ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

Review Article

Open Access

Visualizing Cybersecurity Coverage using MITRE ATT&CK Framework

Shriyash Shete

Zscaler, Inc. Bloomington, IN, USA

***Corresponding author**
Shriyash Shete, Zscaler, Inc. Bloomington, IN, USA.

Received: August 10, 2023; **Accepted:** August 18, 2023; **Published:** August 29, 2023

ABSTRACT

This paper presents an innovative approach to visualizing cybersecurity coverage within the Zscaler Risk360 product, leveraging the MITRE ATT&CK framework. Emphasizing a user-centered design methodology, the study integrates the complex ATT&CK framework into a practical, interactive interface tailored for cybersecurity professionals. This interface combines qualitative and quantitative metrics, enabling users to assess the security posture of their organization effectively. The design process is informed by insights from semi-structured interviews with Chief Information Security Officers (CISOs) and subject matter experts, ensuring relevance and usability. The paper discusses key design decisions, including the integration of complex framework tree structures, color-coded coverage mappings, and a three-pane view for detailed analysis. Additionally, it explores extended use cases beyond the immediate application, suggesting potential for broader applications in various cybersecurity and compliance contexts. This work aims to enhance decision-making in cybersecurity management and inspire future research and development in cybersecurity and data visualization tools.

Keywords: Cybersecurity, Risk Management, Information Visualization, Monte Carlo Simulation, Financial Risk

Introduction

Defending an enterprise network against cyberattacks remains an increasingly difficult challenge that requires, among other things, advanced technologies and innovative approaches for thwarting an adversary's goals. Because new and complex attacks are continuously created, there is a need for a common framework to understand how attackers operate to achieve their objectives. This framework should not only help in understanding the attack but also to understand existing defenses and what mitigations can be put in place to thwart attacks.

This paper explains the interface design process to visualize the Cybersecurity coverage in the context of the Zscaler Risk360 product. It delves deeper into the user-centered design approach that was implemented to achieve the innovation interface solution intended for cybersecurity professionals.

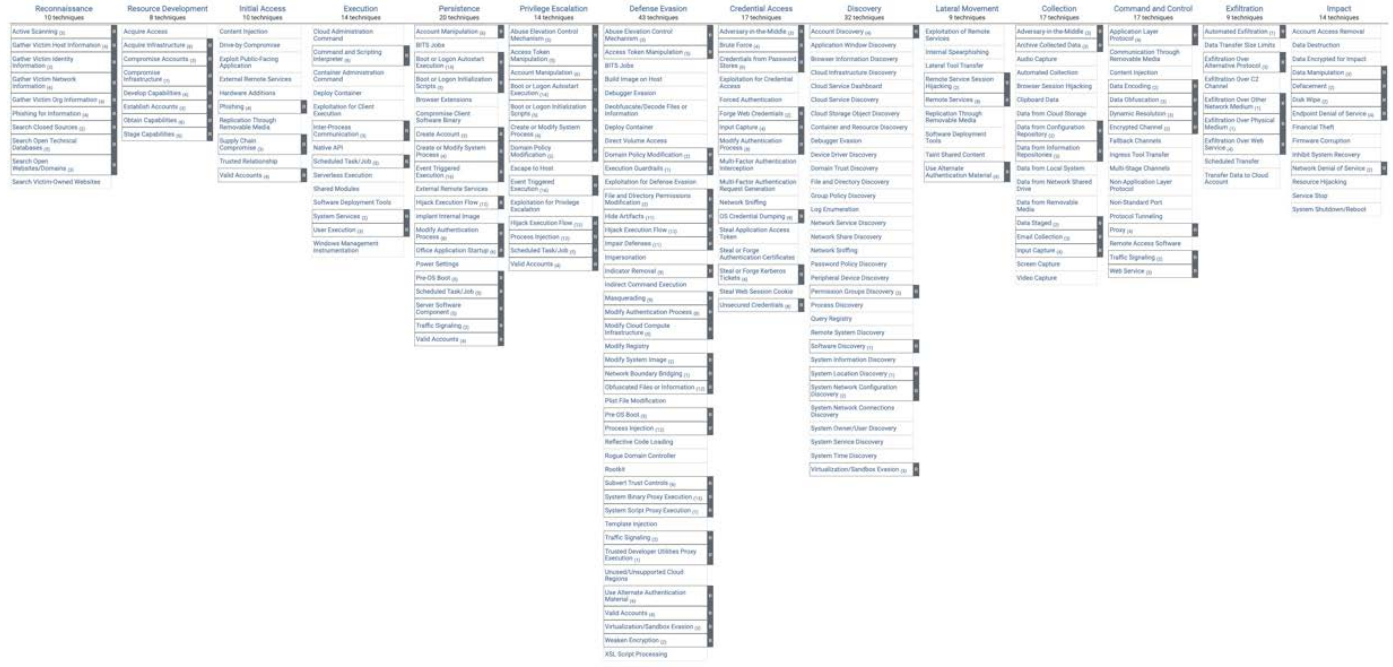
Background

MITRE ATT&CK Model

To help address the challenges of defending against modern attacks, MITRE Corporation developed a process for modeling an adversary's post-compromise behavior at a granular level with a common taxonomy. This model is named the ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework, and it serves as a knowledge base of commonly observed adversarial behaviors to support the efforts of threat intelligence functions, with adversary emulation and defensive gap analysis. ATT&CK was created out of the need to systematically document and catalog adversaries' behaviors based on millions of data points observed from real-life attacks and breaches. The model describes the Tactics, Techniques, and Procedures (TTPs) of adversarial behavior and breaks them into categories based on the sequence of steps involved in an attack. It is not intended to be exhaustive and is very much a living framework that is continuously updated as new TTPs are discovered [1,2].

The ATT&CK model is an ordered list of observed behaviors from known attacks. These behaviors are known as tactics and techniques. ATT&CK is visually organized into a few different matrices: PRE-ATT&CK, Enterprise, and Mobile. Each of these matrices contains various tactics and techniques relevant to its domain. PRE-ATT&CK is a matrix of tactics and techniques related to what attackers do before they try to exploit a particular target network or system. The Enterprise matrix contains tactics and techniques that apply to Windows, Linux, and/or MacOS systems. The mobile matrix contains tactics and techniques that apply to mobile devices. The scope of this paper is limited to the Enterprise Matrix [1,2].

The MITRE ATT&CK framework Enterprise Matrix is composed of 14 tactics, including the first two PRE-ATT&CK tactics, each with associated techniques. The tactics appear in roughly sequential order, following the general stages of a comprehensive (or worst-case) adversarial attack (See Figure 1):



Reconnaissance
10 techniques
Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (4)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (3)
Search Victim-Owned Websites

Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (8)
Compromise Accounts (3)
Compromise Infrastructure (7)
Develop Capabilities (4)
Establish Accounts (3)
Obtain Capabilities (6)
Stage Capabilities (6)

Initial Access
10 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)

Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter (9)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (3)
Native API
Scheduled Task/Job (5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (3)
Windows Management Instrumentation

Persistence
20 techniques
Account Manipulation (6)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (16)
External Remote Services
Hijack Execution Flow (12)
Implant Internal Image
Modify Authentication Process (8)
Office Application Startup (6)
Power Settings
Pre-OS Boot (5)
Scheduled Task/Job (5)
Server Software Component (5)
Traffic Signaling (2)
Valid Accounts (4)

Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism (5)
Access Token Manipulation (5)
Account Manipulation (6)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Domain Policy Modification (2)
Escape to Host
Event Triggered Execution (16)
Exploitation for Privilege Escalation
Hijack Execution Flow (12)
Process Injection (12)
Scheduled Task/Job (5)
Valid Accounts (4)

Defense Evasion
43 techniques
Abuse Elevation Control Mechanism (5)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (11)
Hijack Execution Flow (12)
Impair Defenses (11)
Impersonation
Indicator Removal (9)
Indirect Command Execution
Masquerading (9)
Modify Authentication Process (8)
Modify Cloud Compute Infrastructure (5)
Modify Registry
Modify System Image (2)
Network Boundary Bridging (1)
Obfuscated Files or Information (12)
Plist File Modification
Pre-OS Boot (5)
Process Injection (12)
Reflective Code Loading
Rogue Domain Controller
Rootkit
Subvert Trust Controls (6)
System Binary Proxy Execution (13)
System Script Proxy Execution (1)
Template Injection
Traffic Signaling (2)
Trusted Developer Utilities Proxy Execution (1)
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material (4)
Valid Accounts (4)
Virtualization/Sandbox Evasion (3)
Weaken Encryption (2)
XSL Script Processing

Credential Access
17 techniques
Adversary-in-the-Middle (3)
Brute Force (4)
Credentials from Password Stores (6)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Modify Authentication Process (8)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Unsecured Credentials (8)

Discovery
32 techniques
Account Discovery (4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (1)
System Information Discovery
System Location Discovery (1)
System Network Configuration Discovery (2)
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion (3)

Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (8)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)

Collection
17 techniques
Adversary-in-the-Middle (3)
Archive Collected Data (3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (2)
Data from Information Repositories (3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Screen Capture
Video Capture

Command and Control
17 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Content Injection
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Traffic Signaling (2)
Web Service (3)

Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (4)
Scheduled Transfer
Transfer Data to Cloud Account

Impact
14 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Endpoint Denial of Service (4)
Financial Theft
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking
Service Stop
System Shutdown/Reboot

Figure 1: MITRE ATT&CK Framework by MITRE Corporation

Tactics
Tactics represent the "why" of an ATT&CK technique. It is the adversary's tactical objective for performing an action. Tactics serve as useful contextual categories for individual techniques and cover standard notations for things adversaries do during an operation, such as persist, discover information, move laterally, execute files, and exfiltrate data. A total of 14 tactics have been observed from previous attacks and are defined in the ATT&CK matrix [1,2].

Techniques
Techniques represent "how" an adversary achieves a tactical objective by performing an action. Techniques may also represent "what" an adversary gains by performing an action. For example, an adversary may dump credentials from an operating system to gain access to useful credentials within a network. There may be many ways, or techniques, to achieve tactical objectives, so there are multiple techniques in each tactic category [1,2].

Sub-Techniques
Sub-techniques describe "how" an adversary achieves a tactical objective in more detail, including the specific tools used. For example, an adversary may use spear phishing as a targeted phishing attack to make the phishing technique look more genuine [1,2].

Procedure
Sub-techniques describe "how" an adversary achieves a tactical objective in more detail, including the specific tools used. For example, an adversary may use spear phishing as a targeted phishing attack to make the phishing technique look more genuine [1,2].

Zscaler Risk360
Zscaler Risk360 product aims to provide a holistic security measurement and quantification framework to cybersecurity professionals so that they can assess the overall risk posture of the organization and take necessary actions to mitigate risks. The entire framework is based on the individual risk computation for the underlying hundred plus contributing factors. These contributing factors are nothing but the risk findings in an organization's environment categorized into four stages of a typical cyber breach: 1. External Attack Surface (where the threat actor attempts to discover an organization's external attack surface exposed to the internet), 2. Compromise (the threat actor attempts to compromise an organization's corporate asset via threats delivered from the internet) 3. Lateral Propagation (the threat actor attempts to move laterally within the organization's environment from the compromised asset) and 4. Data Loss (the threat actor steals sensitive data as part of the actions on the objective stage).

These are tailored to CISOs needs to efficiently monitor the security environment of the business and make security enhancement and remediation decisions efficiently. Risk360 assesses thousands of signals from other Zscaler offerings to compute a comprehensive and aggregated risk score. It covers all the underlying contributing factors associated with multiple Zscaler capabilities implemented in the organization's digital environment [3,4].

User Research Analysis
We conducted twelve 30-minute semi-structured interviews with CISOs as well as subject matter experts (SMEs) to discuss the significance of MITRE ATT&CK in cybersecurity and identify the ways to showcase it in the context of Risk360.

From the interviews, we found that the goal of ATT&CK is to break down, classify, and document adversarial behaviors from previously observed attacks in a common language that is consistent and clear. This type of cataloging and identification provides a number of benefits to cyber security professionals, such as the following use cases:

Adversary Emulation
Test and verify defenses against common techniques of adversaries.

Red Team
Create plans and organize operations to avoid certain defensive measures that may be in place within a network.

Evaluate Current Defenses
Assess tools, monitoring, and mitigation capabilities of existing defenses within an organization's environment.

Finding Gaps in Coverage
Identify gaps as a way to prioritize investments for security improvements. Similar security products can also be compared against a common adversarial behavior model to determine coverage.

Prioritize Detections
Identify and rank alerts based on their potential threat level.

Adversary Emulation
Test and verify defenses against com- mon techniques of adversaries.

In this paper, we primarily focus on the 'Evaluate current defenses', 'Finding gaps in coverage' and 'Prioritize detections' aspects that are important for security executives and analysts with titles Chief Information Security Officer(CISO), Chief Security Officer (CSO) and Security Operators in the context of Zscaler Risk360 software.

Overall, we identified the common theme of suggestions: Mapping the risk360 contributing factors with mitigations for various ATT&CK techniques and keeping it as part of the Risk360 interface.

Below are some other key insights we gathered about the MITRE framework:

Qualitative as Well as Quantitative Metrics
through interviews, we found out that cyber security professionals are well-versed with analytical findings and want to see quick numeric data to make sense of the information presented. Hence, instead of only showing the coverage in terms of qualitative metrics using visual mappings, we need to combine them with quantitative findings such as showing the percentage of coverage with the help of a donut chart. For example, if total number for of covered techniques is 83 out of the total 196 techniques then we should highlight 43% using a chart.

MITRE Scoring Rubric
During interviews, one of the subject matter experts pointed out an official scoring rubric that MITRE corporation recommends to assess the effectiveness of the TTPs. They assess each technique's effectiveness in terms of three levels-minimal, partial and substantial. Also they categorize each technique into three control types-protect, detect and respond. We decided to leverage these familiar methodologies and include them in the interface design.

Coverage, Configuration: through our study, we found out that the MITRE attack framework can be utilized to understand two critical data points-1. The number of tactics techniques and sub-techniques are covered by the current Zscaler controls in place and 2. Whether those controls are correctly configured or misconfigured.

Design Inspiration
MITRE Corporation provides a web-based open source tool called ATT&CK Navigator which is highly customizable and can be used for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more. However, the tool requires users to set up the color-coding and mapping manually which is a very difficult task for large enterprises with large security infrastructure. These are often a medley of point solutions, spreadsheets, and manual aggregation of datasets to feed the navigator tool. We used this tool as an inspiration for providing an appropriate level of user control within a single Risk360 software [3,5].

We also took inspiration from the interfaces of Splunk Lantern and Microsoft Sentinel software interfaces which attempt to provide analytical insights through the MITRE ATT&CK framework visualization [6,7].

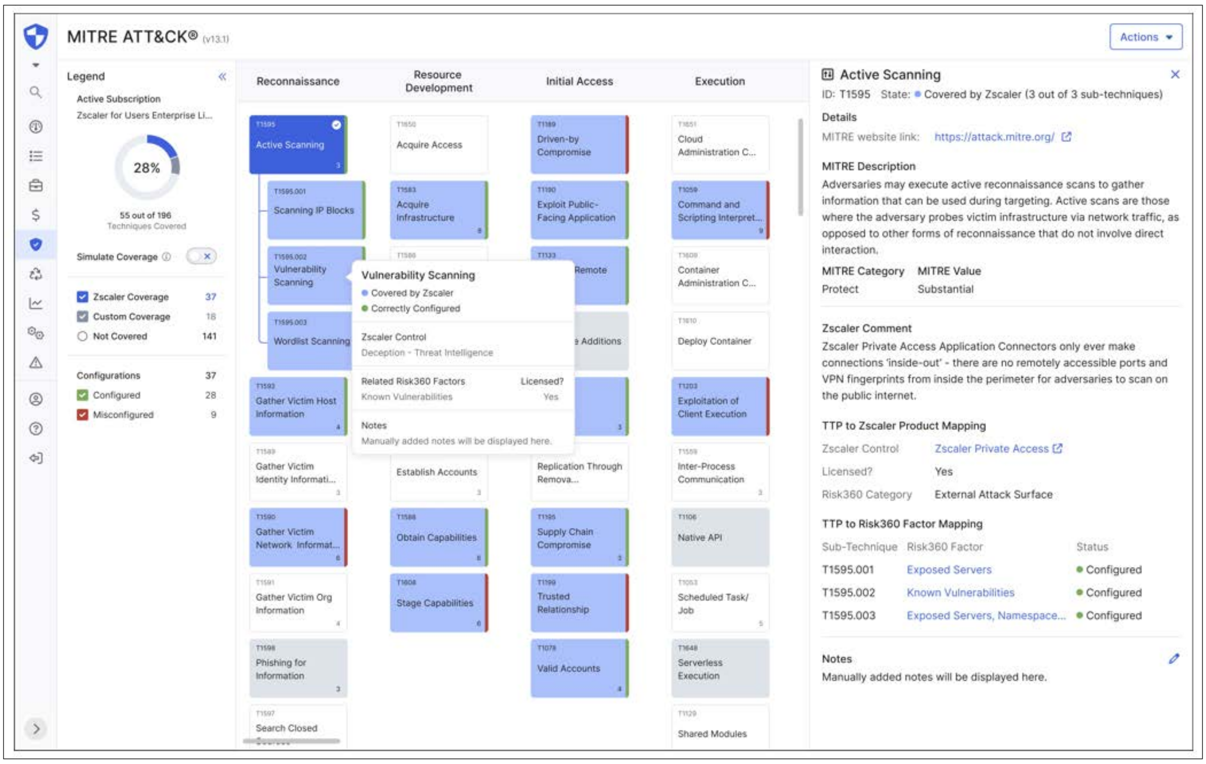
Design
Based on the insights that we gained from our interviews and data analysis, we designed high-fidelity mockups using Figma. Below are some of the key design decisions made:

Complex Tree Structures
Jakob's law of UX states that users spend most of their time on other sites. This means that users prefer your site to work the same way as all other sites they already know. Hence, in this case, we know that the security professionals are familiar with the MITRE ATT&CK website and would expect any other relevant interface to work similarly. Therefore, we decided to preserve the familiarity of the MITRE ATT&CK framework by maintaining the structure and hierarchy of the information. We kept the order of the tactics, techniques and sub- techniques consistent with the official document on the MITRE ATT&CK website. Thus, we assumed that these clickable tree structures with expandable and collapsible tiles, similar to the original familiar interface, would be easy to interact with for the CISOs and security administrators.

Making Sense of the Colors
Another design consideration was to provide a clear visual mapping of the coverage on top of the MITRE ATT&CK framework. With Zscaler coverage tiles represented in its brand color blue, custom covered in gray and not covered in white, we aimed to provide a clear visual indication and separation of different types of coverages quickly to the user. In addition to that, we also represented the configuration status for each technique where a red line meant misconfiguration and a green line depicted a correctly configured technique.

Three Pane View
On a broader level, the screen layout was divided into three sections-the leftmost being the legend panel for a quick overview of the security coverage, the middle one dedicated to the interactive framework itself and the rightmost panel to cover the details of each technique.

Tooltips
Because the framework itself has 196 techniques and 411 sub-techniques in total, and each of them has a long list of associated metrics to be shown inside the details panel, there was a need to quickly display the summary of those details, without the CISOs having to click several times to delve deeper. We used the tooltip design pattern filled with rich summary information that pops up when a user hovers over a technique.


MITRE ATT&CK® (v13.1)
Actions
Legend
Reconnaissance
Resource Development
Initial Access
Execution
T1595 Active Scanning 3
T1595.001 Scanning IP Blocks
T1595.002 Vulnerability Scanning
T1595.003 Wordlist Scanning
T1592 Gather Victim Host Information 4
T1589 Gather Victim Identity Informati... 3
T1590 Gather Victim Network Informat... 6
T1591 Gather Victim Org Information 4
T1598 Phishing for Information 3
T1597 Search Closed Sources
T1650 Acquire Access
T1583 Acquire Infrastructure 8
T1586
Establish Accounts 3
T1588 Obtain Capabilities 6
T1608 Stage Capabilities 6
T1189 Driven-by Compromise
T1190 Exploit Public-Facing Application
T1133 Remote
Additions
3
Replication Through Remova...
T1195 Supply Chain Compromise 3
T1199 Trusted Relationship
T1078 Valid Accounts 4
T1651 Cloud Administration C...
T1059 Command and Scripting Interpret... 9
T1609 Container Administration C...
T1610 Deploy Container
T1203 Exploitation of Client Execution
T1559 Inter-Process Communication 3
T1106 Native API
T1053 Scheduled Task/Job 5
T1648 Serverless Execution
T1129 Shared Modules

Active Subscription
Zscaler for Users Enterprise Li...

28%
55 out of 196
Techniques Covered

Simulate Coverage ⓘ ✕

☑ Zscaler Coverage	37
☑ Custom Coverage	18
○ Not Covered	141
Configurations	37
☑ Configured	28
☒ Misconfigured	9

Vulnerability Scanning
● Covered by Zscaler
● Correctly Configured

Zscaler Control
Deception - Threat Intelligence

Related Risk360 Factors	Licensed?
Known Vulnerabilities	Yes

Notes
Manually added notes will be displayed here.

Active Scanning ✕
ID: T1595 State: ● Covered by Zscaler (3 out of 3 sub-techniques)

Details
MITRE website link: https://attack.mitre.org/

MITRE Description
Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

MITRE Category	MITRE Value
Protect	Substantial

Zscaler Comment
Zscaler Private Access Application Connectors only ever make connections 'inside-out' - there are no remotely accessible ports and VPN fingerprints from inside the perimeter for adversaries to scan on the public internet.

TTP to Zscaler Product Mapping

Zscaler Control	Zscaler Private Access
Licensed?	Yes
Risk360 Category	External Attack Surface

TTP to Risk360 Factor Mapping

Sub-Technique	Risk360 Factor	Status
T1595.001	Exposed Servers	● Configured
T1595.002	Known Vulnerabilities	● Configured
T1595.003	Exposed Servers, Namespace...	● Configured

Notes
Manually added notes will be displayed here.

Figure 2: MITRE ATT&CK Framework Interface in Zscaler Risk360 Software

Simulate Feature

As Zscaler coverage shown in blue depicts the coverage based on customers' existing subscriptions, it is impera- tive to showcase the simulated coverage that a customer can potentially add with other remaining subscriptions. Hence to make it intuitive and aesthetically appealing, we created a separate simulated coverage view that the CISOs and executives could toggle on and interact with to understand the value of purchasing other Zscaler licences as shown in the figure below. Thus it can accelerate the decision-making process for customers and bring upsell opportunities for Zscaler.

Tying it Back to Remediation

As mentioned above, the coverage and visualization fulfil half of the objectives, and the remaining half is to convey whether the covered techniques were correctly configured or not. This was achieved by displaying the clear mapping between each sub-technique and the associated Risk360 contributing factors.

Future Work

Other frameworks (NIST CSF)

We envision that this innovative, security framework-based coverage visualization, and three panel-based approaches, can be used to fulfil other use cases such as representing the coverage based on the NIST CSF or NIST 800 frameworks [8].

GRC Teams

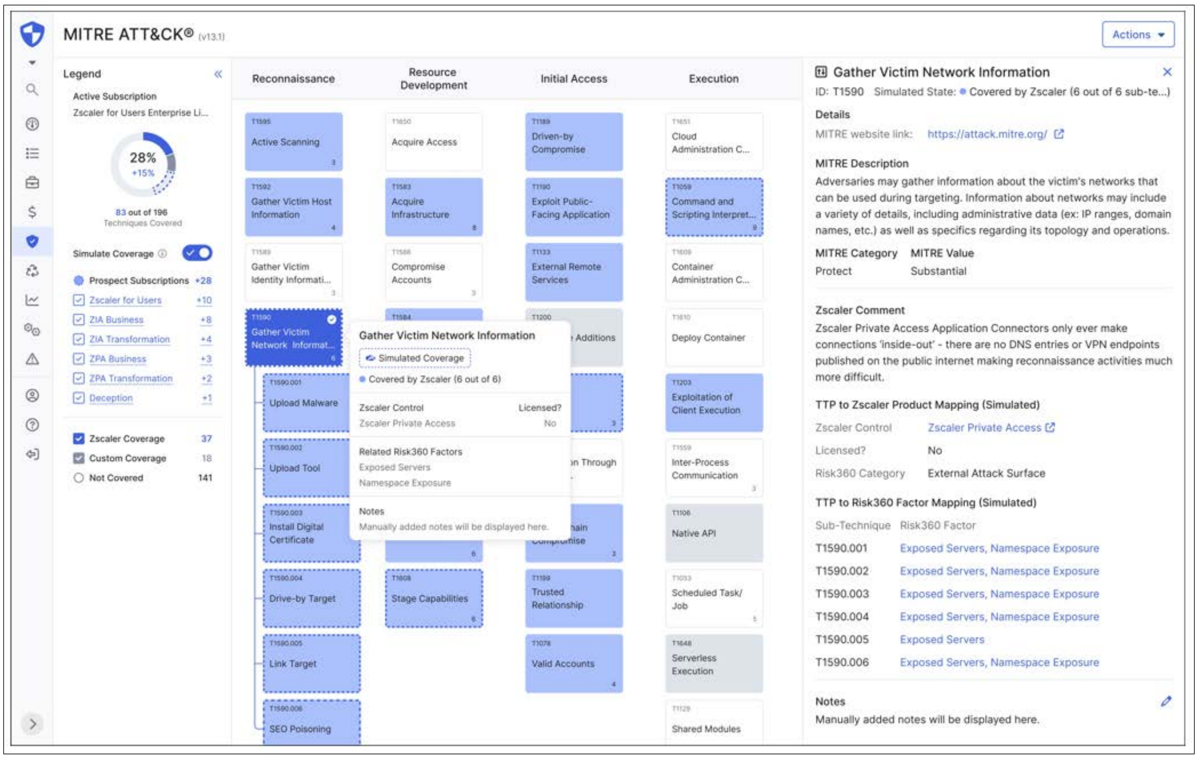
Typically governance risk and compliance teams, use multiple tools to audit, evaluate and understand different regulatory compliance statuses such as ISO, SOC2, GDPR, HIPAA, to name a few. This particular visualization may inspire further innovative workflows, where the additional dimension of compliance can be represented visually to provide a full picture of cyber security risk posture, to the concerned teams. Sales team.

Sales Team

We anticipate that the security coverage view along with the simulated coverage view would be beneficial to secondary personas such as salespersons who intend to use this risk360 product and this MITRE Attack framework to explain the capabilities and upsell more Zscaler services.

Risk Forecast/Prediction/TTP-Based Highlights

Besides the color-coded security coverages, this framework-based visualization can be leveraged to map different cyberattacks by highlighting various tactics, techniques, and procedures involved. It can be used to study different types and stages of cyberattacks to shape future risk predictions.



Gather Victim Network Information

ID: T1590 Simulated State: ● Covered by Zscaler (6 out of 6 sub-te...)

Details

MITRE website link: https://attack.mitre.org/

MITRE Description

Adversaries may gather information about the victim's networks that can be used during targeting. Information about networks may include a variety of details, including administrative data (ex: IP ranges, domain names, etc.) as well as specifics regarding its topology and operations.

MITRE Category	MITRE Value
Protect	Substantial

Zscaler Comment

Zscaler Private Access Application Connectors only ever make connections 'inside-out' - there are no DNS entries or VPN endpoints published on the public internet making reconnaissance activities much more difficult.

TTP to Zscaler Product Mapping (Simulated)

Zscaler Control	Zscaler Private Access
Licensed?	No
Risk360 Category	External Attack Surface

TTP to Risk360 Factor Mapping (Simulated)

Sub-Technique	Risk360 Factor
T1590.001	Exposed Servers, Namespace Exposure
T1590.002	Exposed Servers, Namespace Exposure
T1590.003	Exposed Servers, Namespace Exposure
T1590.004	Exposed Servers, Namespace Exposure
T1590.005	Exposed Servers
T1590.006	Exposed Servers, Namespace Exposure

Notes

Manually added notes will be displayed here.

Figure 3: MITRE ATT&CK Framework Simulate Coverage View

Conclusion

This paper explains how a user-centered design approach can be valuable in representing the complex information of security coverage based on the popular framework of MITRE ATT&CK. Using the color-coded layers approach on top of the original framework enhances usability and caters to multiple personas. With this innovative design solution, we can help cybersecurity professionals make sense of the complex data related to the security posture of the organization. With a thorough usability evaluation of this interface in the future, we hope that this novel approach will spark future conversations, and research directions in the cyber security and data visualization spaces.

References

1. MITRE ATT&CK. MITRE https://attack.mitre.org/.
2. Zscaler White Papers. Zscaler, Inc https://www.zscaler.com/resources?type=white-papers.
3. Zscaler Risk360 Help. Zscaler https://help.zscaler.com/risk360.
4. Zscaler Blog. Zscaler https://www.zscaler.com/blogs.
5. MITRE ATT&CK Navigator. MITRE https://mitre-attack.github.io/attack-navigator/.
6. Splunk Lantern: Assessing and Expanding MITRE ATT&CK Coverage in Splunk Enterprise Security. Splunk https://lantern.splunk.com/.
7. MITRE Coverage in Azure Sentinel. Microsoft https://learn.microsoft.com/en-us/azure/sentinel/mitre-coverage.
8. National Institute of Standards and Technology Cybersecurity Framework. NIST https://www.nist.gov/cyberframework.