ILTA EVOLVE

27 - 30 APRIL 2025 | MYRTLE BEACH, SC

The Kill Chain Reimagined: Starting with the Attacker's End Game

Why the Traditional Kill Chain Falls Short

John Anthony Smith

Founder & Chief Security Officer

Fenix24/Conversant Group

CONVERSANT GROUP

FENIX24

Agenda

- Introductions
- Statistics: Mass/Backup Destruction & Lateral Movement Readiness
- Key Components of the Cyber Kill Chain (Lockheed)
- Why the Kill Chain Falls Short
- Cyber Kill Chain Path: MITRE ATT&CK, NIST, CIS
- High Profile Beaches in the News
- Flipping the Script: Reimagining the Kill Chain
- Surviving a Breach: Breach Context and Pattern
- Hardening in Reverse
- Actions You Can Take Now
- Q&A

Meet the Speaker: John Anthony Smith

Founder & Chief Security Officer, Fenix24/Conversant Group

- **Founder & Chief Security Officer of Fenix24 (a Conversant Group company) and five other tech companies.**
- **Information security fanatic and thought leader with many publications and speaking engagements.**
- **Deep experience with companies in several highly sensitive industries, such as healthcare, financial services, defense, and legal.**
  - **Has overseen the design, build, and/or management of infrastructure for over 500 companies.**
  - **Currently serving as a vCIO and trusted advisor for several companies.**
  - **Former Director of IT for a law firm.**
  - **Designed the ILTA first annual cybersecurity benchmarking survey.**
  - **Worked with law firms all over the world: USA, UK, Australia, New Zealand, Netherlands, Japan.**
- **Led his first breach response over 13 years ago and sadly many more since.**
- **Fervent believer in locating, investigating, and prosecuting cybercriminals.**

WE ARE ON THE BATTLEFIELD EVERY DAY GATHERING REAL-TIME INTELLIGENCE OTHERS CANNOT

Fenix24 is on the front lines every day, battling cyber terrorists through isolation, eradication & recovery, allowing unique insights into constantly changing threat actor tactics.

Athena7 constantly assesses the infrastructure and technical controls' orchestration & capabilities firms are currently using to resist threat actor behaviors and recover from destructive acts.

Grypho5 leverages data from current threat actor tactics (from Fenix24) and orchestrates proven defensive and recovery strategies & tactics to offer the most comprehensive and evolving managed protection.

Argos99 increases cyber resilience and incident recovery by providing companies with expert insights into their own assets, infrastructure, and control configuration improving assured recovery and rigorous resistance.

Console Segmentation and Readiness: By the Numbers

Fenix24's Athena7 battalion found...of assessed organizations:

- **73%** have critical consoles assessable from user segments
- **100%** have critical consoles co-joined to production AD
- **55%** had non-existent or non-restricted MFA
- **45%** had access to IPMI/iLO/iDRAC
- **65%** had same consoles AD joined
- **87%** had no IP restrictions on publicly accessible systems

Console Segmentation and Readiness: Risks Abound

Athena7 assessments showed that nearly all had these risks…

- Using daily driver accounts from production AD for critical console access
- Allowing credential caching in browsers
- Allowing IT password vaults to be production AD SSO joined
- Allowing prod AD joined IT password vaults to store critical console creds, such as break glass
- Having self-service password (users & admins) reset enabled
- No lateral movement protections for admin functions (e.g., MMC, WMI, RDP, PowerShell)
- No admin segment/VLAN for critical consoles
- Critical consoles accessible from production AD creds
- Immutability is not configured, and if it is, it will likely not hold up in breach as configured

EVERYONE THINKS BACKUPS WILL SURVIVE. But Reality Serves Up a Wake-Up Call.

Fenix24 Intel from 2000+ Breaches, 92% From Past 90 Days Experience Some Form of Loss (78 breaches YTD)

84% Critical backups did not survive threat actors' behavior	*Of the 16% that survive…*	**Only 50%** Of backups that survive cannot provide a suitable recovery timeline	*And even when ransom is paid…*	**Only 33%** Of the data will be unrecoverable — corrupted / damaged / deleted

Athena7 Intel

90% Cannot meet their stated RTOs	**Only 86%** Have no survivable backup copies	**76%** Knowingly do not have all known critical data backed up

Key Components of the Cyber Kill Chain (Lockheed)

Reconnaissance. The attacker gathers information about the target organization or system to identify weaknesses to exploit later.

Weaponization. The attacker prepares their payload, coupling with a RAT, virus, or exploit to prepare a weapon that can deliver malicious code effectively.

Delivery. The attacker sends the weaponized payload to the target (phishing emails, drive-by downloads) to gain access to the target environment.

Exploitation. The malicious payload is executed, exploiting vulnerabilities in the target system, triggering zero-day or known exploits.

Installation. The attacker installs malware or backdoors to maintain persistence (trojans, keyloggers, or ransomware), setting up command-and-control beacons.

Command-and-Control. The attacker establishes communication channels to control the compromised system remotely to control and orchestrate attacks.

Actions and Objectives. The attacker fulfills goal of data theft, destruction, or disruption via data encryption/exfiltration, sabotaging systems.

Top Reasons Why the Kill Chain Falls Short

Reconnaissance. It is in fact true that attackers do reconnaissance using data from social media, breaches, news, etc.

Weaponization. It is, true, that most threat actors have malicious intent; however, it is not commonly true that they are using viruses, malicious code, and RATs---commercially available, allowed methods are the most common means.

Delivery. The "weaponized payload" is commonly available commercialized remote access and penetration testing tooling or IT administrative methods, such as TeamViewer, Bomgar, N-Able, ScreenConnect, LogMeIn, WinSCP, Kerberoast, Metasploit, PowerShell, RMM, EDR, etc.

Exploitation. Interestingly, exploitation of "vulnerabilities" may be involved—but rarely; however, it is lack of or poorly orchestrated configuration that leads to execution of malicious behaviors. As a simple example, most breaches involve lateral movement by critical console access, PowerShell, and RDP.

Installation. Persistence is involved in many breaches; however, not all. Persistence is commonly orchestrated with commercially available tooling. Malware, in the traditional since, is not commonly deployed.

Command-and-Control. Commercially available tooling and reverse proxy platforms are commonly employed. As an example, Teleport was very common 12 months ago.

Actions and Objectives. Exfiltration is common to most breaches; however, what is commonly misunderstood is that TAs not only encrypt but DELETE data.

Top Reasons Why the Kill Chain Falls Short

Linear, Static Model. Modern attacks are dynamic, iterative, and active---human-led.

Focus on Perimeter Defense. Heavy focus on preventing initial access allows threat actors to bypass perimeter defense. Tactics: living off the land (LOTL), phishing, insider threats.

Lack of Post-Exploitation Focus. Emphasis on stopping attackers early. Modern attacks persist and adapts post-exploitation, maintaining stealthy access, pivoting across networks---commercial tooling.

Assumes Single Vector Attacks. Adversaries use multi-vector attacks (e.g., phishing + lateral movement + privilege escalation).

Ignores Insider Threats. Security teams focus on external adversaries. However, threat actors commonly gain access to sensitive controls and ingress points, appearing like an insider.

Failure to Address Common Cloud & Hybrid Environments. Modern attacks target cloud, SaaS, and hybrid infrastructures, requiring different detection and response strategies.

Top Reasons Why the Kill Chain Falls Short

Failure to Address Common Cloud & Hybrid Environments. Kill chain was designed for on-premise environment. Modern attacks target cloud, SaaS, and hybrid infrastructures, which require different detection and response strategies.

Understanding Defense Evasion Techniques. Assumption that detection occurs in early stages, but the reality is attackers use "user" & commercially available methods to access systems & data, such as VPN, Citrix, Horizon, TeamViewer, ScreenConnect, etc.

Inability to Handle Lateral Movement. Minimal focus on movement within the network post-breach allows attackers to leverage credential harvesting, pass-the-hash, and kerberoasting (a technique to obtain a password hash of an Active Directory account).

Delayed Detection & Response. Kill chain disruption tactics prioritize prevention & detection. However, assumption of breach first focuses on recovery as a primary means of disruption.

Misses Targeted Attacks & Advanced Persistent Threats (APTs). Assumption of mass-scale attacks, with predictable patterns, allows customize attacks based on target environments, staying undetected for months.

Cyber Kill Chain Path: MITRE ATT&CK Framework

Reconnaissance (Pre-ATT&CK). Scanning for open ports and vulnerabilities, sourcing employee information.

Initial Access. Gaining entry into the target system or network (spear phishing, exploiting public-facing apps)

Execution. Running malicious code on a target system (scripts, malware, malicious attachments).

Persistence. Maintaining access despite reboots, credential changes (creating new accounts, modifying scripts).

Privilege Escalation. Gaining higher-level permissions, such as by exploiting vulnerabilities to gain admin rights.

Defense Evasion. Avoiding detection by disabling security tools and obfuscating scripts/files to impair defenses.

Credential Assess. Stealing account names and passwords by keylogging and dumping password hashes.

Discovery. Identifying internal network resources, such as scanning internal networks, querying system information.

Lateral Movement. Moving within the network through remote desktop sessions and exploiting trust relationships.

Collection. Gather targeted data by collecting files and data bases (data from local systems, screen capture)

Command and Control (C2). Communicating with compromised systems (use of C2 servers, encrypted channels)

Exfiltration. Steal and move data (FTP uploads, encrypted data transfers)

Impact. Damaging or disrupting IT networks via ransomware, data destruction, disk wipe

Cyber Kill Chain Path: NIST Cybersecurity Framework (CSF)

#	Kill Chain Phase	Description	Example Activities
1	Reconnaissance	Gathering info about target organizations/systems	Open-source intelligence (OSINT) scanning, social engineering prep
2	Weaponization	Creating malicious payloads/tools	Crafting
3	Delivery	Transmitting payload to victim	Spear phishing, drive-by downloads, USB drops
4	Exploitation	Executing Code to exploit vulnerabilities	Exploit software, trick users into opening files
5	Installation	Installing malware to maintain access	Remote Access Trojans (RAT) setup, backdoors
6	Command & Control (C2)	Establishing communication to attacker infrastructure	C2 over HTTP(S), DNS tunneling, encrypted channels
7	Actions on Objectives	Achieving attack goals (data theft, disruption, destruction)	Data exfil, system destruction, ransomware execution

Cyber Kill Chain Path: Center for Internet Security Controls (CIS)

#	Kill Chain Phase	Description	Example Activities
1	Reconnaissance	Adversary gathers information on target system / network	Inventory and control of enterprises assets / software assets
2	Weaponization	Create / weaponize malicious payloads	Data protection; malware defenses
3	Delivery	Transmit malicious content to target environment	Emails and web browser protections; network monitoring and defense
4	Exploitation	Exploit vulnerabilities to execute code	Continuous vulnerability management; penetration testing
5	Installation	Install malware or establish persistence	Secure configuration of enterprise assets and software; audit log management
6	Command and Control (C2)	Establishing C2 channels to communicate with compromised systems	Data recovery and resilience; network monitoring and defense
7	Actions on Objectives	Achieve attack goals (exfiltration, disruption, destruction)	Account/access control/network infrastructure management

High-Profile Breaches in the News

July 2025: Walt Disney Co. Slack Accounts Hacked	September 2022: Uber Slack Workspace, Internal Tools Targeted
• Hacker group NullBulge claims responsibility for breach. • Disney employee downloads malware disguised as AI tool. • Attacker gains access to login credentials and infiltrates Disney's Slack environment. • Attacker accesses and leaks over 1.1 TBs of data, compromising 44 million+ Slack messages, exposing sensitive company data.	• Hacker group Lapsus$ compromises Uber contractor's account by likely purchasing their corporate password on the dark web after contractor's personal device is infected with malware. • Attacker contacted contractor via WhatsApp, impersonating Uber's IT support, convincing contractor to approve MFA request and thereby granting access. • Attacker accesses Uber's Slack, other systems.
https://www.msn.com/en-us/news/technology/a-disney-worker-downloaded-an-ai-tool-it-led-to-a-hack-that-ruined-his-life/ar-AA1zOQRm	https://www.theregister.com/2022/09/16/uber_security_incident/

High-Profile Breaches in the News

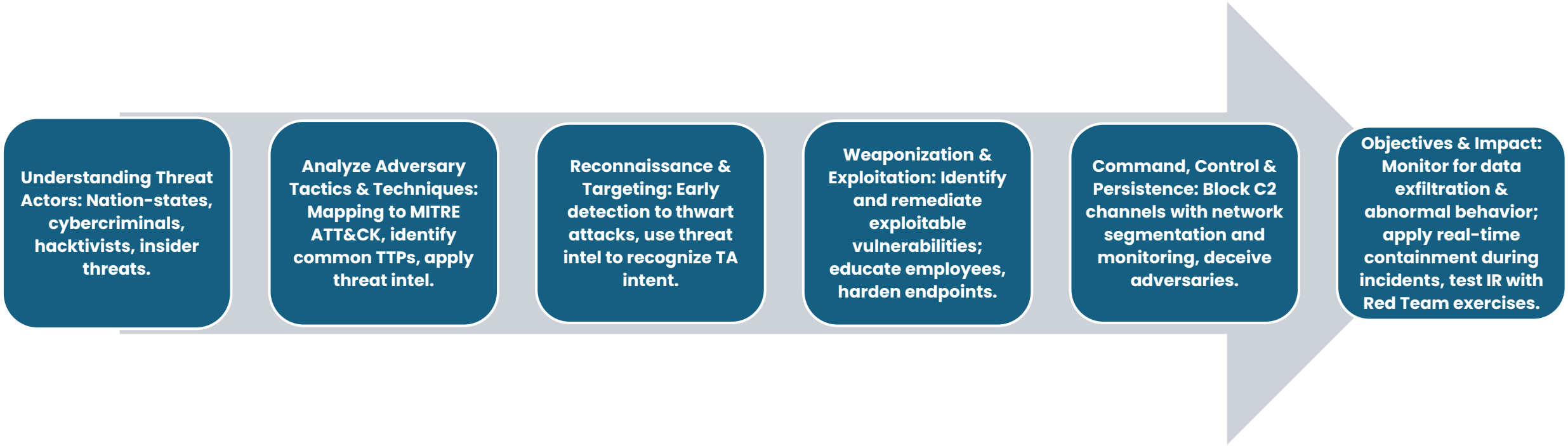
October 2023: British Library Hacked	January 2023: UK Royal Mail Breached
• The British Library suffers a crippling cyberattack, taking down its website and most of its online services, including card transitions, reader registrations, and ticket sales, along with access to its digital library catalog. • Recovery costs library £7 million (US$8.9M), or about 40% of its reserve budget. • Investigators trace unauthorized access at the Terminal Services server to facilitate remote access for external partners and IT admins. https://www.darkreading.com/cyberattacks-data-breaches/key-takeaways-from-the-british-library-cyberattack	• UK's primary postal service experiences significant ransomware attack by Russia-linked threat actor LockBit. • Breach particularly impacts Heathrow Worldwide Distribution Centre, leading to substantial disruption to international shipments. • "Absurd" ransom demand of £67 million (US $80M) not paid. https://www.theregister.com/2022/09/16/uber_security_incident/

Flipping the Script:

Why Rethink the Traditional Kill Chain

- Increasing ease of harvesting authentication tokens and user creds
- Increasing sophistication of supply chain---Shared responsibility but no capability
- Threat actors can bypass MFA and harvest creds with great ease
- Attacks are no longer “viruses”---human-led, active
- Conventional defenses not enough: perfect prevention is impossible
- Defense is complicated (and nearly impossible) by largely non-existent perimeters
- Abused IT access to systems in the primary cause of destructive acts
- Cloud & SaaS proliferation have blurred lines and confused recovery readiness
- Hardware & software vendors (and orgs) commonly do not understand breach

Along the Kill Chain: Know Your Enemy



Harden in Reverse: Assured Recovery

Resist The Threat Actors

Assure Recovery

Compromise Credentials

- No forced password hygiene.
- Password length too short (12 char).
- Password caching allowed in browsers.
- Weak forms of MFA permitted - SMS and phone call; strong MFA not in use.
- Passwords & tokens likely cached on personal devices
- No geo-blocking, impossible travel, or malicious logon detection enabled in MS Authenticator or Okta.
- Vendors have access to VPN.
- There is no standard web browser: Chrome browser is in use & personal e-mail access is not blocked.
- Personal webmail and social media platforms are not blocked.
- Device trust is not required for VPN.
- SaaS, cloud-based tools are accessible off the VPN.

Persistent Access

- VPN could be accessed without corporate device.
- Always-on, full VPN not used.
- SOC minimally involved in kill chain, requires explicit approval from client.
- No geo-blocking of outbound and inbound traffic.
- RBAC and least privilege are not uniformly enforced across admin consoles.
- No complimentary AV/EDR platform on endpoints.
- Unauthorized code permitted to execute.
- Commercially available remote access tools are not blocked.
- Unrestricted egress possible from Org offices.
- MFA self enrollment permitted.
- Weak OKTA configuration: daily driver accounts used for administration.

Elevated Access

- Users permitted to cache credentials in browser: Cached passwords and browser-based password managers used in the environment.
- Personal password mangers used by IT.
- Password vault accessible from public internet (Bitwarden), not isolated on admin/mgmt segment.
- Local admin accounts with poor credential management policy are used for admin functions in the environment.
- No PAM tool in the environment to perform proper credential management of admin accounts.
- SSPR is enabled for admins, weak forms of MFA are allowed for reset (e-mail, mobile, office).
- Service accounts not restricted to specific sources and targets.

Lateral Movement

- MFA is not required for administrative function via PowerShell, WMI, MMC, RDP, and Windows Remote Management.
- MFA is not required while on LAN/VPN.
- EDR not natively IP restricted to dedicated mgt/admin segment.
- Administrative systems accessible from user segments & VPN.
- PIM is not in use within Entra ID.
- Segmented administrative Azure AD/EntraID tenant does not exist.
- vCenter and ESXi hosts are domain joined.
- Access to AD not secured: no lateral movement defense.
- SOC minimally involved in kill chain, requires explicit approval from client.
- vCenter and NetApp are integrated.

Data Exfiltration

- Firewall rules are not reviewed regularly.
- External collaboration settings within Azure are misconfigured, potentially causing data loss or leak.
- Outbound traffic is unrestricted by port.
- VPN split tunnel is used.
- Organization data is not automatically removed from mobile devices when an account is disabled.
- No effective blocking of file sharing, personal storage, remote access software, password vaults, hacking tools, & other commercially & maliciously available software used for exfiltration.
- Deep packet inspection not observed in the environment.
- Access to Org data & SaaS apps is not restricted to corporate devices.
- Internet browsing is permitted from servers, printers, and other unneeded segments, devices.

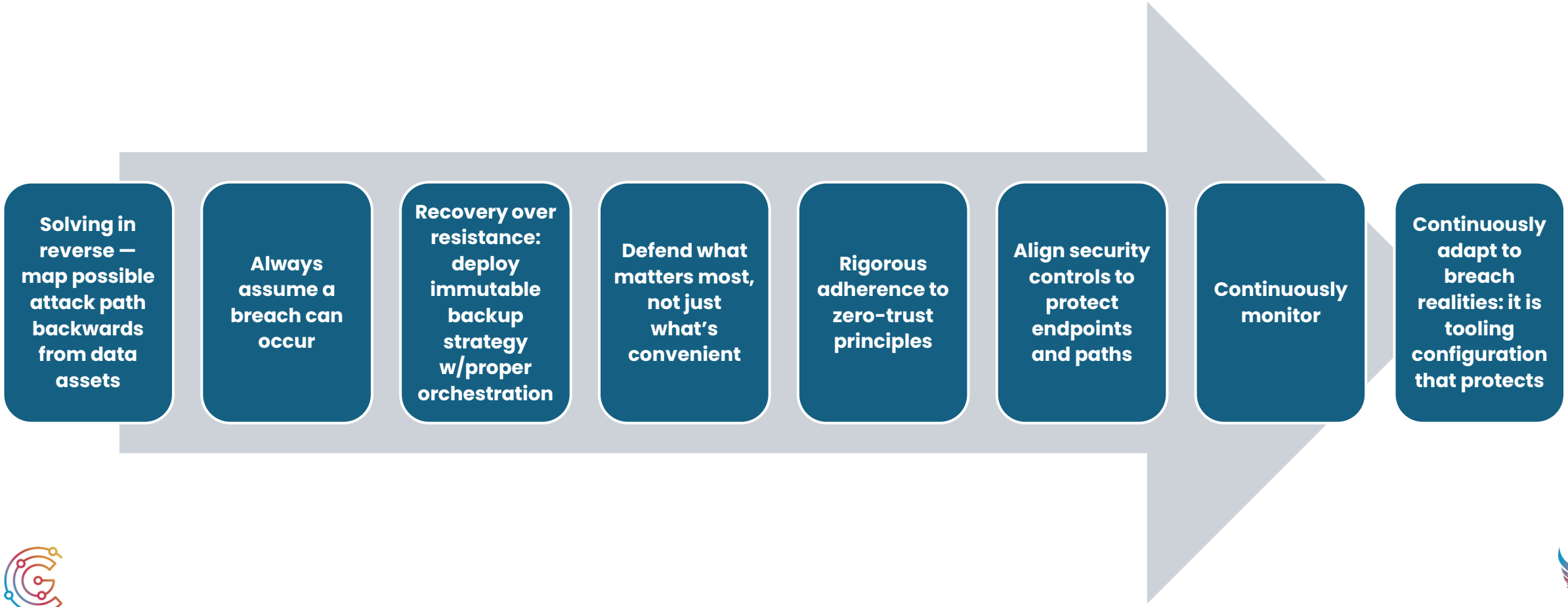
Backup Destruction

- Most backups are not immutable.
- Maintain only a single, non-immutable backup copy.
- The remote, immutable backup copies are 30 days old.
- Backup consoles/devices are accessible from user segments and domain credentials.
- MFA is not applied to the backup storage and software.
- All production data/systems are not being backed up.
- NetApp snapshots are not immutable, credentials stored in Bitwarden, and Bitwarden configuration is weak.
- Backup of SaaS providers not under the control of the Org---Workday.
- Office 365 backups are not immutable.
- Mass recovery capability is not tested: Mass destruction recovery time likely very long.
- AWS backups reside in same tenant.
- AWS S3 not backed up.

Mass Encryption/ Destruction

- Veeam, vCenter, iLO, EDR, ESXi, AWS, Azure, NetApp, & Bitwarden are accessible from user segments.
- No IP restrictions on EDR Console.
- vCenter, ESXi, Veeam, Azure, & AWS are domain joined.
- Hypervisor & backup tools accessible from user segments and with domain credentials with no MFA.
- No separate VLAN, jump box, or ACL to limit access to sensitive infrastructure consoles.

Reimagining the Kill Chain: Modern Cyber Defence Principles



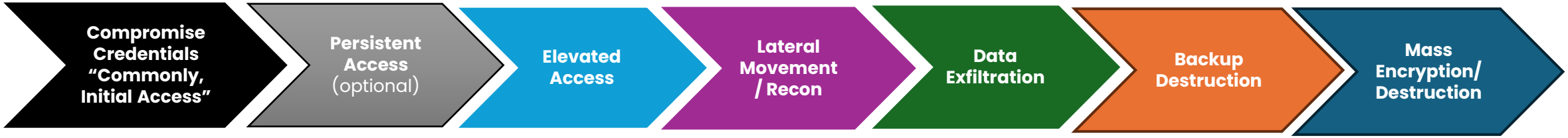
Why Breach Context & Pattern Matter

- If this pattern is to be disrupted, **disruption must be done in reverse (right to left)** — starting with the attackers end game, not the following the flow of the attack (left to right) — which is the common defense philosophy.
- Basically, all organizations are overinvesting in the first five tranches and largely ignoring the last two tranches.
- Despite organizations' best investment & effort, resistance controls and infrastructure are largely orchestrated poorly. There are many reasons for this, but the foundational reason is the LACK of BREACH CONTEXT!

Lack of Breach Context causes destruction.

- Breach context, if leveraged as a guide to Breach Pattern disruption, commonly will dictate configuration that is contrary to industry "best practice" or "common IT understanding."
- **Without Breach Context, defenders are left to their own best judgment** about how systems should be orchestrated and, therefore, commonly make significant missteps that will exacerbate TA destructive possibility.

TA Progression Commonly Easy



- **Compromise creds:** If you allow your users to: (1) Access SaaS apps or remote access tech from personal devices, (2) Cache creds in browsers while allowing access to personal email services, (3) Use SSPR with weak MFA methods and no facilitated enrollment of MFA & MDM, or (4) Use weak MFA more generally, creds and MFA are easily bypassed.

- **Persistent Access:** If your: (1) VPN or Citrix doesn't require methods of establishing device trust (such as Intune membership, domain membership, and certificate presence) before it checks username, password, & MFA, (2) Remote access technologies, such as Bomgar, N-Able, ScreenConnect, GotoAssist, etc., are not blocked by default, or (3) Users are allowed to self-enroll in Intune or MFA, persistent access is easily established.

- **Elevated Access:** If IT staff: (1) Are permitted to use any browser they desire, (2) Can access sensitive consoles directly from their workstations, (3) Can cache credentials in browsers, (4) Can access sensitive consoles publicly, (5) Use daily drivers for administration, (6) Use password vaults not sanctioned and secured by the org, or (7) Can log into sensitive consoles with production AD creds, then elevation will be simple.

- **Lateral Movement:** If IT staff: (1) Can RDP directly to servers (not whether they do, but if they CAN), (2) Can use PowerShell, RDP, VMI, WinRM, MMC, etc. to servers without MFA, (3) Can access critical consoles from user segments, and (4) Critical consoles are accessible with production AD creds, lateral movement and ultimately mass destruction will be simple.

Vendor "Immutability" Is Not Enough

IMMUTABILITY: A security principle that states the data in storage cannot be changed, encrypted, or deleted by any means. Even if a threat actor were able to gain access to the data, they would not be able to modify or destroy it because there are no IT administrative technical overrides to the retention lock.

In Fenix24's (2000+) actual breach experiences,

84%

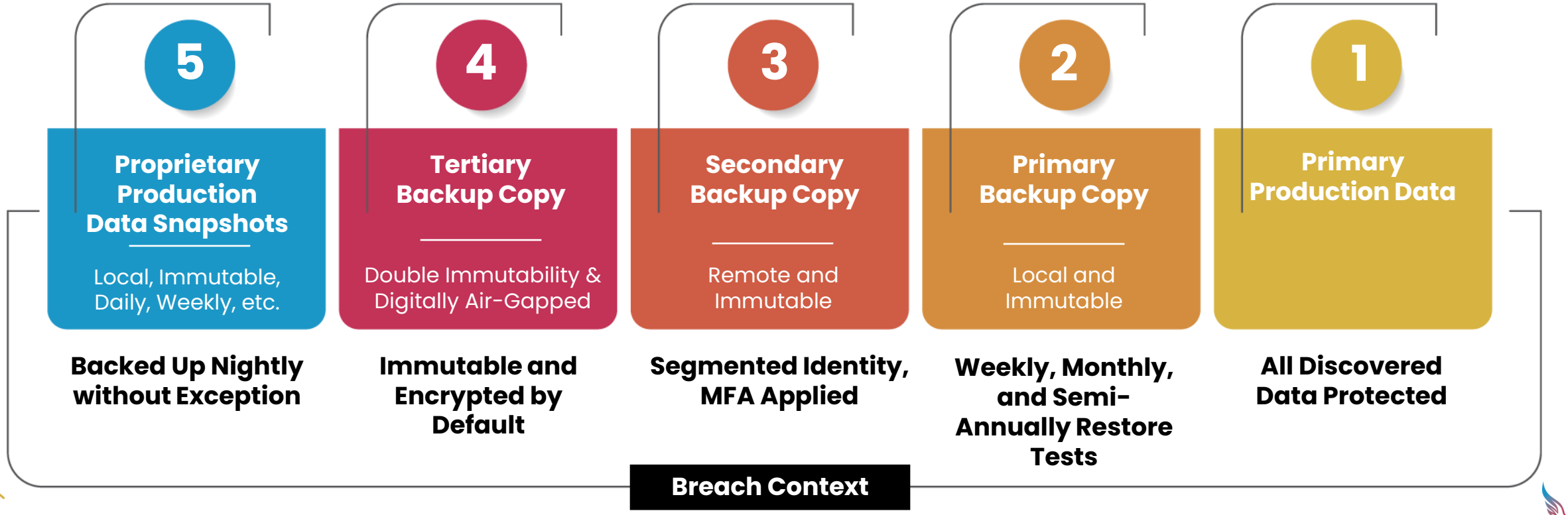
of data thought to be immutable

DOES NOT SURVIVE!

If threat actors gain access, they can change settings and destroy / encrypt data believed to be "immutable."

Survivability, 5-4-3-2-1

5-4-3-2-1 Grypho5 Proprietary Method:



WHAT TO DO NOW: Actions You Can Take

Assess the organization's recovery capabilities against breach contact (Athena7).

- Evaluate the efficacy of the organization's key applications' data and critical infrastructure.
- Measure survivability, usability, and timely recoverability against a proper definition of immutability, breach context, and breach context born principles.

Establish retainer with a restoration company (Fenix24).

Align leadership to mass recovery realities – point and time (Athena7).

Prioritize mass recovery. Mass destruction most likely form of disaster for companies.

- Assure recovery from mass and backup destruction.
- Reassure recovery continually (Grypho5).

Establish a recovery zone where mass restoration can be safely tested and RTO measured (Grypho5).

Regularly test and harden recovery capabilities to establish predictable recovery timelines (Grypho5).

Complicate and obfuscate critical console administrative identity (Grypho5).

- Segment critical consoles, such as password vaulting, EDR, vCenter, and storage.
- Apply MFA to all administrative functions.

Questions and Comments

Come Chat With Us

If you would like a copy of the presentation, please scan the QR code.

ILTA EVOLVE

THANK YOU!

Take Our Survey