RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: NCS-T01

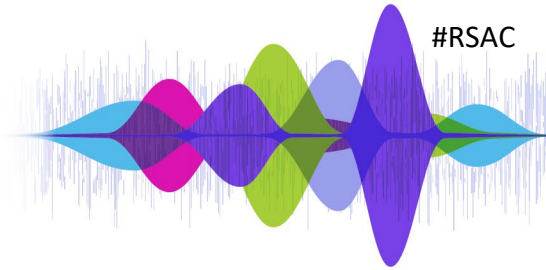
Modern Architectures: Mapping SASE to the Cyber Kill Chain

Niki Portell

Technical Solutions Architect
World Wide Technology
https://www.linkedin.com/in/niki-portell

Lucas Skipper

Technical Solutions Architect
World Wide Technology
https://www.linkedin.com/in/lkskipper



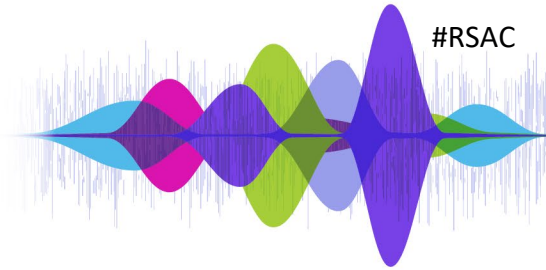
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of their respective employers, the RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.


5.2M USD
21 Days
14K USD/min

Agenda



- Introduction & Relevance
- Historic Network Security Architecture VS Modern Cyber Security Challenges
- What is SASE & SSE?
- The Cyber Kill Chain & How SASE maps
- Different Approaches to SSE/SASE Architectures
- Conclusion & Why Frameworks Matter
- Apply

Ransomware: A Pervasive Threat

19

Average number of ransomware attacks, **every second,** in 2023 **

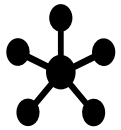
???%

Of organizations globally have experienced ransomware attacks

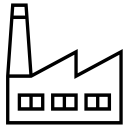
$1.82M

Average cost to remediate in 2023 *

Phishing, Spear Phishing (targeted with urgency)



Scanning (persistent, obfuscated, distributed)



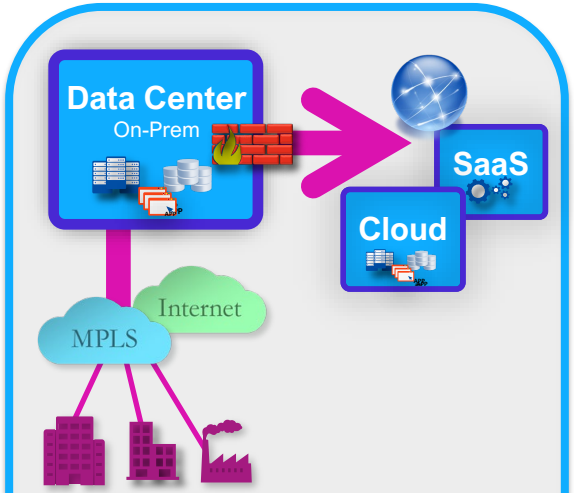
Local access (USB drive, Wi-Fi)

Identity (AD, SaaS)

RSAC 2025 Conference

Historic Network Security vs. Modern Security Challenges

Progression of Network Security Architectures

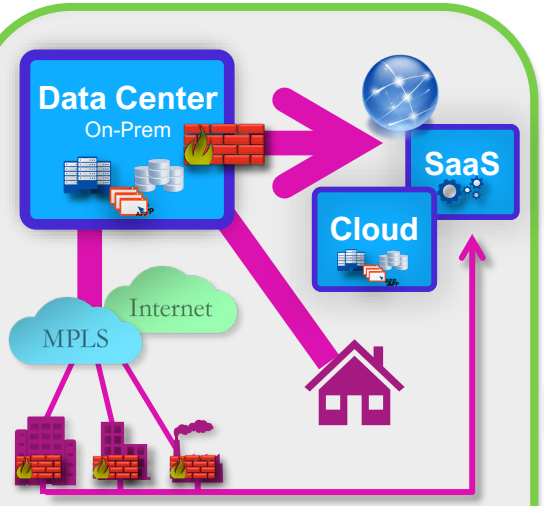


2000's

- **Efficacy:** Lack of Comprehensive Coverage
- **Efficiency:** Tool Sprawl

2006 AWS

2007 NGFW



Early 2010's

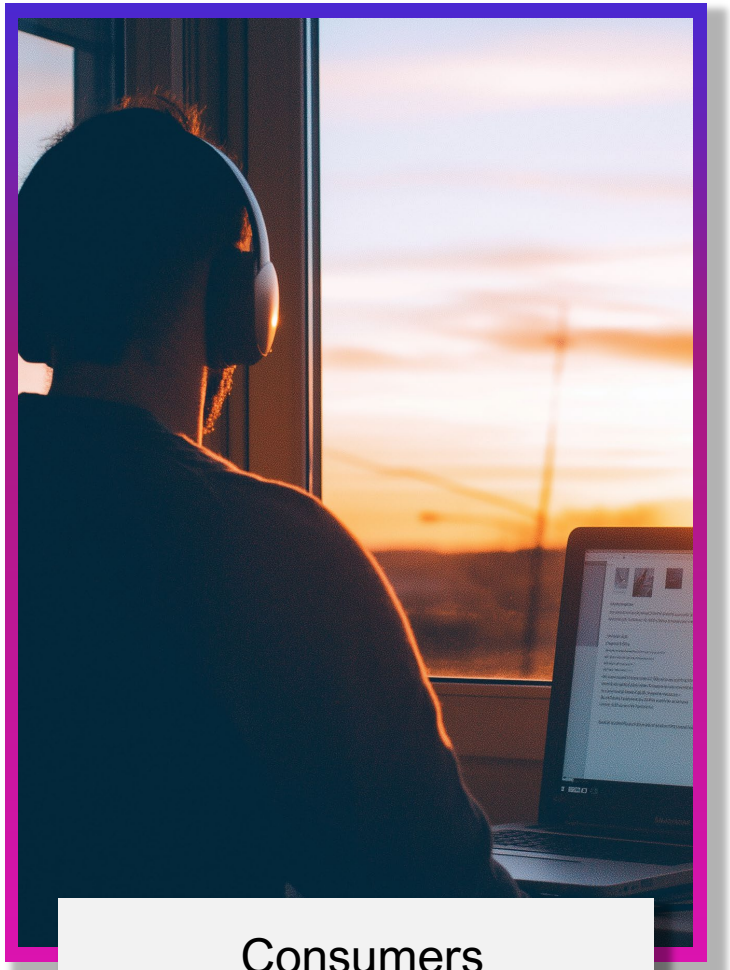
- **Efficacy:** Integration Complexity
- **Efficiency:** Resource Demands

2012 CASB

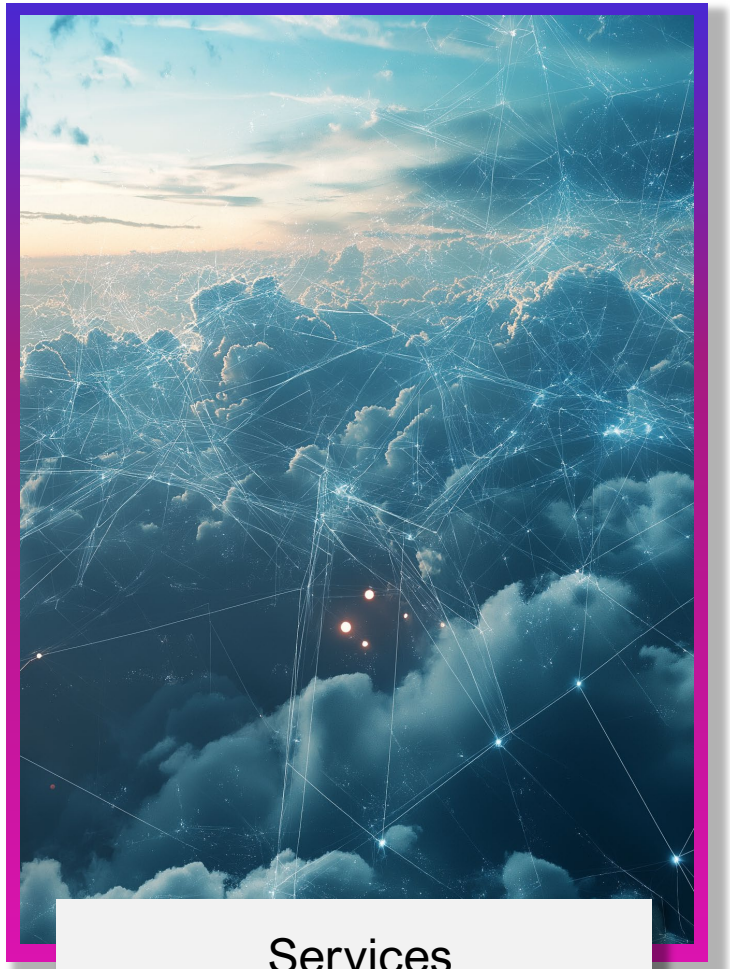
Today

As the needs of our organizations evolve, how do we adapt?

Everything is Everywhere



Consumers
(Users, Contractors, Headless Devices)



Services
(Applications, Data Storage, Internet)

Threats
(Insider Threats, Third-Party Threats, Lateral Movement)

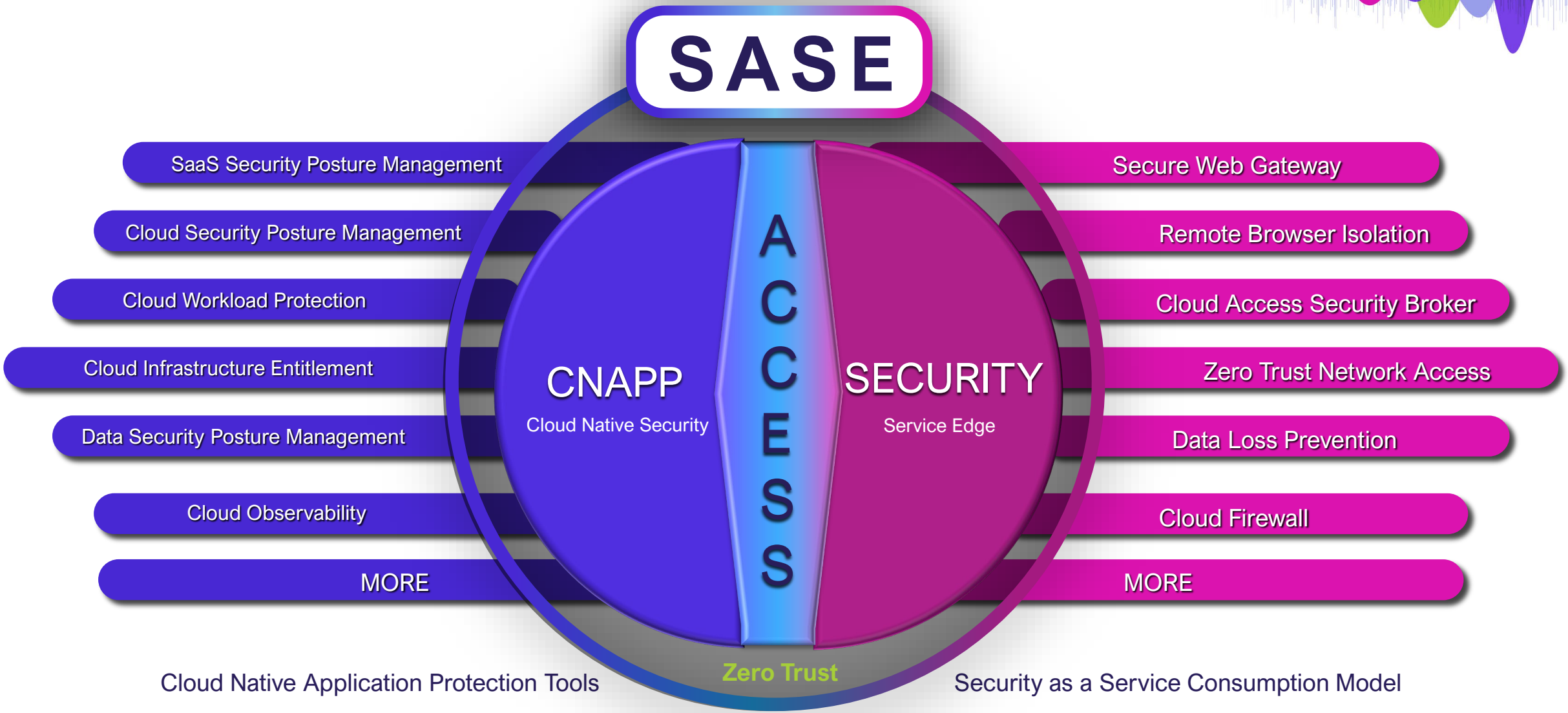
Traditional Security Strategies do not effectively address these use cases

RSAC™ 2025 Conference

What is SASE?

Many Voices.
One Community.

Secure Access Service Edge



Cloud Native Application Protection Tools

Security as a Service Consumption Model

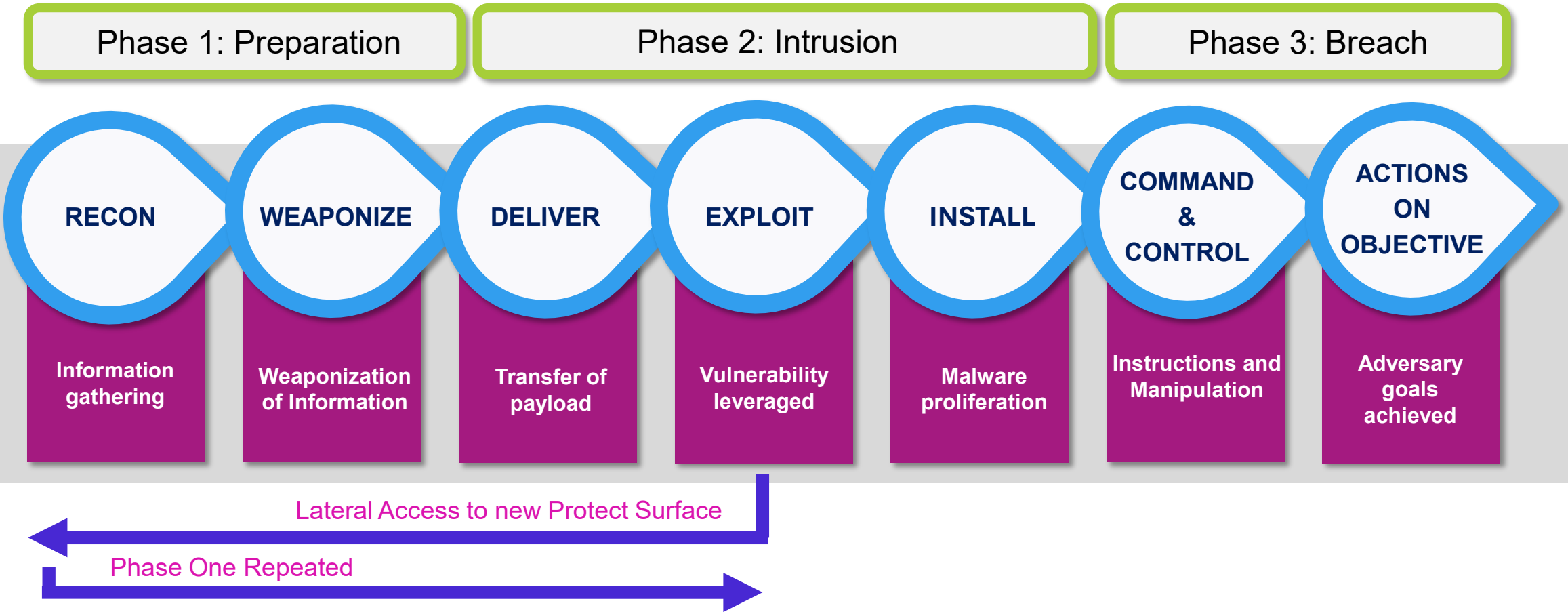
RSAC 2025 Conference

Cyber Kill Chain

Overview and Mapping Exercise

Many Voices.
One Community.

The Cyber Kill Chain: Attacker's View



Phase 1: Attacker's Perspective

Reconnaissance

We will add a decoy address to obfuscate:
-D <*decoy1*>[,<*decoy2*>][,ME]

We may also spoof our source address and port:

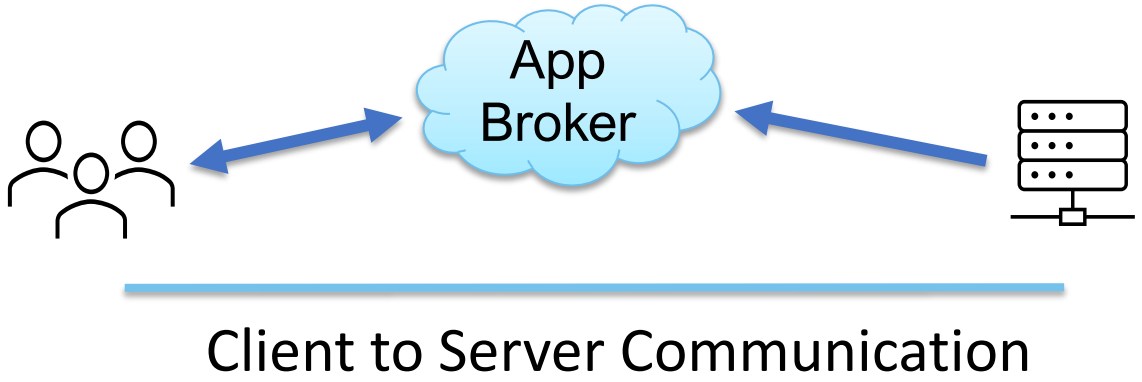
-S <*IP_Address*>
--source-port <*portnumber*>

- Scanning with obfuscation

```
[root@research scripts]# nmap -Pn --script vuln testphp.vulnweb.com -p 8443
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-25 11:09 -03
Nmap scan report for testphp.vulnweb.com (176.28.50.165)
Host is up (0.29s latency).
rDNS record for 176.28.50.165: rs202995.rs.hosteurope.de
```

Phase 1: Defender's Perspective

Reconnaissance



- ✓ Zero Trust Principles
- ✓ Proxy ZTNA: Inside-Out Connection *or*
- ✓ Network ZTNA: Ingress access managed by SSE provider (IP/DNS)

Phase 1: Attacker's Perspective

Weaponization

Sharing CVEs: (iSee857, 2025)

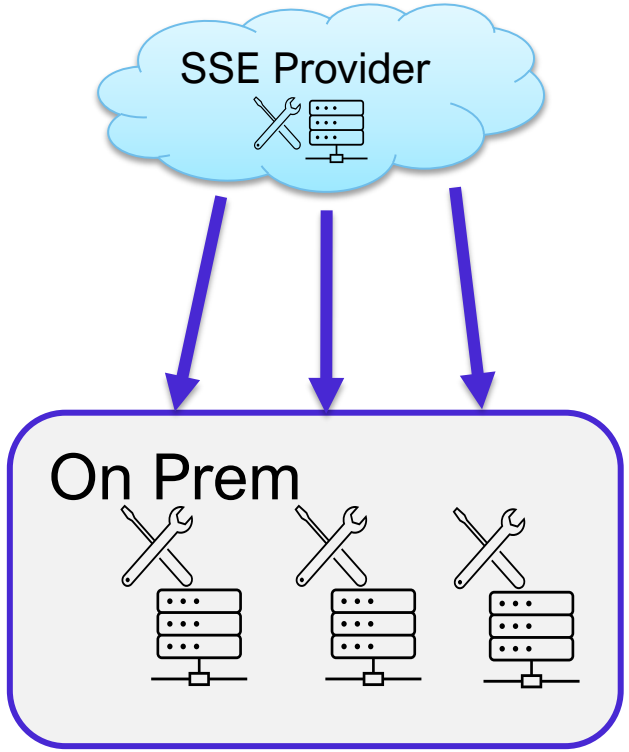
- CVE for web management UI

Phase 1 Preparation → Phase 2 Intrusion → Phase 3 Breach

Phase 1: Defender's Perspective

Weaponization

- ✓ Staying ahead of threats
  - ✓ Automated management & patching
- ✓ Secure 3rd party access
  - ✓ Agent *or* Browser



Phase 1 Preparation → Phase 2 Intrusion → Phase 3 Breach

Phase 2: Attacker's Perspective

Delivery &

Exploit

Delivery:

- PHP Script Injection authentication bypass
- Chain CVEs together to gain admin access

Exploit:

- Modify logging/alerting
- Setup persistent access (tunnel)
- Repeat phase 1 from new vantage point
  - AD recon > exploit
  - Vulnerable Hypervisor

Phase 2: Defender's Perspective

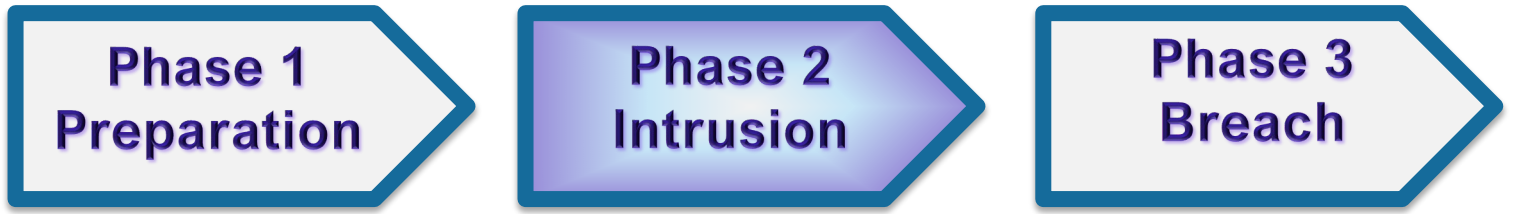
Delivery & Exploit

Delivery:

- ✓ Behavior Monitoring
- ✓ Web App Security
  - ✓ OWASP Top 10
  - ✓ Cloud Firewall (IPS)
- ✓ Remote Browser Isolation

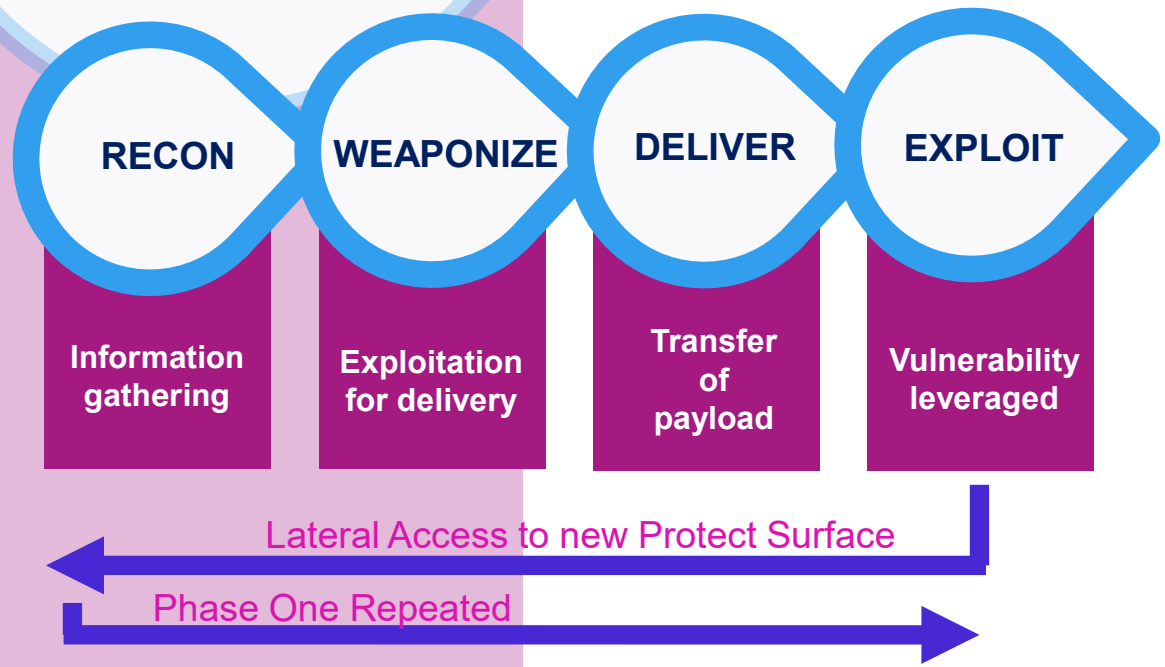
Exploit:

- ✓ SSE provider logging and auditing
- ✓ Centralized Observability
  - ✓ Integration with SIEM/SOAR
- ✓ No "low hanging fruit"



Phase 2: Attacker's Perspective

Exploit (Continued)

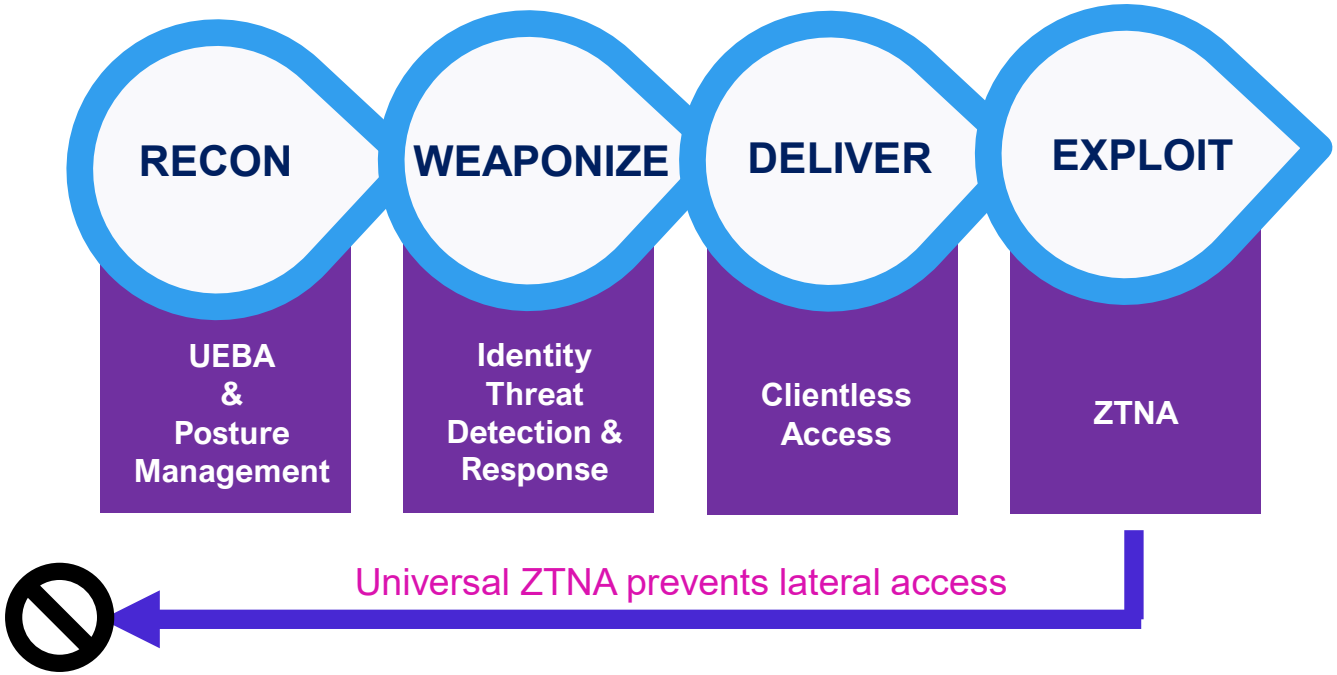


- Phase 1 repeats
- Identity-based recon
  - Misconfiguration in ADCS
  - Kerberos "roasting" attack
    - Privilege escalation to create ESX Admins group (CVE-2024-37085)
      - Hypervisor admin access

Phase 2: Defender's Perspective

Exploit (Continued)

- ✓ Policies based on Identity
- ✓ Universal ZTNA
  - ✓ Always On
  - ✓ Stop Lateral Movement
  - ✓ Least Privilege Access

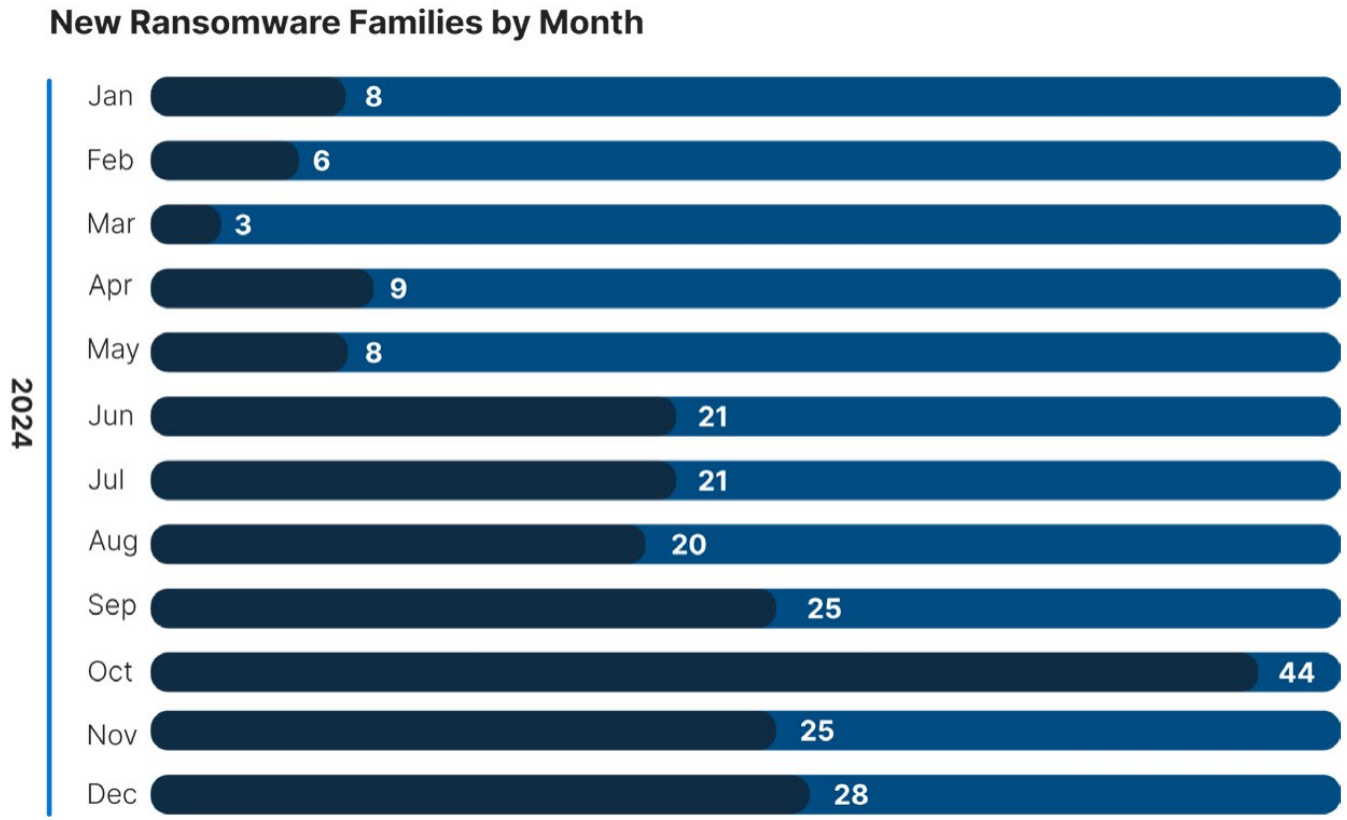


Phase 1 Preparation → Phase 2 Intrusion → Phase 3 Breach

Phase 2: Attacker's Perspective

Installation

- Leveraging Ransomware as a Service
  - Lockbit 3.0 builder



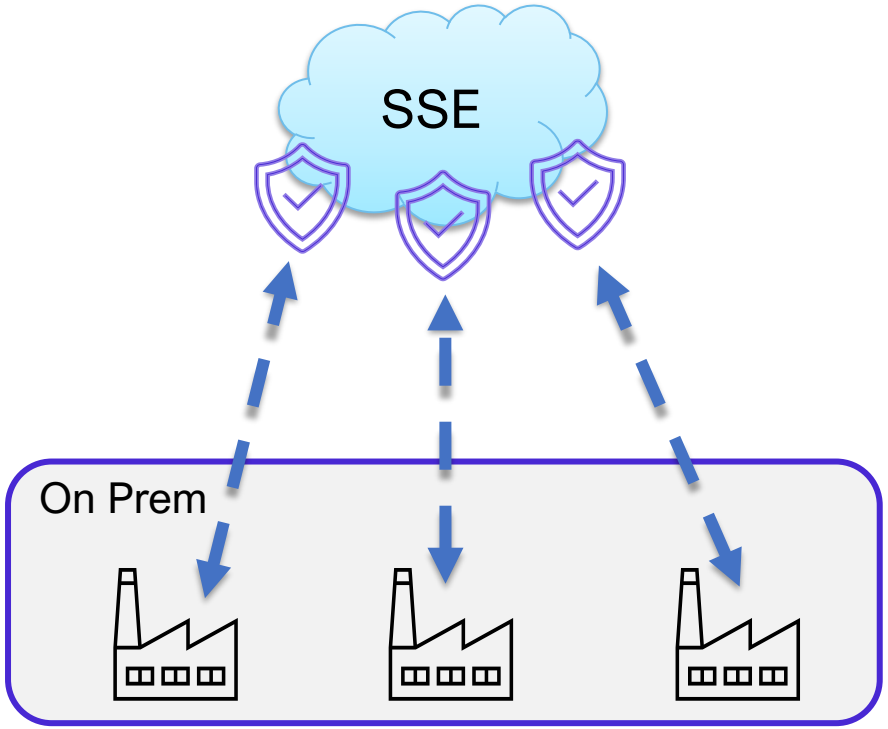
(Recorded Future, 2025)

Phase 1 Preparation → Phase 2 Intrusion → Phase 3 Breach

Phase 2: Defender's Perspective

Installation

- ✓ SWG with Malware Sandboxing
- ✓ Applying Zero Trust to Non-humans
- ✓ Integrations with Endpoint Monitoring and Protection tools



Phase 1 Preparation → Phase 2 Intrusion → Phase 3 Breach

Phase 3: Attacker's Perspective

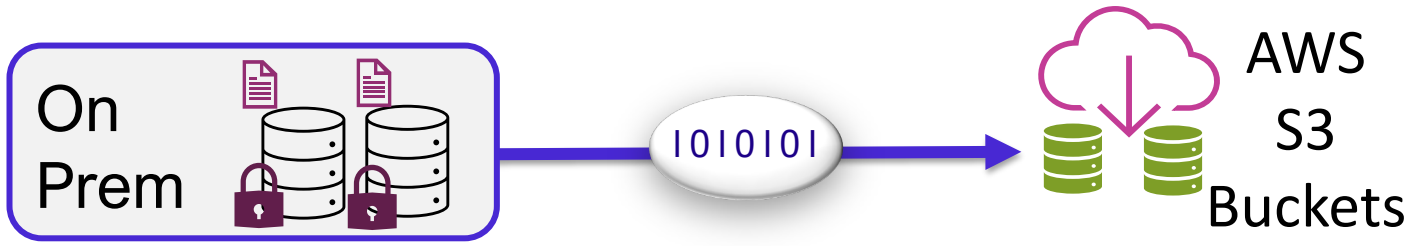
C2 & Actions on Objectives

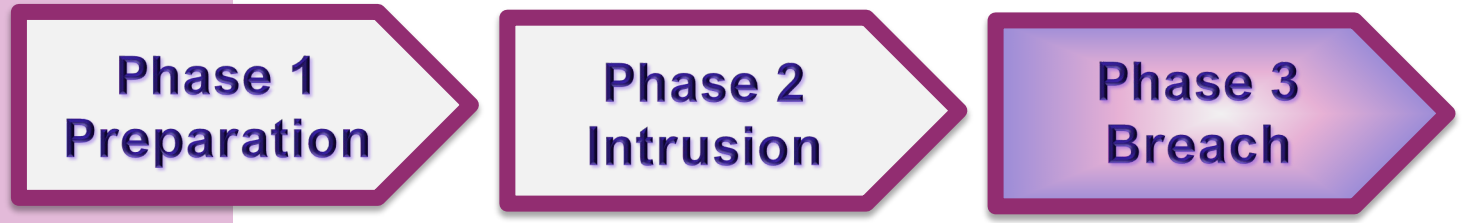
Command and Control (C2):

- Instructions and Payloads sent for exfiltration to S3 buckets
- Instructions and payload sent to encrypt and ransom

Actions on Objectives:

- Data exfiltration completed
- Encrypt and ransom





Phase 3: Defender's Perspective

C2 & Actions on Objectives

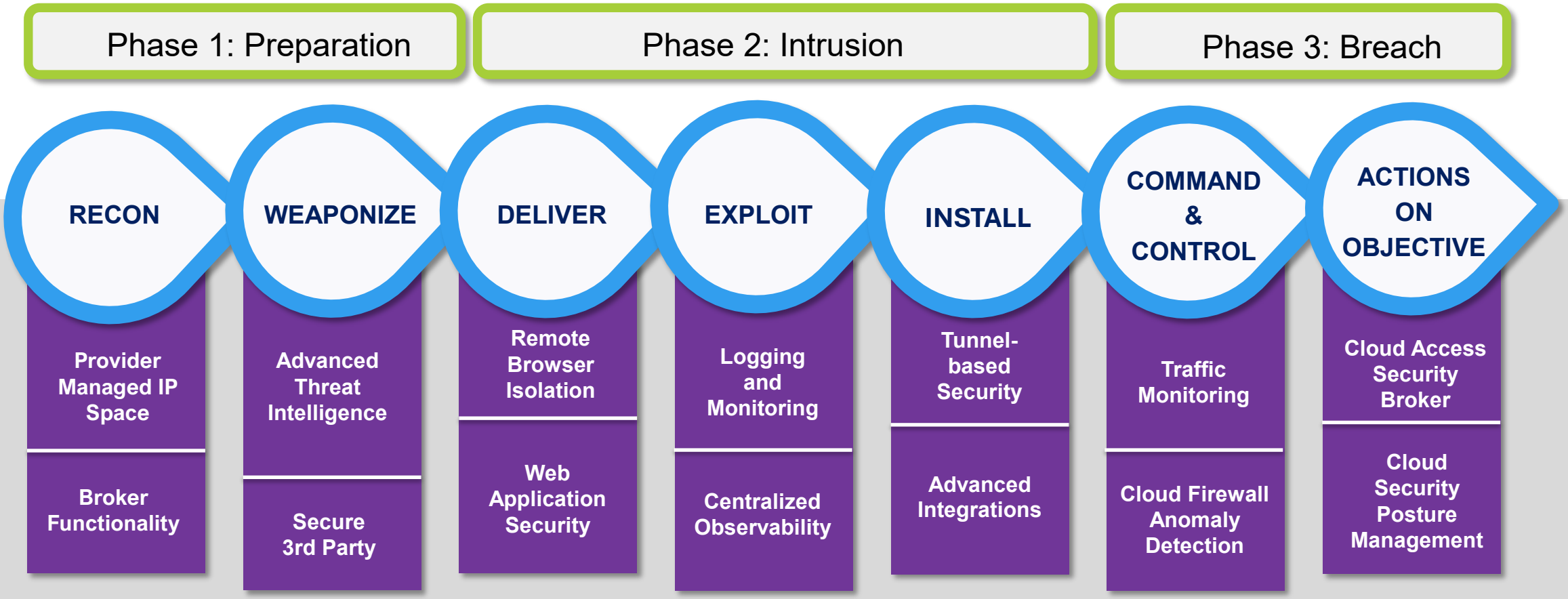
Command and Control (C2):

- ✓ Traffic Decryption at Scale
- ✓ Cloud Firewall
- ✓ Anomaly Detection

Actions on Objectives:

- ✓ Cloud Access Security Broker (CASB)
  - ✓ Data Loss Prevention (DLP)
- ✓ Cloud Security Posture Management
  - ✓ Posture Checking
  - ✓ Alerting
  - ✓ Auditing

The Cyber Kill Chain: Defender's View



From a **single**, **cloud delivered**, **zero trust**, policy enforcement point

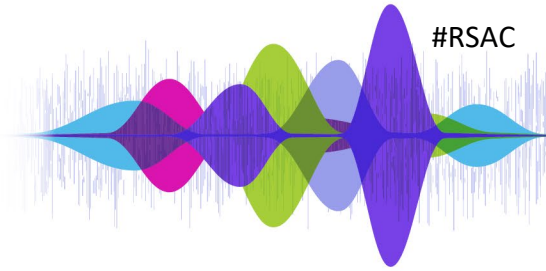
RSAC 2025 Conference

Different Approaches to SSE/SASE Architecture

Network, Proxy, Multi-Vendor, Single Vendor, Unified

Many Voices.
One Community.

Network vs. Proxy ZTNA

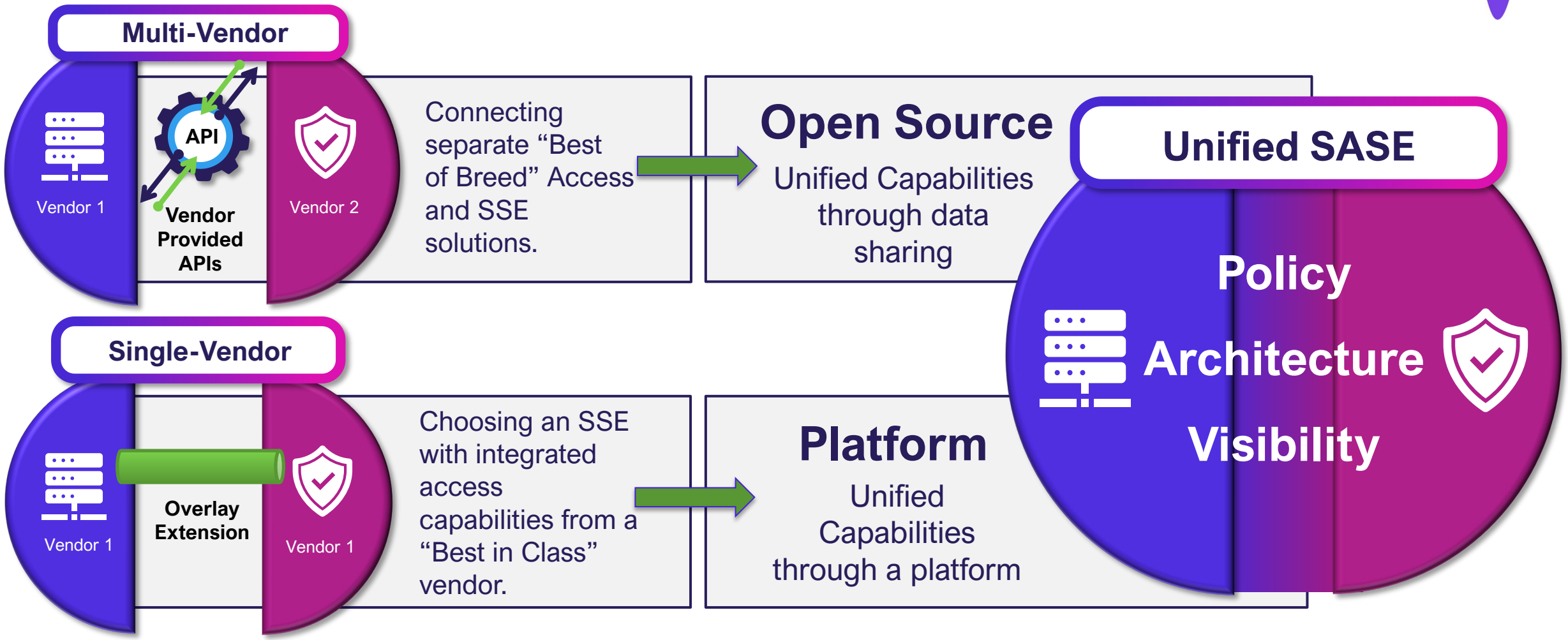


Network	Proxy
Tunnel Based Configuration	App Based Configuration
Dedicated Infrastructure	Shared Infrastructure
Inbound And Outbound Connectivity	Outbound Only Connectivity
Any App Any Port Support	App Support Considerations
Flexible Traffic Engineering	Proxy Managed Traffic
Lateral Movement Risk	Improper Usage Risk

VS

*Today's modern architecture is moving towards a full hybrid approach.

SASE Models & Vision



RSAC 2025 Conference

Conclusion

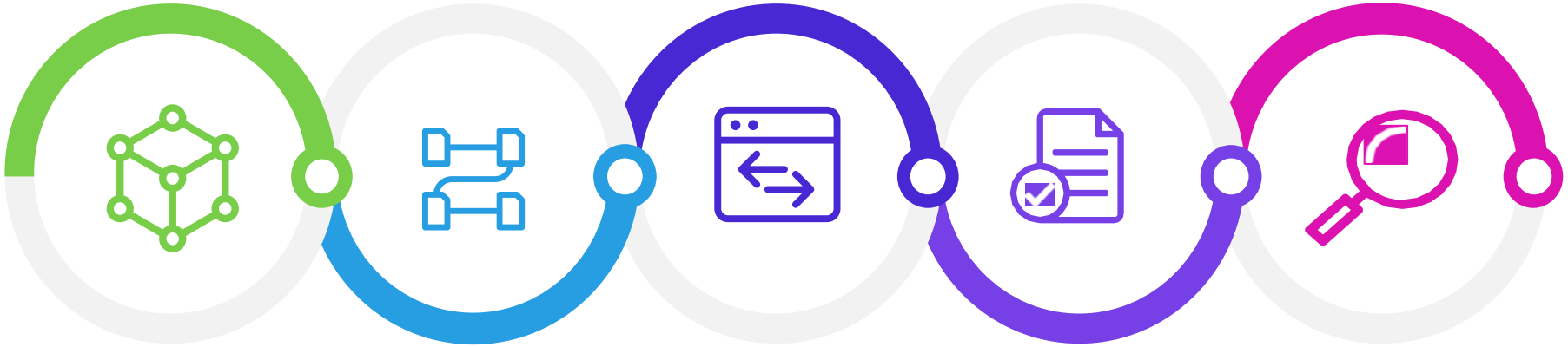
Why Frameworks Matter

Many Voices.
One Community.

Zero Trust Tactics: A Phased Approach

Map
Transaction Flows

Create Zero Trust
Policy



Define Protect
Surface

Build a Zero Trust
Architecture

Monitor and Maintain
the Environment

Apply What You Have Learned Today

Next Week

- Begin to identify protect surfaces
- Create common vocabulary
- Identify tools for Red Teaming
- Chose a framework to map business outcomes

3 Month Goal

- Have a roadmap for use-case adoption covering tactical and strategic milestones
- Begin evaluating security solutions that meet your requirements to transition and transform

6 Months & Beyond

- Begin implementing the candidate solution monitoring progress of each use-case aligned to the roadmap
- Ensure integrations map to unified observability strategies
- Expand strategy to additional protect surfaces

Regularly scheduled meetings for Governance Council to assess gaps

Tabletop/Cyber Range exercises, board education, policy reviews, use case mapping

Foundational Elements Throughout

RSAC™ 2025 Conference

Many Voices.
One Community.

Q&A

Reach out to us at:

https://www.wwt.com/profile/nicole-portell/bio

https://www.wwt.com/profile/lucas-skipper/bio

Bibliography

- Baran, G. (2025, February 13). *Massive IoT Data Breach*. Cyber Security News. Retrieved February 19, 2025, from https://cybersecuritynews.com/massive-iot-data-breach/
- Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023, September). *Guide to Operational Technology (OT) Security*. NIST Computer Security Resource Center. Retrieved February 19, 2025, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf
- Kulkarni, S., & Roza, M. (2024, March 5). *Defining the Zero Trust Protect Surface*. Cloud Security Alliance. Retrieved February 19, 2025, from https://cloudsecurityalliance.org/artifacts/defining-the-zero-trust-protect-surface
- Lefebvre, H., Legner, C., & Teracino, E. A. (2024, November 24). *5 Pillars for Democratizing Data at Your Organization*. Harvard Business Review. Retrieved February 19, 2025, from https://hbr.org/2023/11/5-pillars-for-democratizing-data-at-your-organization
- (2022). *The Cyber Kill Chain*. Lockheed Martin. Retrieved February 19, 2025, from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- iSee857 (2025, February 12). *CVE-2025-0108-PoC*. Github. Retrieved February 21, 2025, from https://github.com/iSee857/CVE-2025-0108-PoC?tab=readme-ov-file

Bibliography

- Fitch, S. C., & Muckin, M. (2019, February 24). *Defendable Architectures*. Lockheed Martin. Retrieved February 19, 2025, from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Defendable-Architectures.pdf
- Chen, J. (2021, October 28). *Network Scanning Traffic Observed in Public Clouds*. Unit 42. Retrieved February 20, 2025, from https://unit42.paloaltonetworks.com/cloud-network-scanning-traffic
- Kime, C. (2023, July 14). *How To Use Nmap for Vulnerability Scanning: Complete Tutorial*. eSecurity Planet. Retrieved February 20, 2025, from https://www.esecurityplanet.com/networks/nmap-vulnerability-scanning-made-easy/
- Lyon, G. (2022). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Nmap. Retrieved February 20, 2025, from https://nmap.org/book/toc.html
- Borges, E. (2020, May 26). *How to Detect CVEs Using Nmap Vulnerability Scan Scripts*. SecurityTrails. Retrieved February 20, 2025, from https://securitytrails.com/blog/nmap-vulnerability-scan
- https://www.trmlabs.com/post/ransomware-in-2024-latest-trends-mounting-threats-and-the-government-response#:~:text=In%202024%2C%20ransomware%20payments%20and,just%20payments%20that%20have%20accelerated
- Source: John Kindervag, ON2IT BV, “NSTAC ZT Briefing,” Briefing to the NSTAC (ZT-IdM) Subcommittee. Arlington, VA, September 8, 2021.

Bibliography

- Rollin, B. (2023, March 29). *Active directory pentesting: Cheatsheet and beginner guide*. Hack The Box. Retrieved February 21, 2025, from https://www.hackthebox.com/blog/active-directory-penetration-testing-cheatsheet-and-guide
- Remmons-r7 (2024, July 29). *CVE-2024-37085*. AttackerKB. Retrieved February 21, 2025, from https://attackerkb.com/topics/2lIWJbMF0o/cve-2024-37085
- Walter, F. (2024, February 8). *The Easiest Way to Find CVEs at the Moment? GitHub Dorks!* Medium. Retrieved February 21, 2025, from https://medium.com/@dub-flow/the-easiest-way-to-find-cves-at-the-moment-github-dorks-29d18b0c6900
- Insikt Group (2025, January 28). *2024 Annual Report*. Recorded Future. Retrieved February 27, 2025, from https://www.recordedfuture.com/

Bibliography

- (2024, April 1). *The State of Ransomware 2024*. Sophos. Retrieved February 28, 2025, from https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf
- Palatty, N. J. (2025, January 9). *100+ Ransomware Attack Statistics 2025: Trends & Cost*. Getastra. Retrieved February 28, 2025, from https://www.getastra.com/blog/security-audit/ransomware-attack-statistics/
- (n.d.). *2024 Thales Data Threat Report*. Thales Group. Retrieved February 28, 2025, from https://cpl.thalesgroup.com/data-threat-report