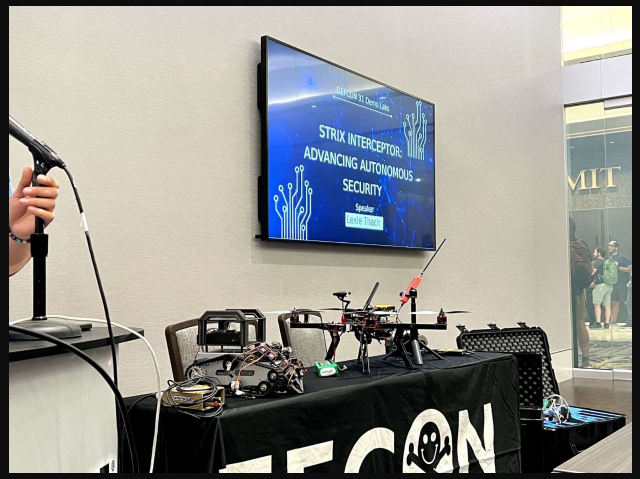
The Role of IoT

- The Internet of Things (IoT) is revolutionizing our world. However, with billions of connected devices, the security challenges are immense. Ensuring the security of these devices is paramount to prevent unauthorized access or data breaches.



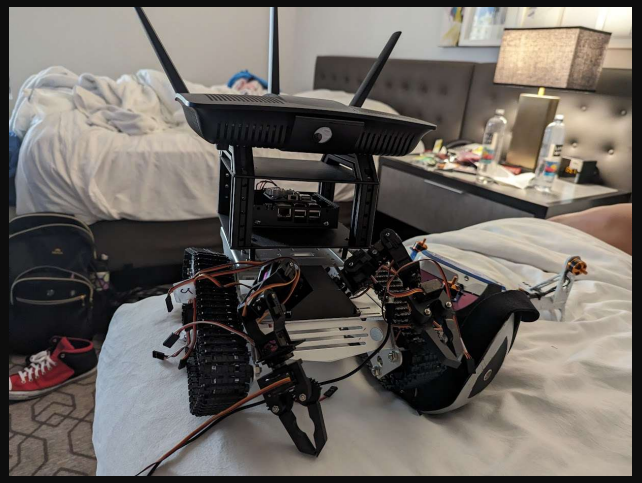
Drone and UAS/UGV Security Concerns and Incidents

- Drones and UAS/UGVs are becoming increasingly popular. While they offer numerous benefits, they also present security challenges. Unauthorized access, data breaches, and physical threats are some of the concerns associated with these technologies.



Robotics and Satellite Systems Security

- Robotics and satellite systems play a crucial role in various sectors. However, they are susceptible to remote hacking attempts and physical tampering. Ensuring the security of these systems is of utmost importance.
- Some notable events:
  - Viasat KA-SAT Network Attack – During Russia's invasion of Ukraine, satellite assets and infrastructure became significant targets. Viasat's KA-SAT network experienced a deliberate attack that affected modems across Europe. (Feb 2022)
  - Starlink Dish Hacking - Lennert Wouters, a cybersecurity expert from KU Leuven University in Belgium, demonstrated that it was possible to hack a Starlink satellite dish. He revealed that it cost him just $25 to acquire the parts for the hack. (Aug 2022)



- Developing an AI-Enabled Cybersecurity Model to Protect Satellite Systems from Cyber Threats
- 10 Defining Moments in Cybersecurity and Satellite in 2022

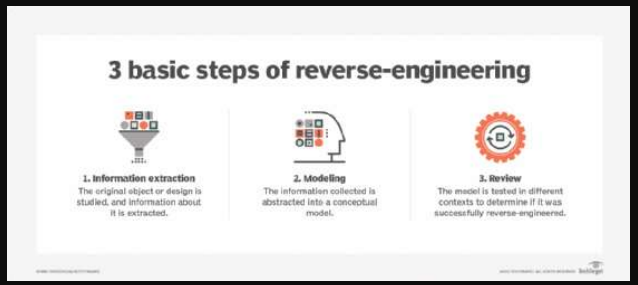
The Cyberpunk Influence

- Cyberpunk fiction has often mirrored or even predicted real-world security trends. From hacking to corporate espionage, the lines between fiction and reality are blurring.
- As cyberpunk warned of unchecked tech's pitfalls, our discussions on AI, IoT, and biometrics echo these cautionary tales. The genre's foresight underscores the importance of proactive cybersecurity in our increasingly digital world.

The Human Element

- Cybersecurity isn’t just about technology; it's about the people behind it. The industry grapples with a staffing challenge, with 59% of leaders indicating their teams are understaffed. This isn’t merely a numbers game; it's about equipping teams with the right skills. Communication, critical thinking, problem-solving, teamwork, and attention to detail are some of the essential skills required in the industry. Skills such as reverse engineering still require a human element.

- [ISACA's 2023 State of Cybersecurity report]



Global Collaboration

- Cybersecurity is a global challenge. International collaboration is essential to address global threats and share best practices. Joint efforts and agreements can pave the way for a more secure digital future

Preparing for the Future

- The future holds promise and challenges. A significant 78% anticipate a surge in demand for technical cybersecurity contributors in the coming year. Concurrently, 48% foresee an increase in the demand for cybersecurity managers. Budgetary considerations are also evolving, with 51% predicting at least a modest increase in the next year. This could be a response to the multifaceted threat landscape, the integration of AI in cybersecurity, and the need for skilled professionals to navigate these challenges.

- ISACA's 2023 State of Cybersecurity report

Conclusion & Call to Action

- In conclusion, the cybersecurity landscape is ever-evolving. It's crucial for all of us to stay informed, proactive, and collaborative. Let's work together to build a secure digital future.

Q&A

Thank you for your attention. I'm now open to any questions you may have.

References

1. Forbes Tech Council. (2023, October 26). *Cybersecurity Awareness Month: What's Still Needed After Twenty Years*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/10/26/cybersecurity-awareness-month-whats-still-needed-after-twenty-years/

2. Deloitte Insights. (2022). *Future of Cybersecurity and AI*. Deloitte. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html

3. TandF Online. (2023). *AI and Machine Learning in Cybersecurity*. Taylor & Francis Online. https://www.tandfonline.com/doi/full/10.1080/23311916.2023.2272358

4. CSIS. (2022). *Biometrics and Security*. Center for Strategic & International Studies. https://www.csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/other-projects-9

5. BeyondTrust. (2022). *BeyondTrust Cybersecurity Trend Predictions 2023*. BeyondTrust. https://www.beyondtrust.com/blog/entry/beyondtrust-cybersecurity-trend-predictions-2023

6. ISACA. (2023). *State of Cybersecurity 2023: Navigating Current and Emerging Threats*. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/state-of-cybersecurity-2023-navigating-current-and-emerging-threats