

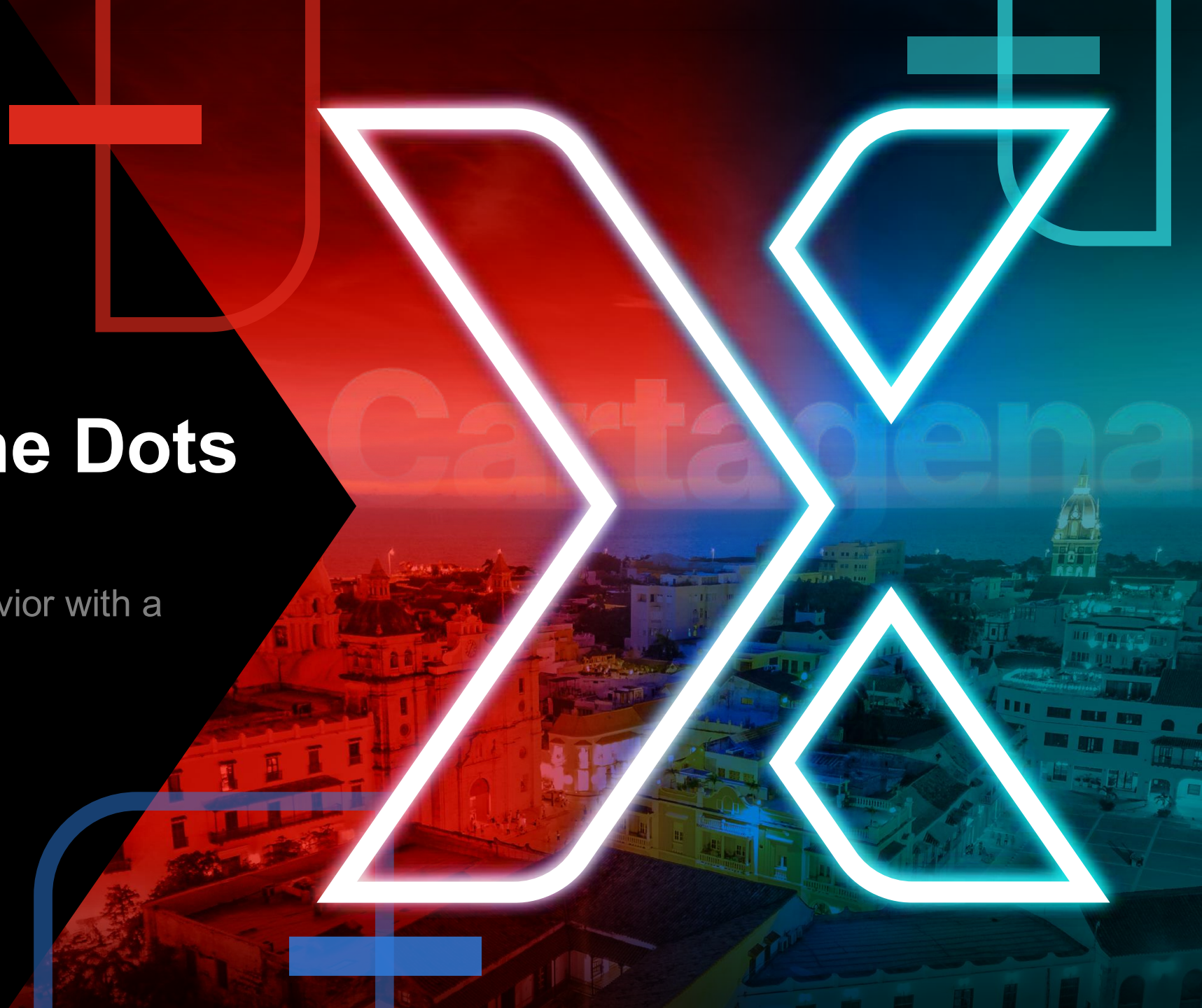


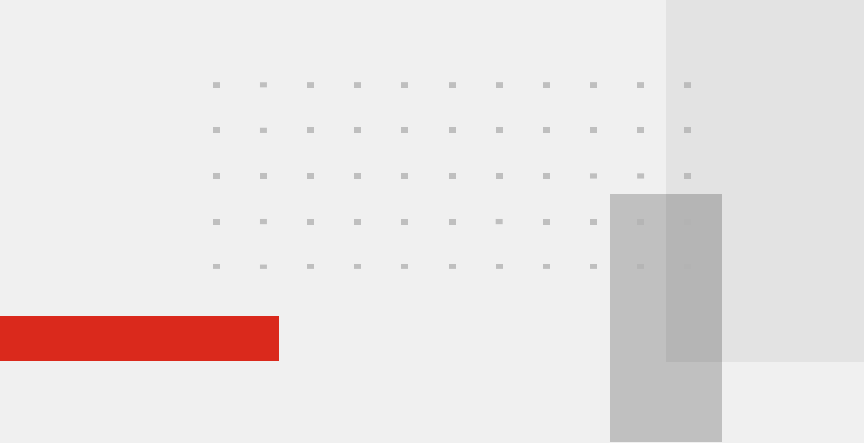
Connecting the Dots of an Attack

Understanding Attacker Behavior with a TTP-First SecOps Approach

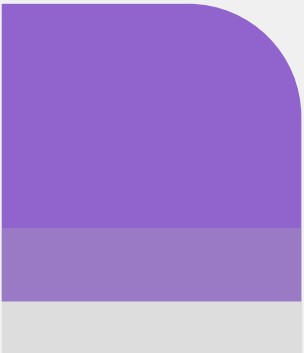


Cesar Rios
Systems Engineer
crios@fortinet.com
3113839317





Agenda



01 Business Scenario

02 When tools don't talk

03 TTP-First Philosophy: One continuous attack

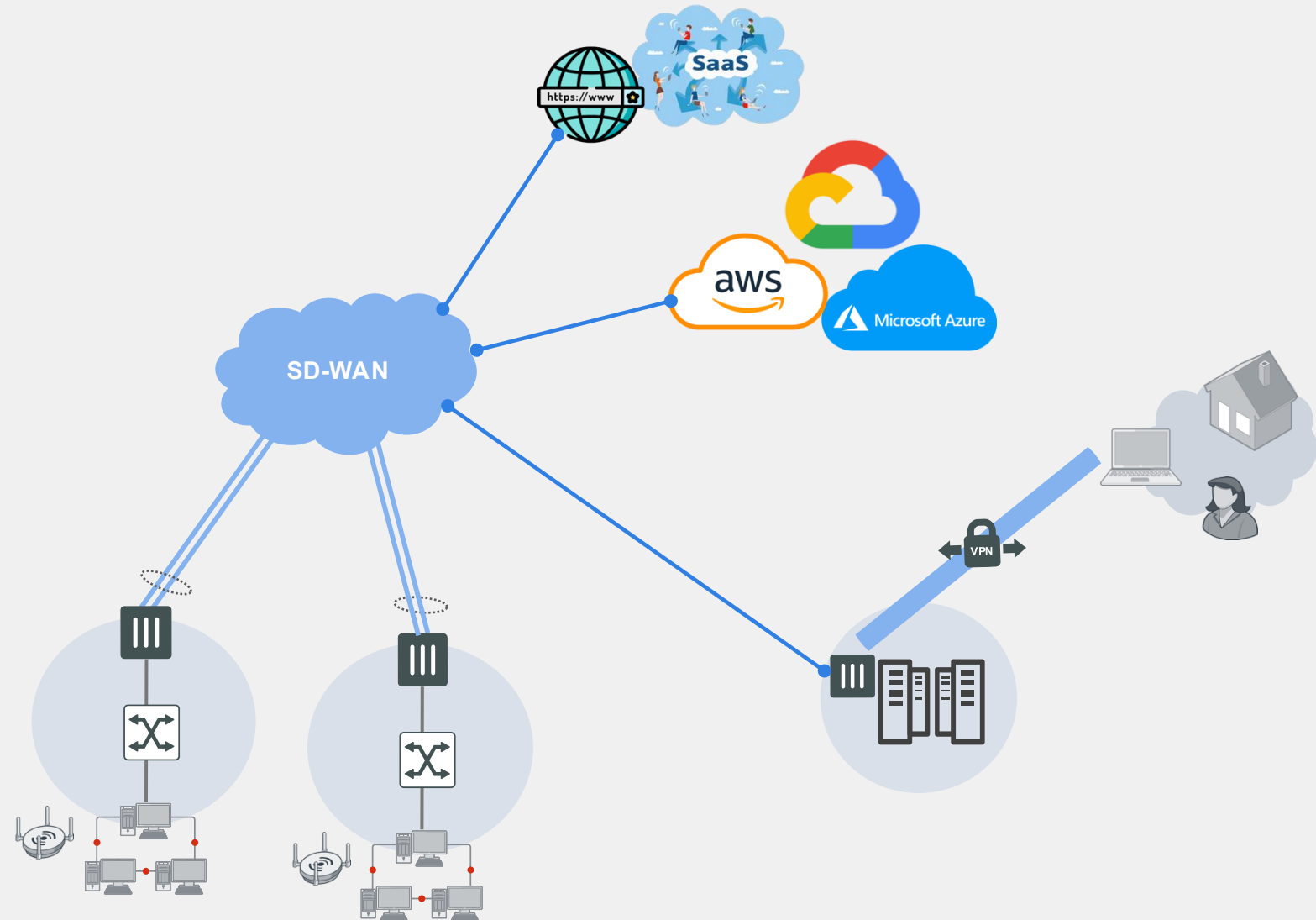
04 Architecting TTP-First SecOps with Fortinet

05 From Alerts to Behavior: SecOps Services

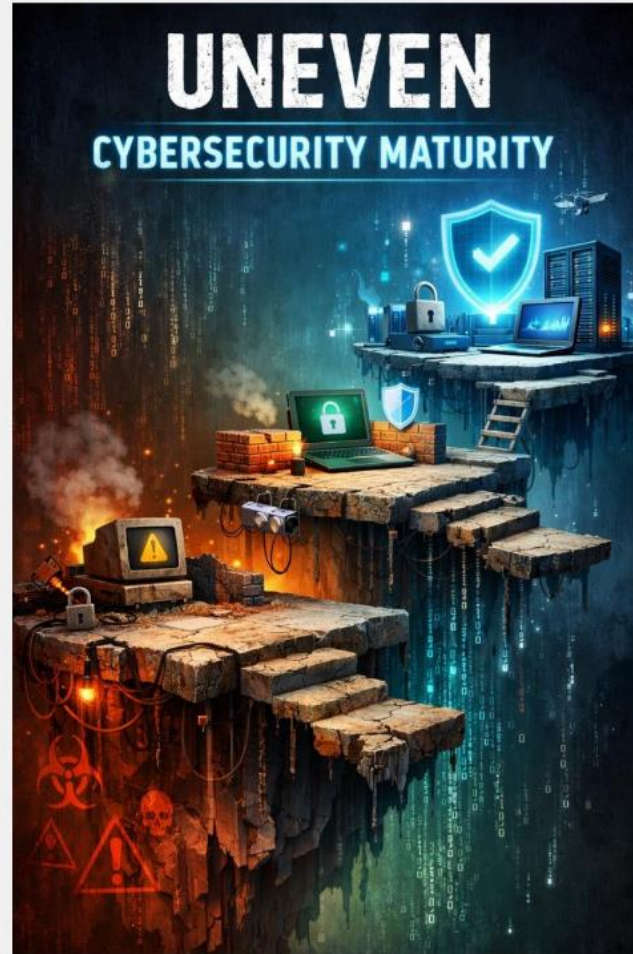
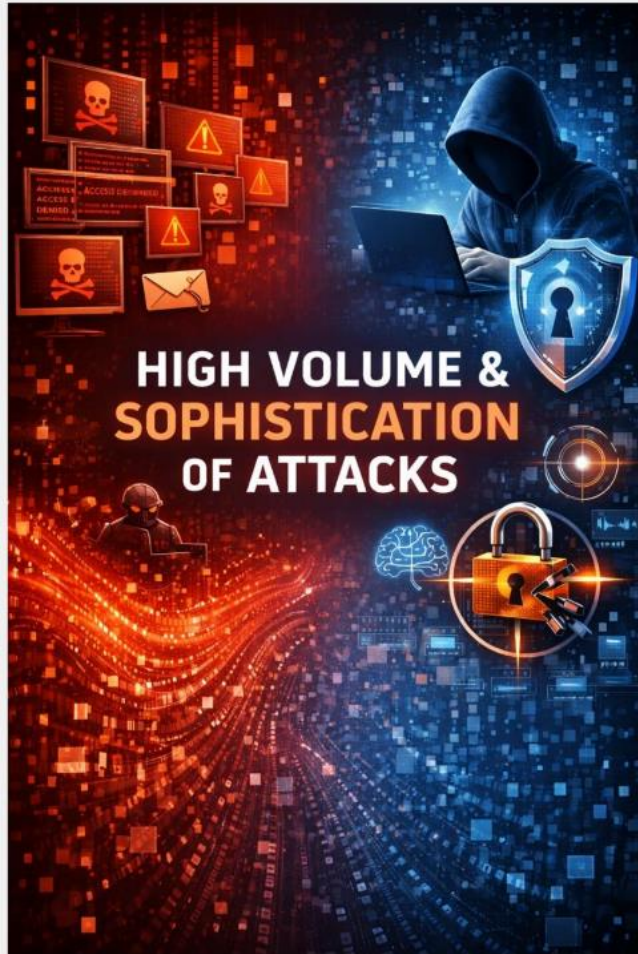
06 Labs



Common Enterprise IT Components



Enterprise Challenges



SOC Challenges

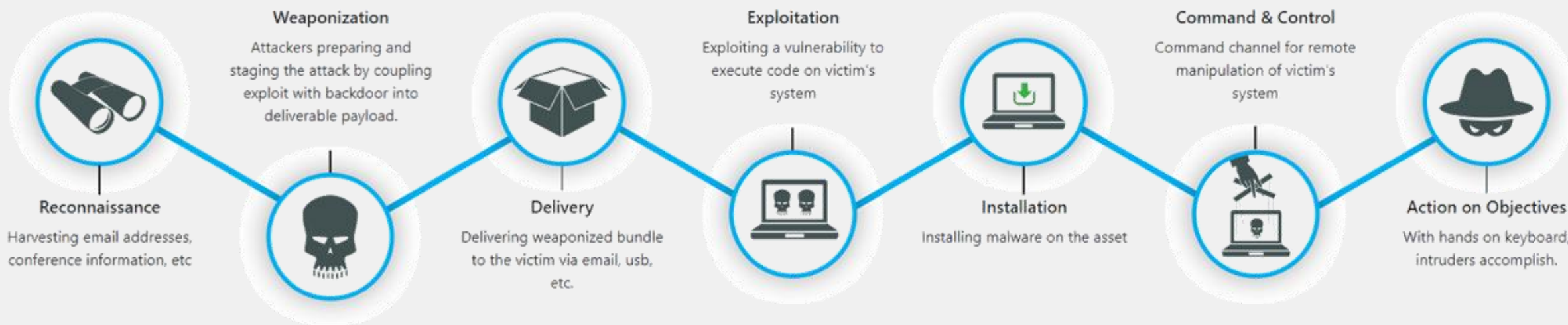


FORTINET | COLOMBIA
& ECUADOR
XPERTS26

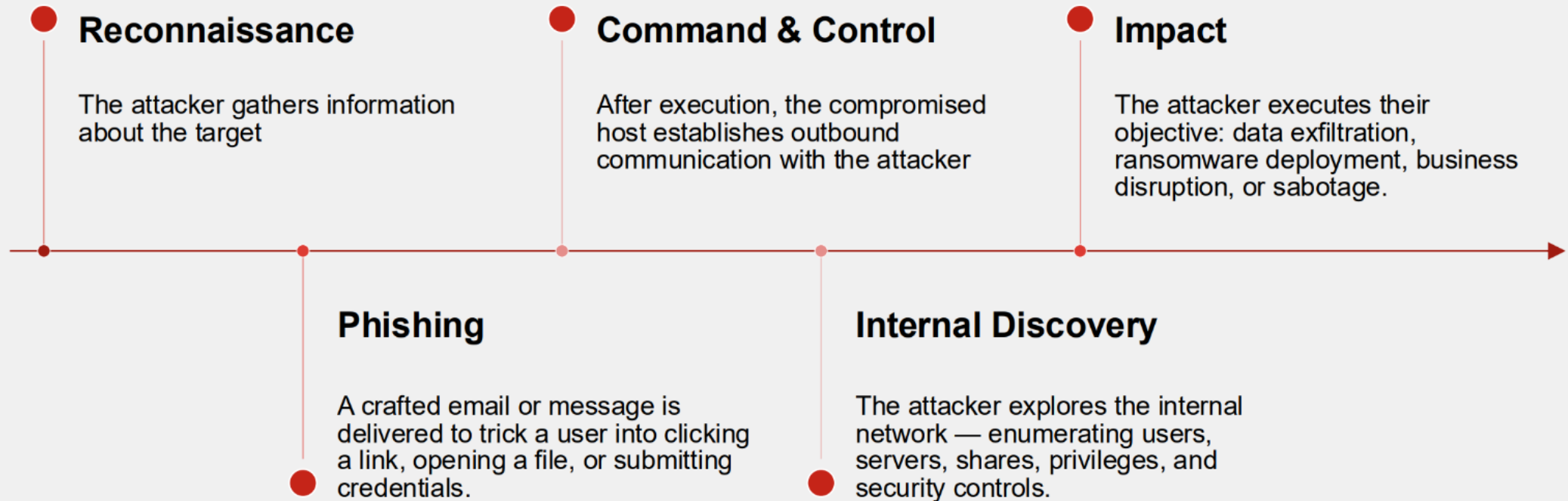
When Tools don't Talk



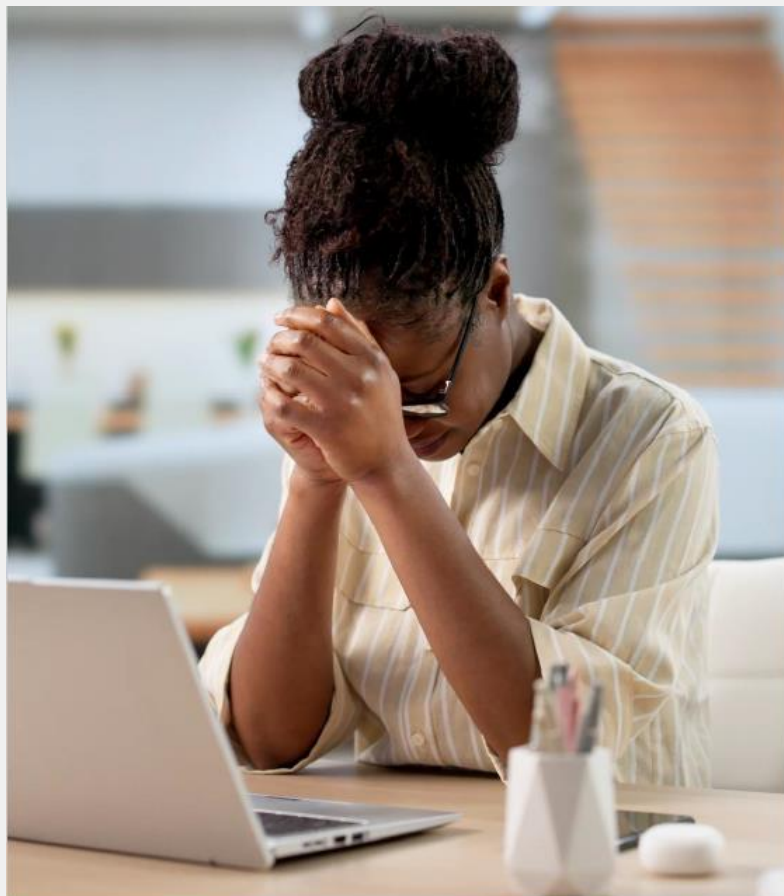
The Kill Chain



One Attack, Five Phases



Every control worked, the SOC still failed



FORTINET | COLOMBIA
XPERTS26 & ECUADOR

TRACK SECOPS



MITRE | **ATT&CK™**

Another matrix to memorize...

ATT&CK Matrix for Enterprise

layout: side ▾

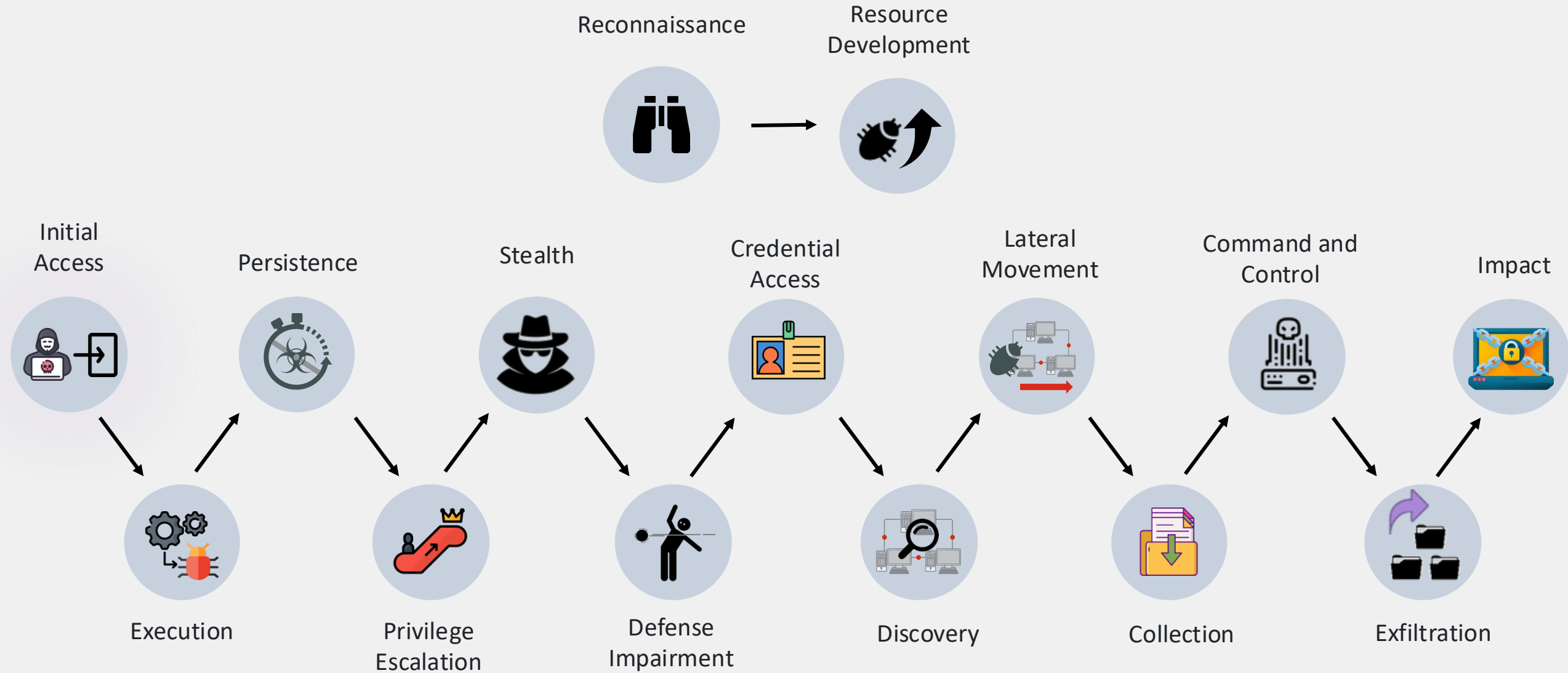
show sub-techniques

hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Stealth	Defense Impairment	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
12 techniques	9 techniques	11 techniques	20 techniques	22 techniques	13 techniques	30 techniques	18 techniques	17 techniques	34 techniques	9 techniques	17 techniques	18 techniques	9 techniques	15 techniques
Active Scanning (3)	Acquire Access	Content Injection	BITS Jobs	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Access Token Manipulation (5)	Disable or Modify System Firewall (3)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Cloud Administration Command	BITS Jobs	Access Token Manipulation (5)	BITS Jobs	Disable or Modify Tools (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Command and Scripting Interpreter (13)	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Build Image on Host	Domain or Tenant Policy Modification (2)	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (3)	External Remote Services	Container Administration Command	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Downgrade Attack	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Content Encoding (2)	Data Manipulation (3)	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Deploy Container	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Exploitation for Defense Impairment	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Encoding (2)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Replication Through Removable Media	ESXi Administration Command	Compromise Host Software Binary	Create or Modify System Process (5)	Direct Volume Access	File and Directory Permissions Modification (2)	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Query Public AI Services	Generate Content (2)	Supply Chain Compromise (3)	Exploitation for Client Execution	Create Account (3)	Domain or Tenant Policy Modification (2)	Execution Guardrails (2)	Modify Authentication Process (9)	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Email Bombing
Search Closed Sources (2)	Obtain Capabilities (7)	Trusted Relationship	Hijack Execution Flow (12)	Create or Modify System Process (5)	Escape to Host	Hide Artifacts (14)	Modify Cloud Compute Infrastructure (5)	Modify Authentication Process (2)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Valid Accounts (4)	Input Injection	Event Triggered Execution (13)	Event Triggered Execution (13)	Hijack Execution Flow (12)	Indirect Command Execution	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (6)	Hide Infrastructure	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Wi-Fi Networks	Inter-Process Communication (3)	Exclusive Control	Exploitation for Privilege Escalation	Indicator Removal (3)	Obfuscated Files or Information (18)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Search Threat Vendor Data			Native API	External Remote Services	Process Injection (12)	Indirect Command Execution	Pre-OS Boot (5)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Inhibit System Recovery
Search Victim-Owned Websites			Poisoned Pipeline Execution	Implant Internal Image	Scheduled Task/Job (5)	Masquerading (12)	Process Injection (12)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
			Scheduled Task/Job (5)	Modify Authentication Process (5)	Valid Accounts (4)	Obfuscated Files or Information (18)	Reflective Code Loading	Plist File Modification	Group Policy Discovery		Data Staged (2)	Protocol Tunneling		Resource Hijacking (4)
			Serverless Execution	Modify Registry		Pre-OS Boot (5)	Rootkit	Prevent Command History Logging	Local Storage Discovery		Email Collection (3)	Proxy (4)		Service Stop
			Shared Modules	Office Application Startup (6)		Process Injection (12)	Selective Exclusion	Rogue Domain Controller	Log Enumeration		Input Capture (4)	Remote Access Tools (3)		System Shutdown/Reboot
			Software Deployment Tools	Power Settings		Pre-OS Boot (5)	Social Engineering (2)	Safe Mode Boot	Network Service Discovery		Screen Capture	Traffic Signaling (2)		
			System Services (3)	Pre-OS Boot (5)		Scheduled Task/Job (5)	System Binary Proxy Execution (14)	Subvert Trust Controls (6)	Network Share Discovery		Video Capture	Web Service (3)		
			Trusted Developer Utilities Proxy Execution (3)	Scheduled Task/Job (5)		Server Software Component (6)	System Script Proxy Execution (2)	Weaken Encryption (2)	Network Sniffing					
			User Execution (5)	Server Software Component (6)		Software Extensions (2)	Template Injection		Password Policy Discovery					
			Windows Management Instrumentation	Software Extensions (2)		Traffic Signaling (2)	Traffic Signaling (2)		Peripheral Device Discovery					
				Traffic Signaling (2)		Trusted Developer Utilities Proxy Execution (3)	Trusted Developer Utilities Proxy Execution (3)		Permission Groups Discovery (2)					
				Valid Accounts (4)		Unused/Unsupported Cloud Regions	Unused/Unsupported Cloud Regions		Process Discovery					
									Query Registry					
									Remote System Discovery					
									Software Discovery (2)					
									System Information Discovery					
									System Location Discovery (1)					

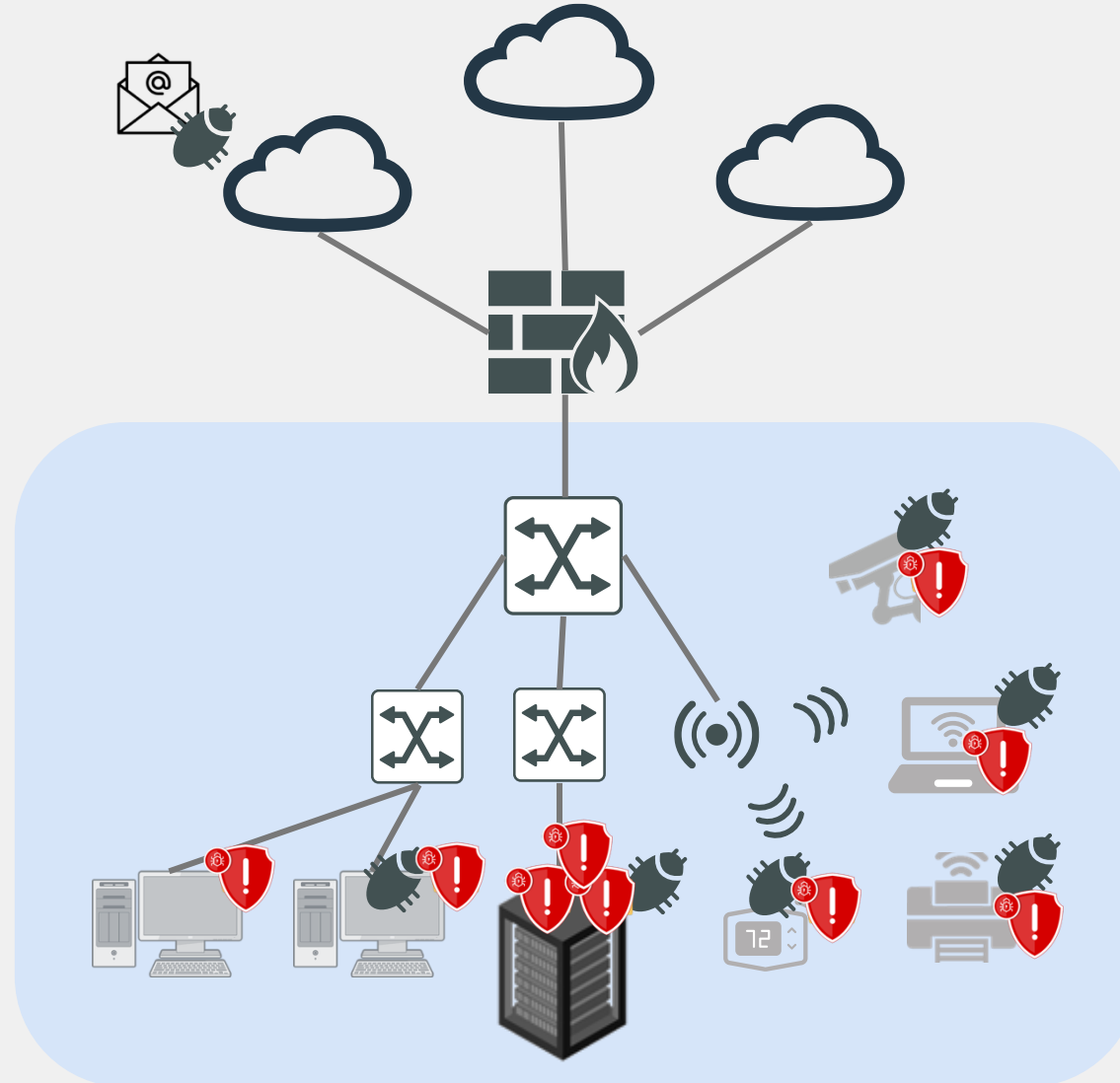


How an attacker operates



An example...

Initial Access	
11 techniques	
Content Injection	
Drive-by Compromise	
Exploit Public-Facing Application	
External Remote Services	
Hardware Additions	
Phishing (4)	
Replication Through Removable Media	
Supply Chain Compromise (3)	
Trusted Relationship	
Valid Accounts (4)	
Wi-Fi Networks	



TTP-First Core Focus

The challenge is understanding what the attacker is doing — fast enough to stop them

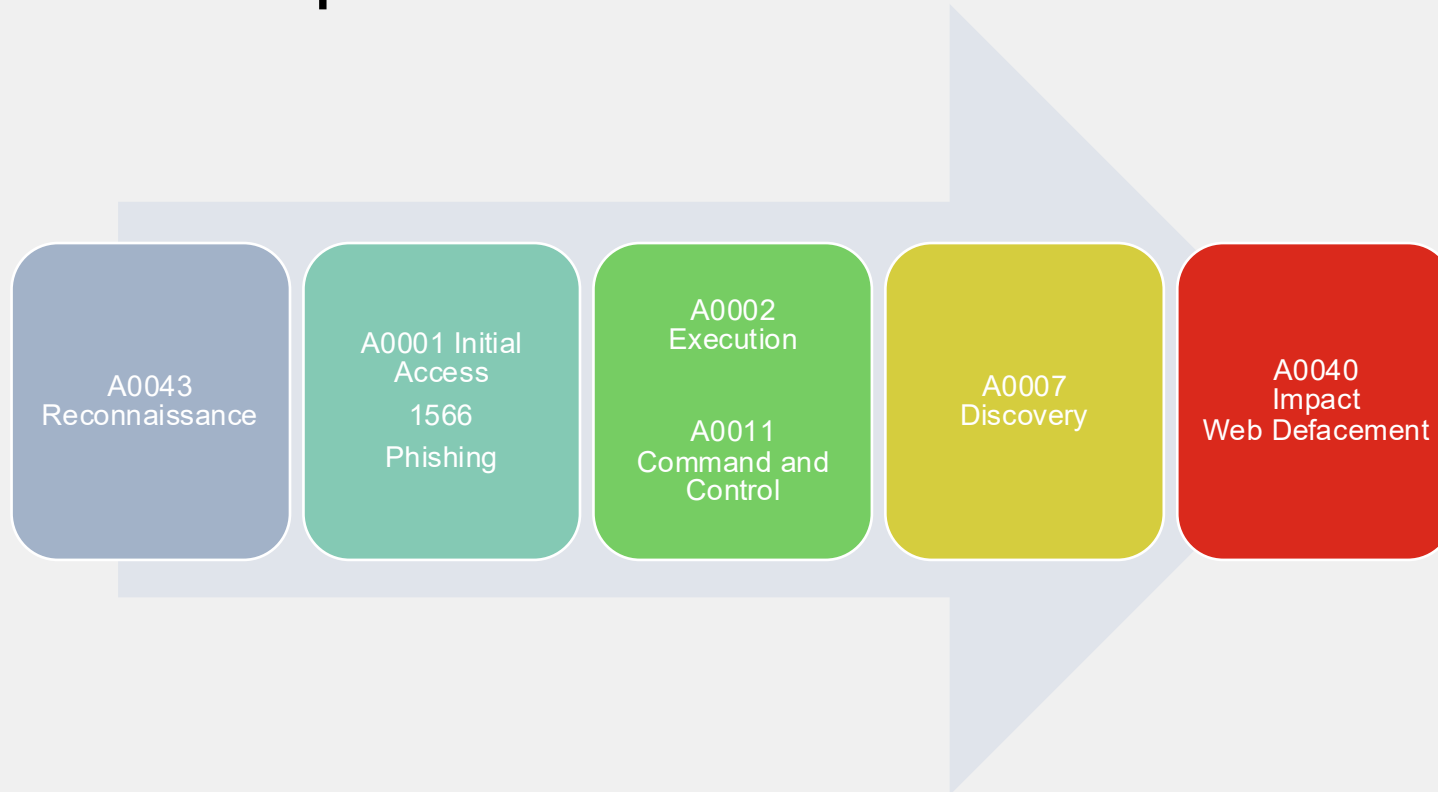
- **Detect attacker behavior early** Identify tactics and techniques *before* impact, not after compromise.
- **Connect the dots across events** Correlate email, endpoint, network, and application signals into a **single attack story**.
- **Investigate using a common language** Use **MITRE ATT&CK** to describe *what the attacker is doing*, not just *what fired*.
- **Reduce detection & investigation time** Move from hours/days of manual analysis to **minutes with contextual investigation**.
- **Enable confident response** Analysts act with clarity — and responses become candidates for **automation**.



The Attack Story

One Attack, Five Phases

An external attacker progresses step-by-step through the environment, leaving **partial signals at each phase**.



Each lab represents a **phase of the same attack**, observed and investigated through **MITRE ATT&CK behaviors**, not isolated alerts.

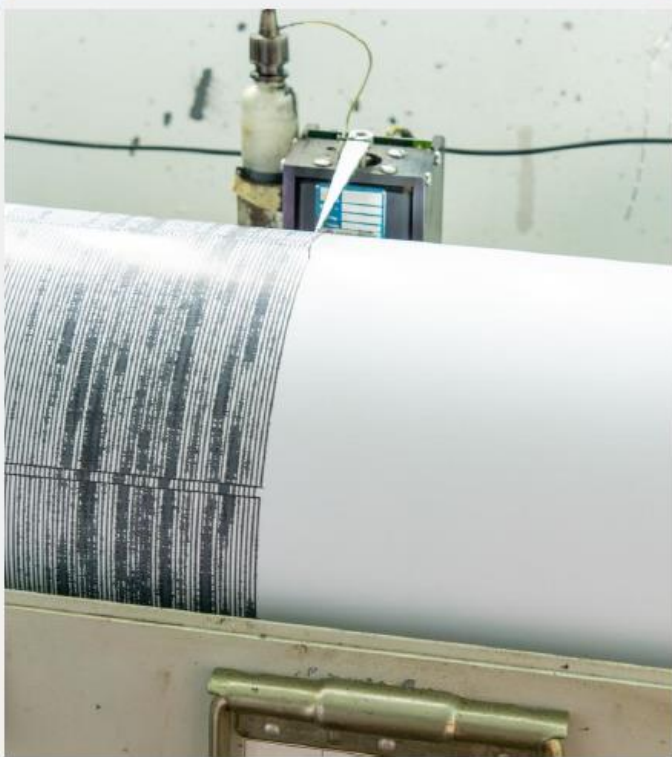
FORTINET | COLOMBIA
XPERTS26 & ECUADOR

Architecting TTP- First SecOps with Fortinet

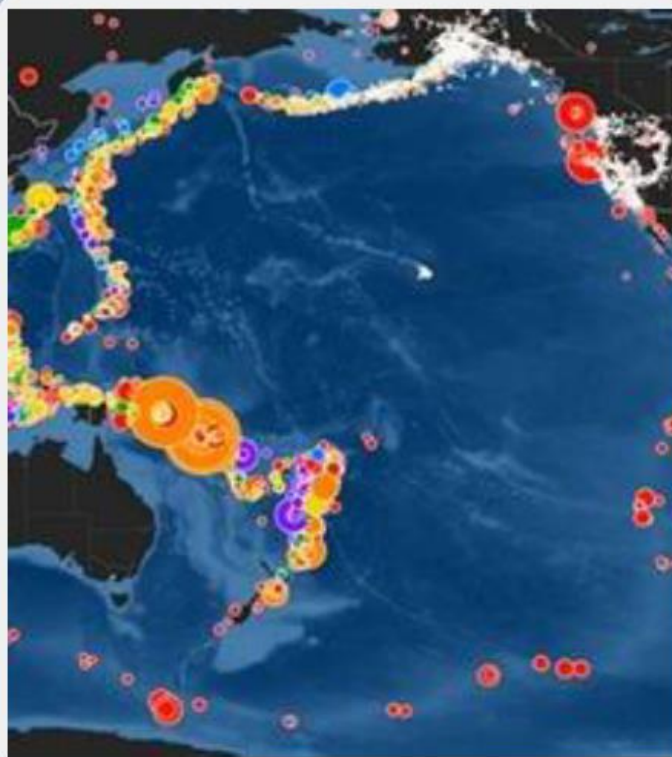


From Tools to Telemetry Architecture

Tools



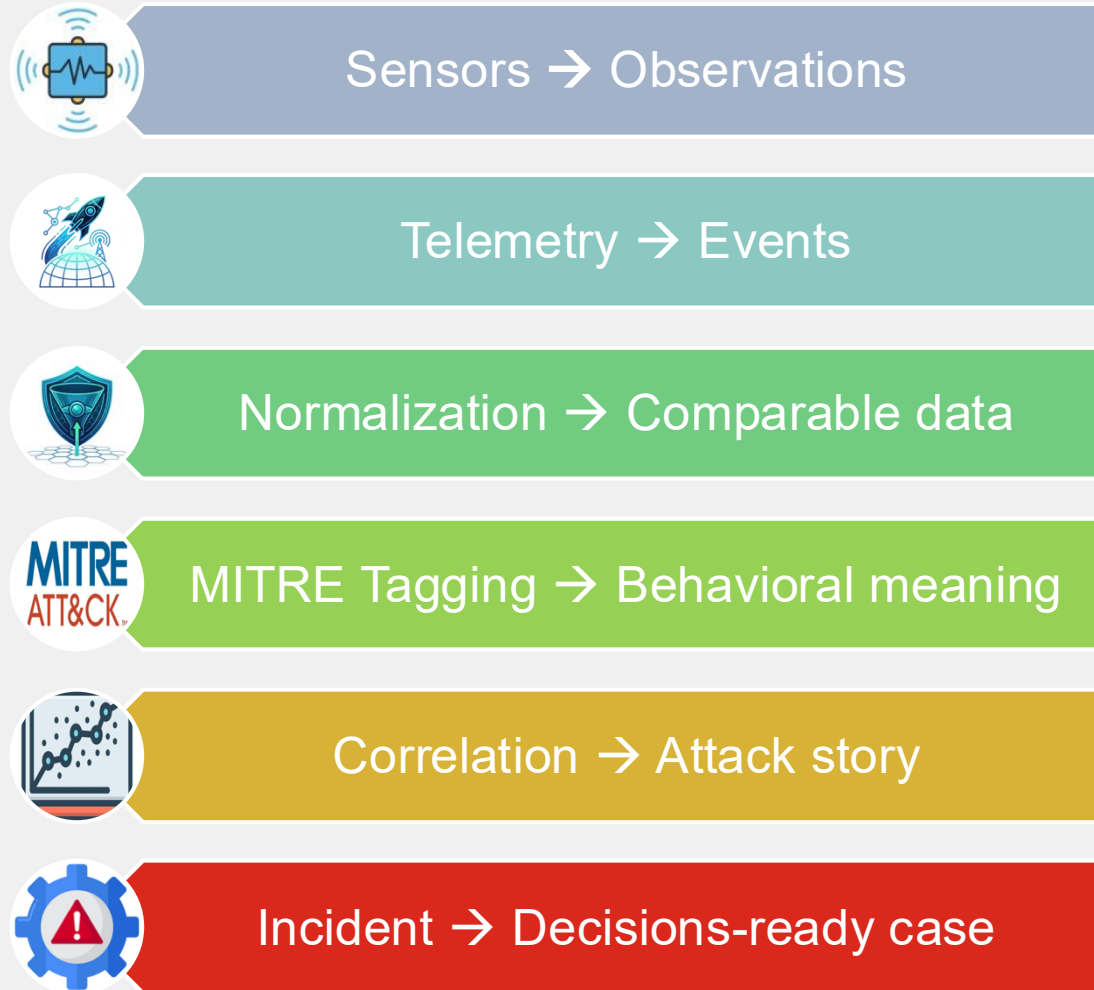
Telemetry



Correlation



Data Flow Architecture



Telemetry Roles

FortiAnalyzer

- Centralized log intelligence
- Parsing & enrichment
- Structured visibility

FortiSIEM

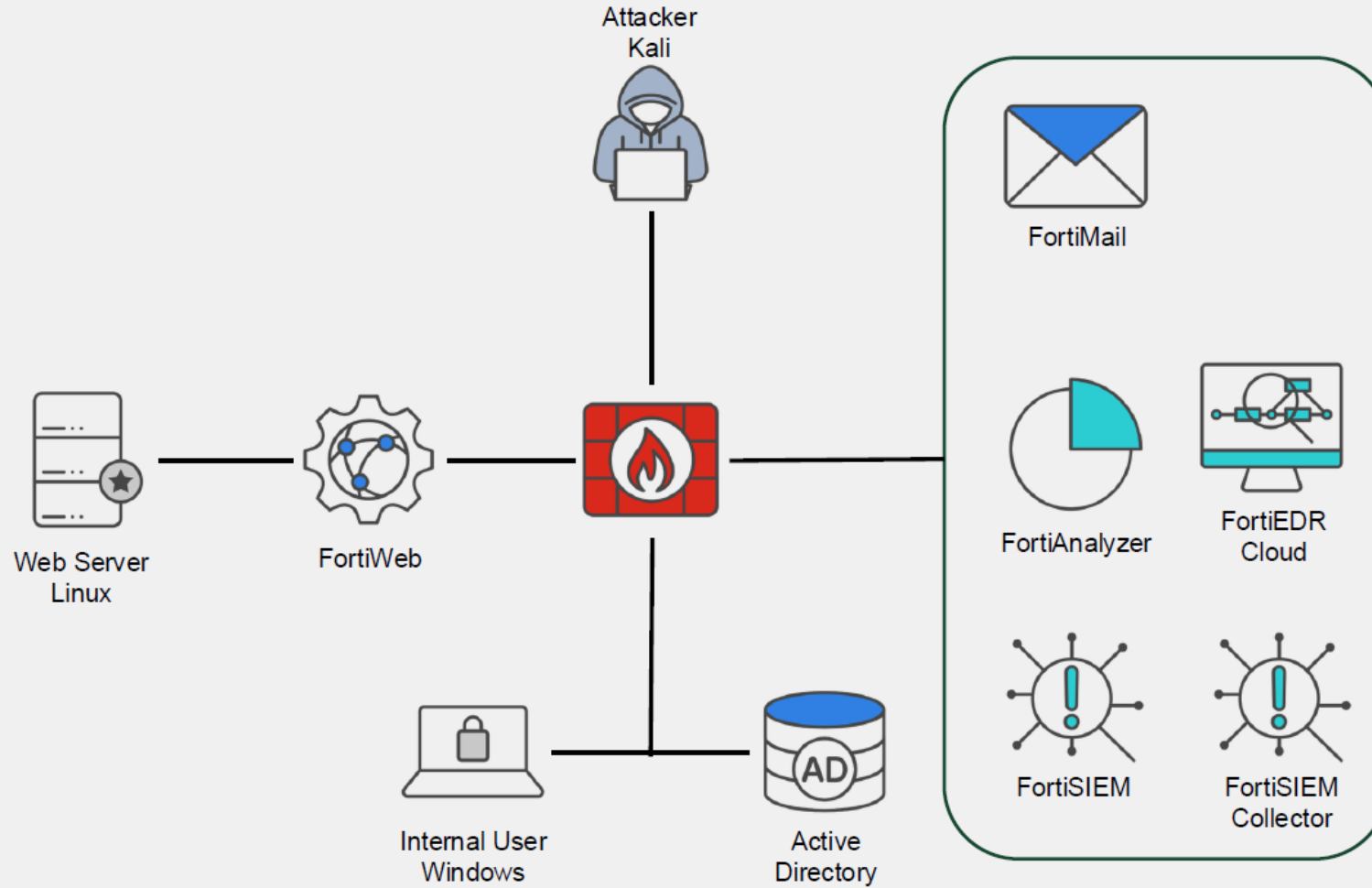
- Multi-source correlation
- Incident logic
- Timeline construction

FORTINET | COLOMBIA
XPERTS26 & ECUADOR

**From Theory to
Practice**

Cartagena

The architecture



The Attacker

Scarlet Jackal

Motivation

- Public defacement as a visibility and reputational attack
- Demonstrate persistent access to the environment
- Cause brand and customer trust impact

Modus Operandi

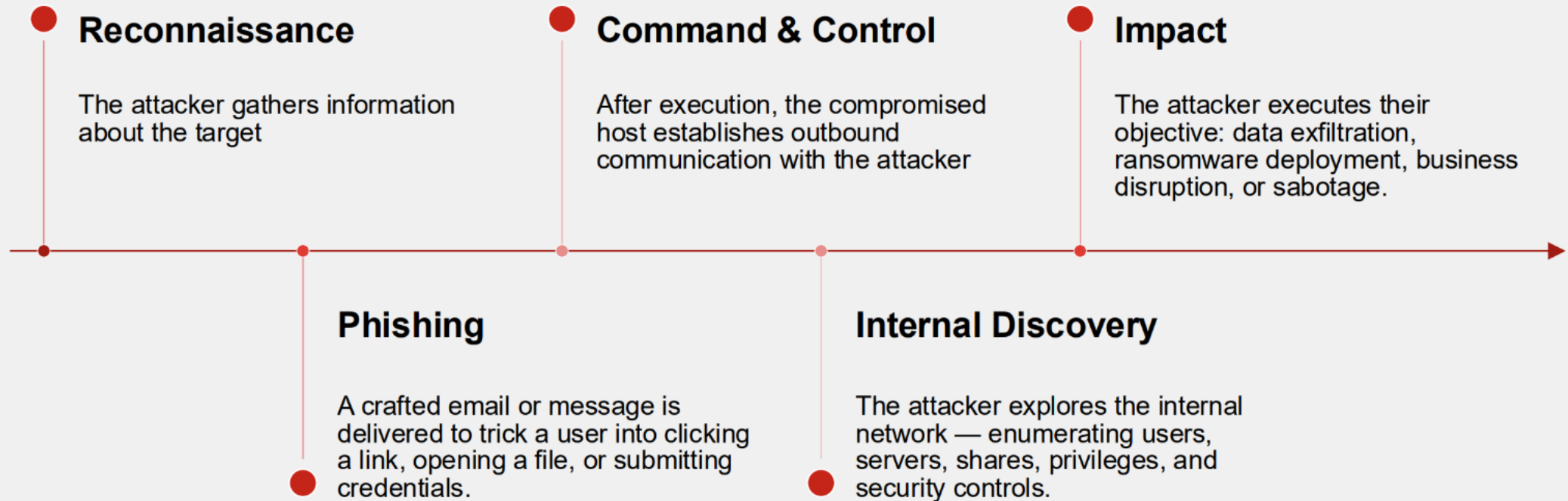
- Targeted, low-volume attacks (not mass campaigns)
- “Low and slow” techniques
- Abuse of legitimate channels (email, HTTPS)
- Clear progression through MITRE ATT&CK tactics

FORTINET | COLOMBIA
XPERTS26 & ECUADOR

Let's start with the
track



One Attack, Five Phases



Acceso al laboratorio

<https://latam.amerintlxperts.com/secops/TTP-First26/00-ttp-index.html>



User: amerintlxperts
Pass: xPerts2026!

Phase 1 – External Reconnaissance

Activities

Scarlet Jackal begins passive and active reconnaissance against *Latam Retail Group*.

Identifies:

- Public web portals
- Exposed technologies
- Potential attack surface related to campaigns

Activity includes:

- Selective scanning
- Gradual service enumeration

SOC Reality

- Low-severity scanning alerts
- No immediate response

MITRE Focus

- Reconnaissance (T1595, T1046)
- *The attack starts here — but no one calls it an incident.*



30 min

Phase 2 – Phishing for Initial Access

- **Activities**

- Using information gathered during reconnaissance, the attacker launches a targeted phishing campaign:
- Email impersonates:
 - An invoice
 - A trusted supplier document
- A corporate user executes the payload
- Results in:
 - Local code execution
 - Simulated persistence attempts
 - Initial internal network activity

- **SOC Reality**

- Email and endpoint alerts appear separately
- No connection to previous reconnaissance

- **MITRE Focus**

- Initial Access (T1566)
- Execution (T1204)
- *One click bridges the external world with the internal network.*



30 min

Phase 3 – Command & Control Communication

- **Activities**

- The compromised host establishes outbound communication:
- Periodic beaconing
- Encrypted outbound traffic
- Use of common, legitimate protocols

- **SOC Reality**

- Traffic appears normal
- No correlation with phishing or execution activity

- **MITRE Focus**

- Command and Control (T1071, T1095)
- *The attacker is inside — and no one knows yet.*



50 min

Phase 4 – Internal Discovery - Lateral Movement

- **Activities**

- With stable access, Scarlet Jackal begins exploring the internal environment:
- Discovers:
 - Internal segmentation
 - DMZ-hosted web servers
 - Paths to public-facing assets
- Identifies the route to the final target

- **Business Impact**

- Brand damage
- Loss of customer trust
- Executive-level escalation

- **MITRE Focus**

- Impact (T1491)
- *The SOC “detects” the attack when it becomes visible to everyone.*



30 min

Phase 5 – Web Defacement

- **Activities**

- The attacker leverages internal knowledge to:
- Access the web server in the DMZ
- Modify public content
- Publish a visible defacement message

- **Business Impact**

- Brand damage
- Loss of customer trust
- Executive-level escalation

- **MITRE Focus**

- Impact (T1491)
- *The SOC “detects” the attack when it becomes visible to everyone.*



30 min



FORTINET

COLOMBIA
& ECUADOR

XPERTS26

FORTINET | COLOMBIA
& ECUADOR
XPERTS26

Cartagena



<http://192.168.152.51:5000/>

