THE MITRE ATT&CK® FRAMEWORK

AND YOUR PENETRATION TEST

Thomas Freeman, CISSP, CISA, CISM, GPEN, GCIH, GCWN

June, 2025

SIKICH®

ABOUT THOMAS

DIRECTOR of OFFENSIVE SERVICES

- Former life: (since 1989)
  - Development
  - CADD Trainer
  - Director of IT
  - College Educator (10,000+ hours)
- Information Security Certifications
  - General – CISSP (expired)
  - Auditor – CISA (expired)
  - Manager – CISM (expired)
  - Penetration Tester - GPEN
  - Incident Handler – GCIH
  - Intrusion Analyst - GCIA
  - Windows Security Administrator - GCWN
- Penetration Testing Consultant
- Forensic Investigator / Incident Response Consultant
- Security Awareness Trainer

SIKICH®

SIKICH OPERATIONAL **PILLARS**

GOVERNMENT SERVICES

AUDIT
Federal
State
Quality Control

Consulting
Federal
State

ASSURANCE, TAX & WEALTH MGT

ASSURANCE

TAX CONSULTING

WEALTH MANAGEMENT

CLIENT SOLUTIONS

RISK
GRC
SOC
Cybersecurity
Oracle Risk

TRANSACTION ADVISORY
Transaction Advisory
Investment Bank
Valuation Services

BUSINESS ADVISORY
Client Accounting Solutions
Human Capital
Marketing

DATA & AI
Data and AI Strategy
Ecosystem Modernization
Data Governance

MICROSOFT
ERP
CRM
Cloud Solutions

REGULATED INDUSTRIES
ERP
RQ&C
Salesforce

SIKICH®
ACCOUNTING TECHNOLOGY ADVISORY

ABOUT CYBERSECURITY

OUR INFORMATION SECURITY SERVICES

We help customers understand security and compliance risks, how to avoid them and what to do should a security incident occur.

- INCIDENT RESPONSE **CONSULTING**
- PENETRATION **TESTING**
- VULNERABILITY **SCANNING**
- IT **AUDITS**
- COMPLIANCE **ASSESSMENT**
- RISK **ADVISORY**
- SECURITY **AWARENESS TRAINING**

SIKICH®

SIKICH.COM

You perform regular penetration tests.

Executives want to see KPIs so they can have confidence that your security controls are working.

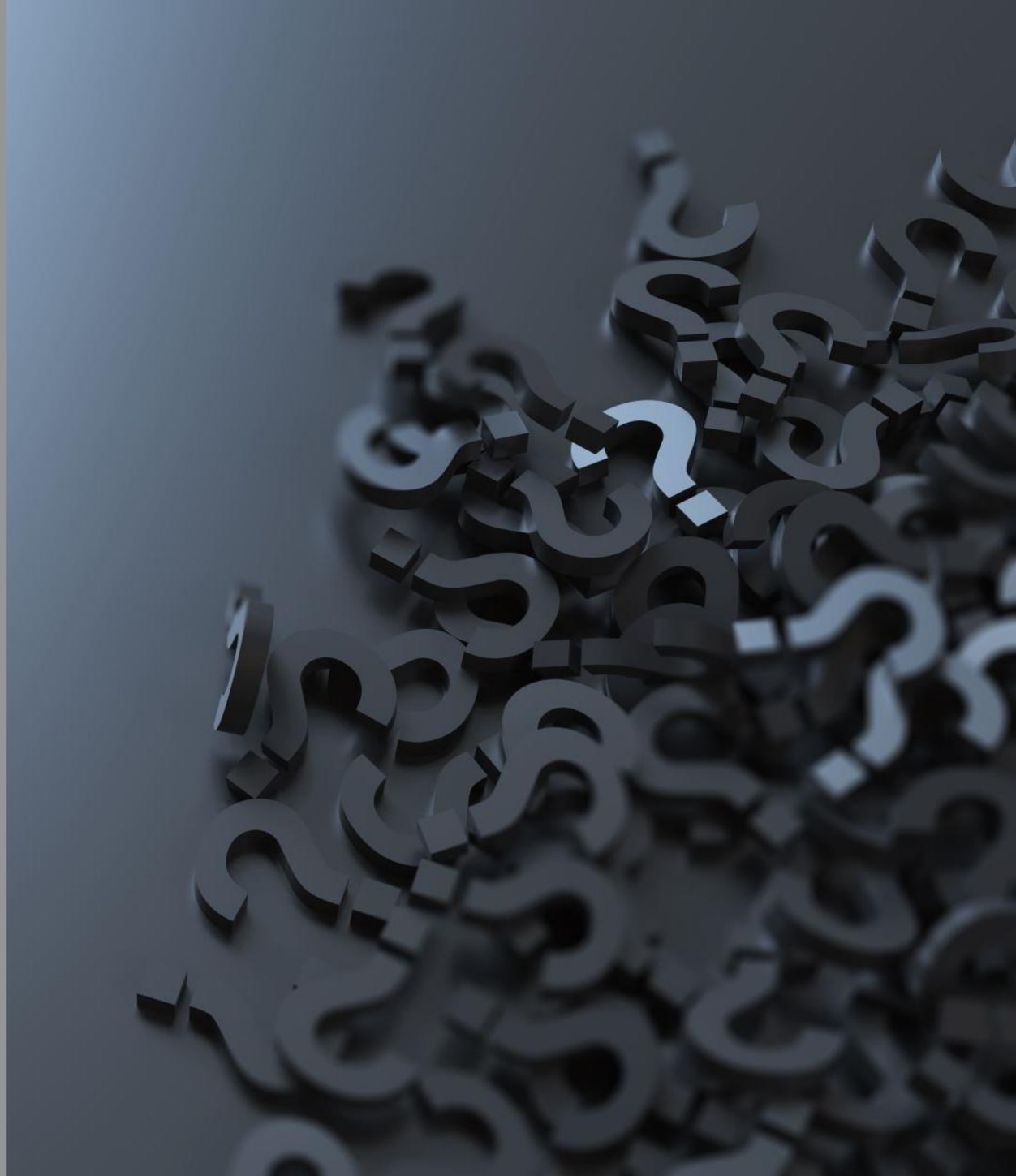
SIKICH®

Penetration test methodologies have become standardized, and you are getting similar results every year.

SIKICH®

How can you get more ROI from your penetration tests?

SIKICH®



THE MITRE ATT&CK® FRAMEWORK (MAF)

helps you perform testing specific to **YOUR THREATS** while measuring your security.

SIKICH®

Let’s take a moment to review a pen test.

SIKICH®

PREPARED FOR:

SAMPLE CLIENT, INC.

- *March 1, 2022* *Testing started*
- *May 9, 2022* *Testing completed*

SUBMITTED BY:

Sikich LLP
Thomas Freeman, OISSP, GPEN, GOIH, GOWN
MANAGER
13400 Bishops Lane, Suite 300
Brookfield, WI 53005
262.317.8512
thomas.freeman@sikich.com

PENETRATION TESTING METHODOLOGY

SIKICH®

SIKICH.COM

EXECUTIVE SUMMARY

RESULTS SUMMARY

Using automated and manual methods, Sikich attempted to discover and exploit system-, network- and application-layer vulnerabilities.

EXTERNAL TESTING

Sikich identified a web page that did not properly sanitize user input, which allowed for a reflected cross site scripting (XSS) attack to be performed. Sikich discovered that end-of-life software, including web servers, and Remote Desktop Protocol (RDP) were accessible from the Internet. The associated vulnerabilities disclosed users on the systems.

INTERNAL TESTING

Sikich attempted to gain unauthorized access to internal network targets. Sikich used several attack chains to discover resources and capture credentials. Sikich used the credentials to gain access to multiple systems where Sikich extracted additional credentials that allowed it to pivot within the environment and repeat the process. Sikich discovered an internal email server that allowed unrestricted email relaying and could be utilized for phishing or data exfiltration. Some hosts used weak remote desktop authentication or plaintext protocol services, or served applications that could be accessed with no or default credentials, including a tape backup system that provided Sikich with administrative access to the backup library. Sikich was unable to bypass endpoint detection and response (EDR) software on the hosts or compromise Active Directory domains.

The count of vulnerabilities for the entire penetration test was:

HIGH	MEDIUM	LOW
5	7	1

ATTACK NARRATIVE

ATTACK NARRATIVE

Sikich performed the following as part of the simulated attack against the Client environment.

RECONNAISSANCE

Sikich performed both passive and active reconnaissance on the Client digital presence, which focused on enumerating Client infrastructure and other pieces of information that could be used later in the penetration test.

Sikich performed domain-based enumeration using domain name server (DNS) brute forcing and targeted search queries to try discovering additional hostnames, IP addresses, web applications, sensitive corporate information and personal details about Client employees. Where applicable, and with Client's approval, Sikich added discovered targeting information to the scope of this engagement.

DISCLOSED CREDENTIALS

Sikich searched a database of publicly available third-party breach data for email addresses matching the *client.com* domain. Data breaches of Internet-connected organizations occur frequently, and these breaches often result in a public disclosure of email address and password data. Sikich identified unique credentials in publicly available breach data. Sikich attempted to leverage the credentials during testing but did not find evidence that the associated passwords were in use within the Client environment.

Client should consider implementing a program to proactively monitor publicly available breach data for signs of compromised accounts. One site that can assist in monitoring such information is the "Have I Been Pwned?" website via its *Domain search* functionality (**https://haveibeenpwned.com/DomainSearch**).

FINDINGS

END-OF-LIFE SOFTWARE

RISK: HIGH

Software that is no longer supported by the developer is likely to contain remotely exploitable vulnerabilities that may allow an attacker or a worm to take complete control of the remote systems.

DETAILS/HOSTS IMPACTED

Systems were running end-of-life software, including the following instance Sikich identified.

IP ADDRESS	PORT	DESCRIPTION
109.203.112.163	1433/tcp	Microsoft SQL Server 2014 12.00.5000, SP2
198.163.185.80	---	Microsoft Windows Server 2008 R2

RECOMMENDATIONS

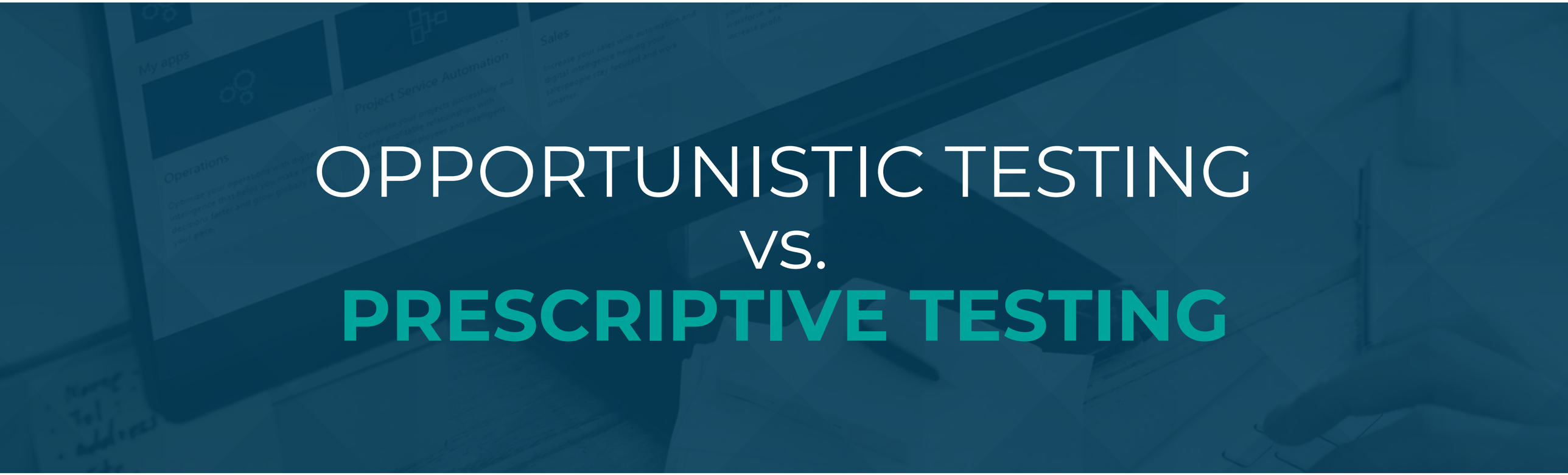
Client should:

- Upgrade software to versions actively supported by the developer
- Inspect their environment to verify there are no other instances of end-of-life software
- Apply all service packs and critical updates for all services and verify that the installed patch levels of the services are not susceptible to the vulnerabilities

ADDITIONAL REFERENCES

NIST Special Publication 800-40 Rev. 3: Guide to Enterprise Patch Management Technologies

https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final



OPPORTUNISTIC TESTING
VS.
PRESCRIPTIVE TESTING

SIKICH®

OPPORTUNISTIC TESTING

1. Identify the extent of scope
    - Deep dive OSINT review
    - External footprint
    - Cloud footprint
    - Social engineering targets
    - Internal networks
    - Mobile applications
    - Web applications
    - Wi-Fi networks
    - Physical locations

OPPORTUNISTIC TESTING

2. Test the scope
    - Live hosts scanning
    - Service fingerprinting
    - Vulnerability scanning
    - Identify points of interest and manually exploit
3. Report
    - Findings sorted by severity
    - Attack narrative (when present) may provide information on how findings can be chained for impact.
4. Retest any remediated findings

PRESCRIPTIVE TESTING

1. Identify the extent of scope
    - Deep dive OSINT review
    - External footprint
    - Cloud footprint
    - Social engineering targets
    - Internal networks
    - Mobile applications
    - Web applications
    - Wi-Fi networks
    - Physical locations
    - Threat actors who commonly target your industry

SIKICH®

PRESCRIPTIVE TESTING

2. Test the scope
    - Live hosts scanning
    - Service fingerprinting
    - Vulnerability scanning
    - Identify points of interest and compare to map of attacks common to your industry
    - Consider how Advanced Persistent Threat (APT) actors chain these attacks and then exploit
3. Report
    - Findings sorted by severity
    - Attack narrative maps to common industry attacks and describes the chain that creates greatest impact (which may have a lower severity finding as the key pin).
4. Retest any remediated findings

RED TEAM, PURPLE TEAM, PENTEST = PRESECRIPTIVE PENTEST

RED TEAM = Extremely narrow scope, longer engagements, designed to emulate an APT, test the SOC's ability to detect and respond appropriately. NO communication between testing and SOC analysts.

PURPLE TEAM = Narrow scope, focus is on training SOC to detect and respond appropriately. LOTS of communication between testing and SOC analysts.

PENTEST = Broad scope, no effort to hide. The focus is on determining if security controls are detecting and blocking a large breadth of malicious activity. Some communication between testing team and SOC Analysts.

PRESCRIPTIVE PENTEST = Broad scope, no effort to hide. The focus is on making sure security controls are detecting malicious activity that is commonly used in attacks against your industry. Some communication between testing team and SOC Analysts.

SIKICH®

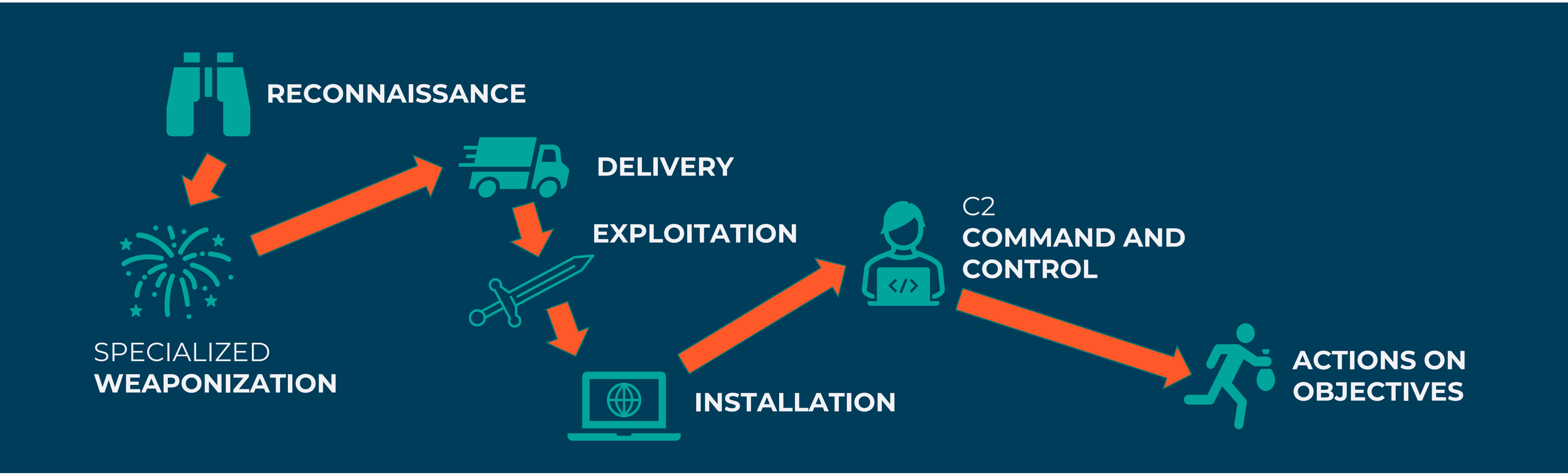
NOW LET ME INTRODUCE THE

MITRE ATT&CK® FRAMEWORK (MAF)

SIKICH®

THE CYBER KILL CHAIN

DEVELOPED BY LOCKHEED MARTIN
What adversaries must complete in order to achieve their objectives

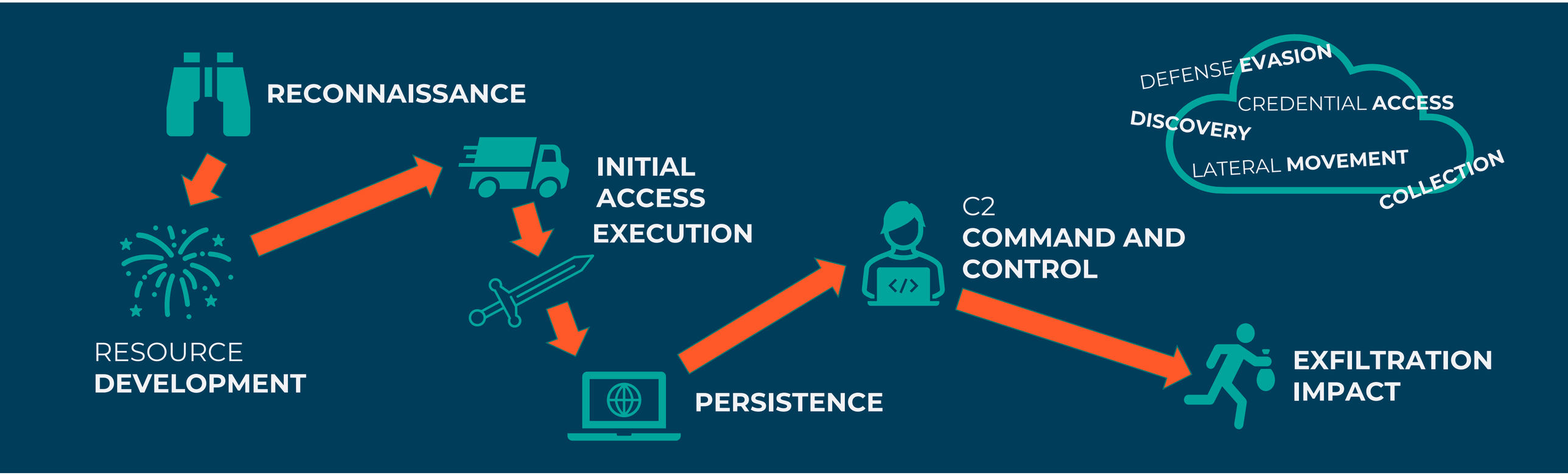


SIKICH®

SIKICH.COM

THE MITRE ATTACK®

KNOWLEDGE BASE OF TACTICS, TECHNIQUES AND PROCEDURES (TTP)
A foundation for the development of specific threat models specific to your industry



SIKICH®

SIKICH.COM

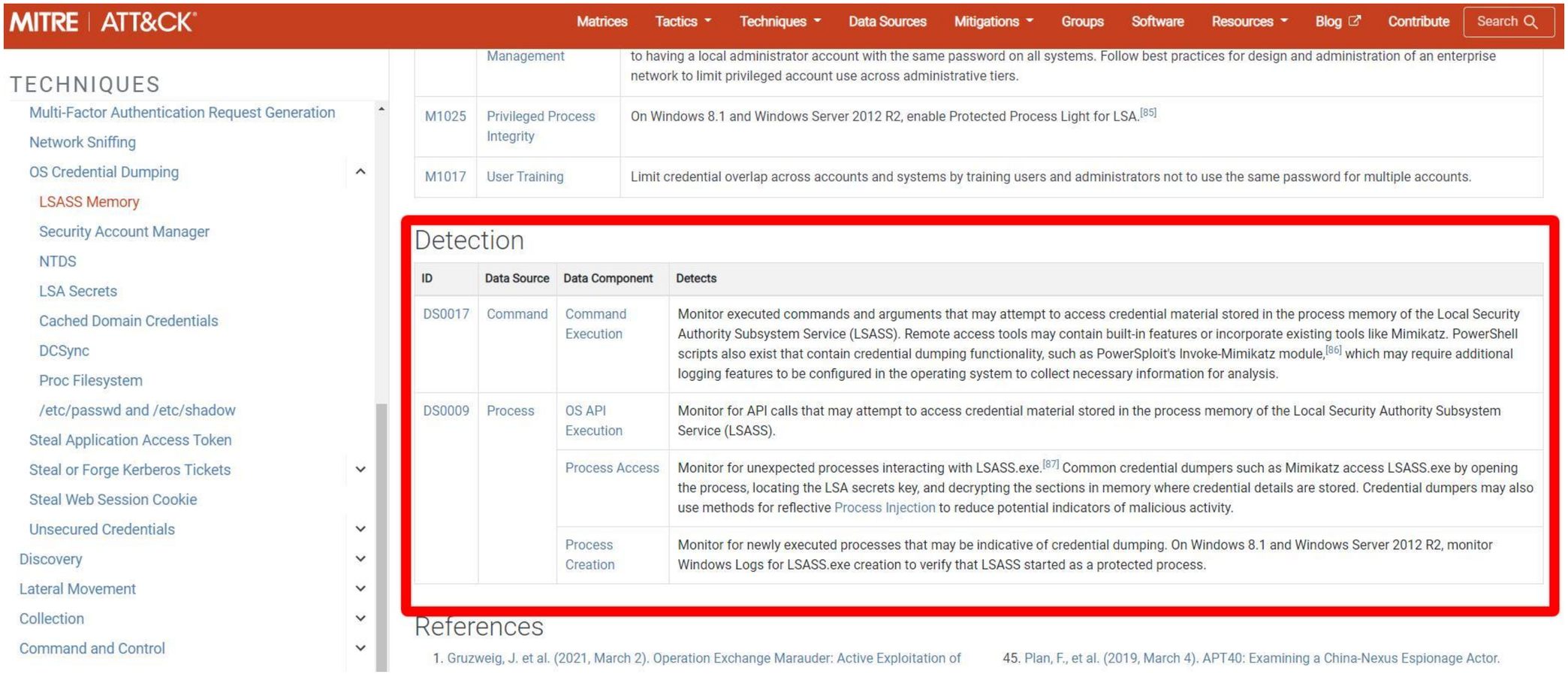
THE MITRE ATTACK®

USING THE MAF

you can prescribe TTPs
that your security team can use to measure
your ability to detect and respond.

SIKICH®

THE MITRE ATTACK®



MITRE | ATT&CK®

Matrices Tactics Techniques Data Sources Mitigations Groups Software Resources Blog Contribute Search

TECHNIQUES

- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping
  - LSASS Memory
  - Security Account Manager
  - NTDS
  - LSA Secrets
  - Cached Domain Credentials
  - DCSync
  - Proc Filesystem
  - /etc/passwd and /etc/shadow
- Steal Application Access Token
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Unsecured Credentials
- Discovery
- Lateral Movement
- Collection
- Command and Control

	Management	to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.
M1025	Privileged Process Integrity	On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA.[85]
M1017	User Training	Limit credential overlap across accounts and systems by training users and administrators not to use the same password for multiple accounts.

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). Remote access tools may contain built-in features or incorporate existing tools like Mimikatz. PowerShell scripts also exist that contain credential dumping functionality, such as PowerSploit's Invoke-Mimikatz module,[86] which may require additional logging features to be configured in the operating system to collect necessary information for analysis.
DS0009	Process	OS API Execution	Monitor for API calls that may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS).
		Process Access	Monitor for unexpected processes interacting with LSASS.exe.[87] Common credential dumpers such as Mimikatz access LSASS.exe by opening the process, locating the LSA secrets key, and decrypting the sections in memory where credential details are stored. Credential dumpers may also use methods for reflective Process Injection to reduce potential indicators of malicious activity.
		Process Creation	Monitor for newly executed processes that may be indicative of credential dumping. On Windows 8.1 and Windows Server 2012 R2, monitor Windows Logs for LSASS.exe creation to verify that LSASS started as a protected process.

References

1. Gruzweig, J. et al. (2021, March 2). Operation Exchange Marauder: Active Exploitation of

45. Plan, F., et al. (2019, March 4). APT40: Examining a China-Nexus Espionage Actor.

SIKICH®

THE MITRE ATTACK®

MAF focuses on ATTACKS

TESTING focuses on VULNERABILITIES
that are targeted during attacks

SIKICH®

THE MITRE ATTACK®

PLAINTEXT PASSWORDS ACCESSIBLE VIA LSASS

RISK: HIGH

In order to support legacy single sign-on (SSO), Windows stores NTLM credential hashes and passwords in plaintext in the Local Security Authority Subsystem Service (LSASS). This storage can allow an attacker with SYSTEM privileges to retrieve these hashes and plaintext passwords via tooling such as Mimikatz. NTLM hashes may be passed to other systems for access in place of passwords. Storing passwords in plaintext negates the need for any cracking effort, regardless of password length or complexity.

DETAILS/HOSTS IMPACTED

Hosts stored plaintext credentials using reversible encryption within LSASS, including the following instances Sikich identified.

HOST	HOSTNAME	WINDOWS VERSION
[Redacted]	[Redacted]	Windows 7
[Redacted]	[Redacted]	Windows 7

RECOMMENDATIONS

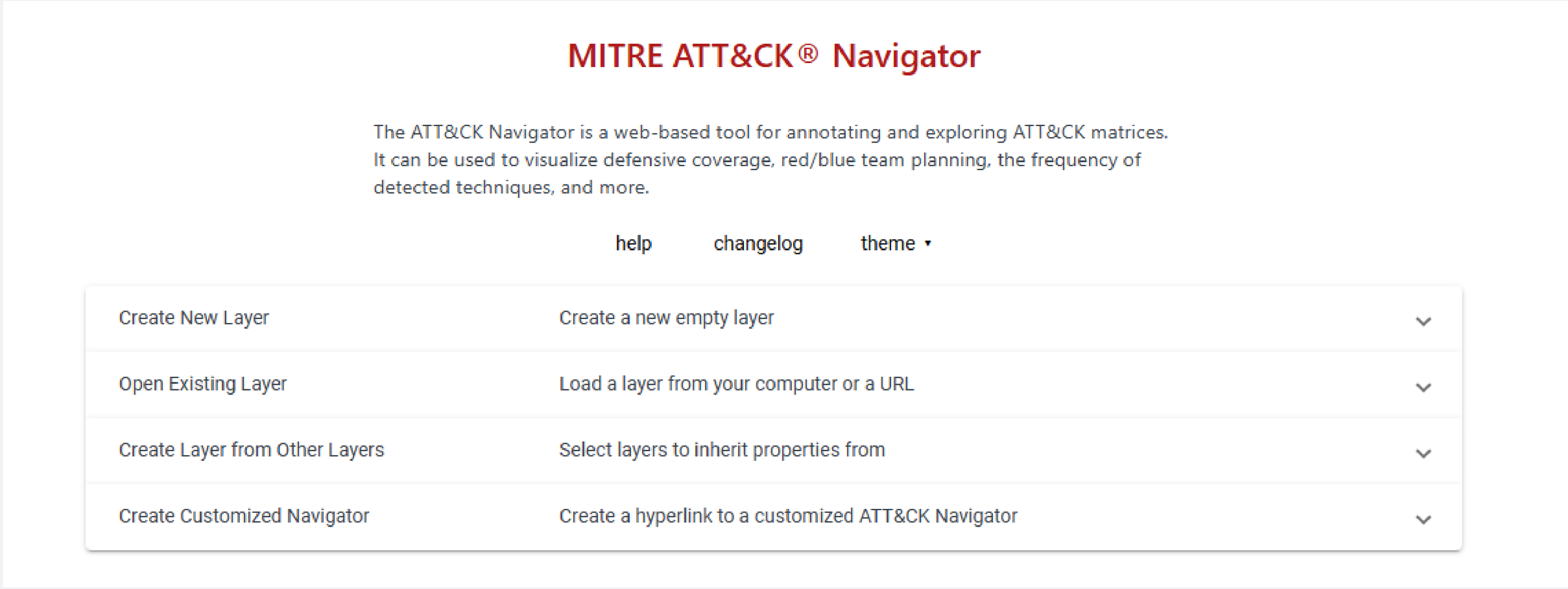
Client should:

- Implement Local Security Authority (LSA) protection

MAF - PRESCRIPTIVE NAVIGATOR **WALK THROUGH**

SIKICH®

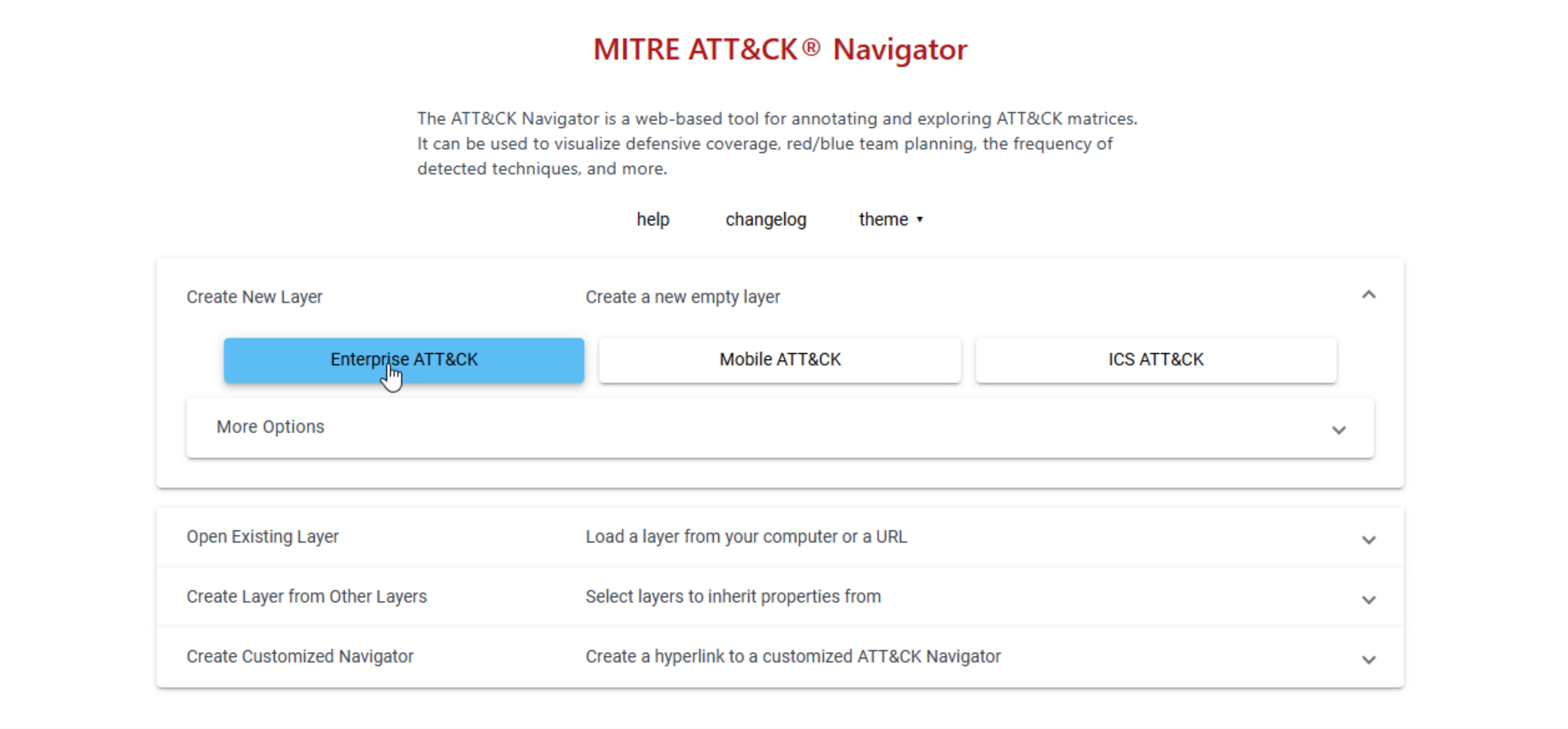
THE MITRE ATTACK® Navigator



SIKICH®

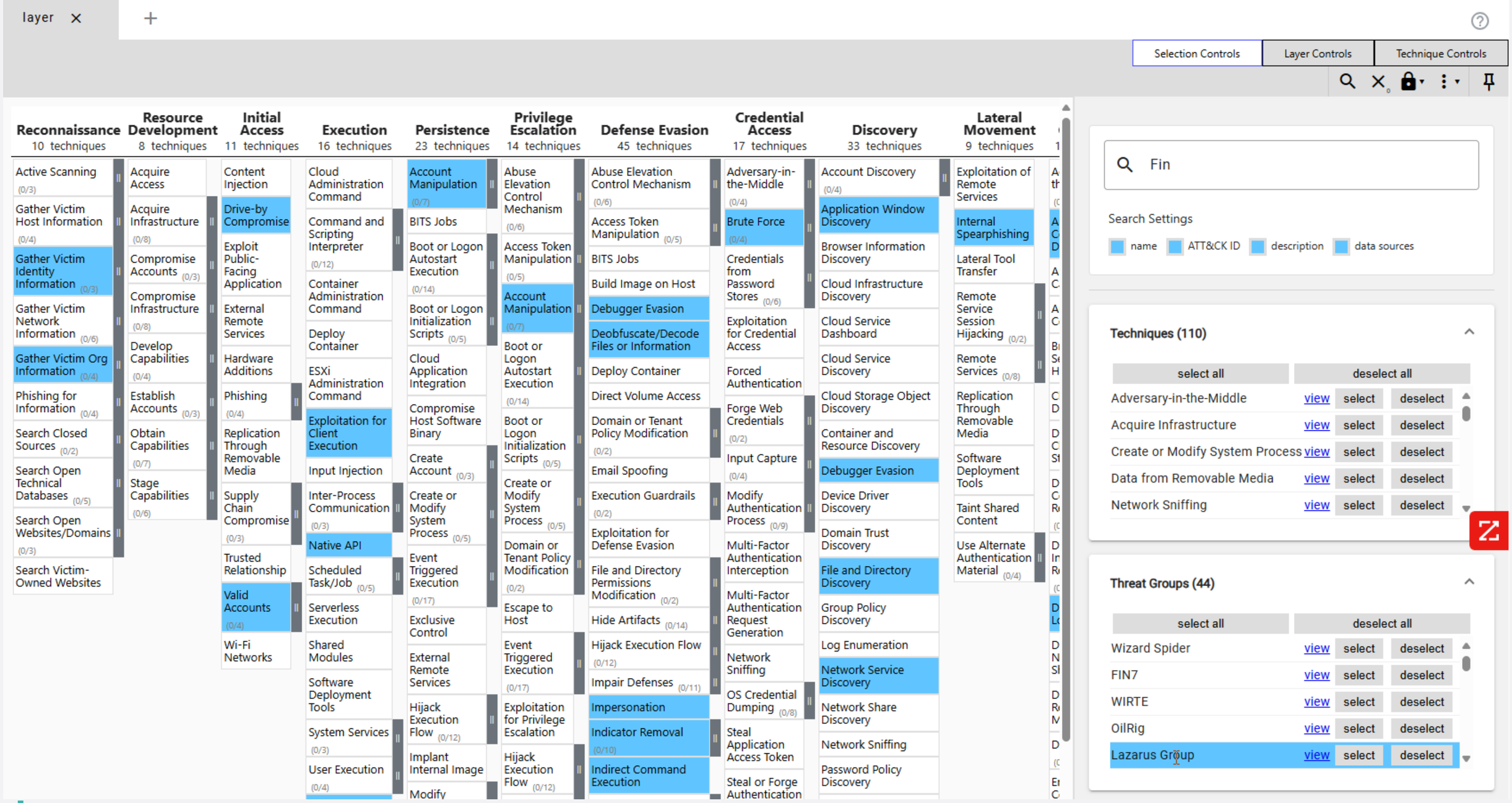
SIKICH.COM

THE MITRE ATTACK® Navigator



SIKICH®

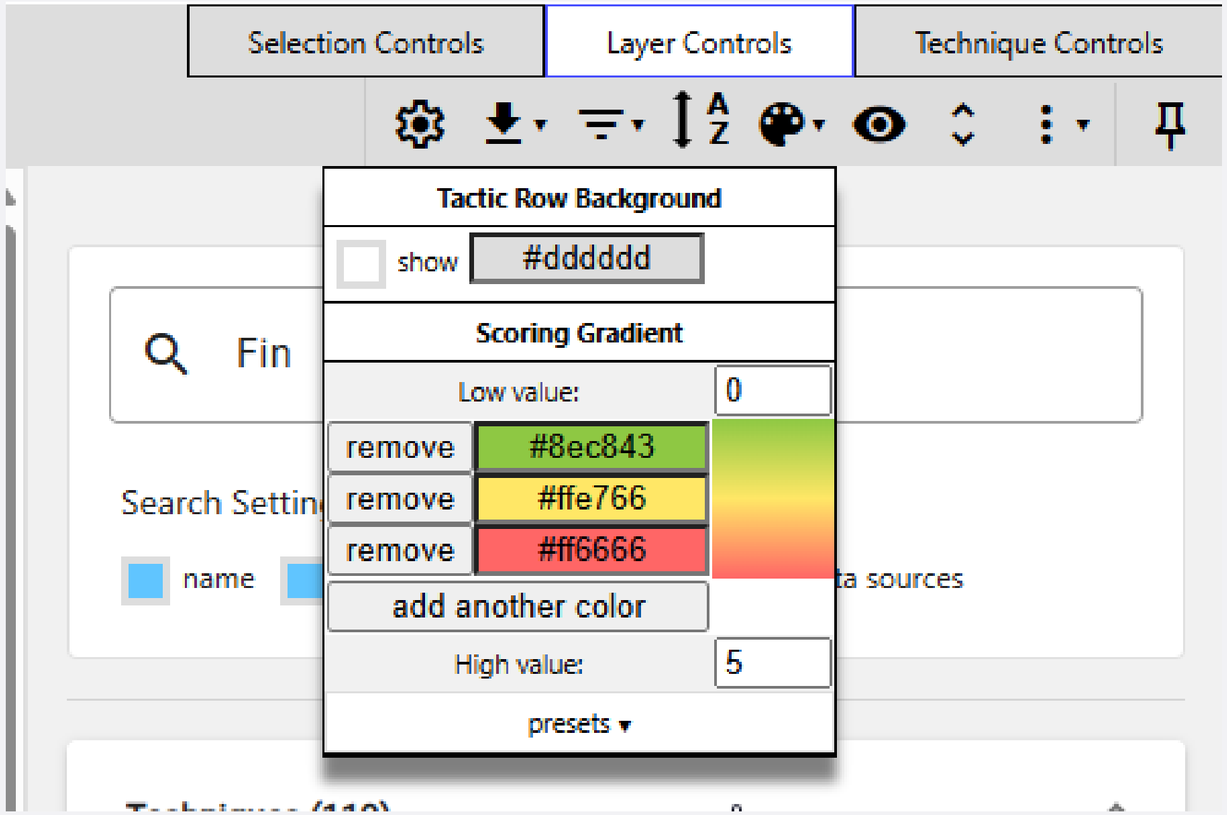
SIKICH.COM

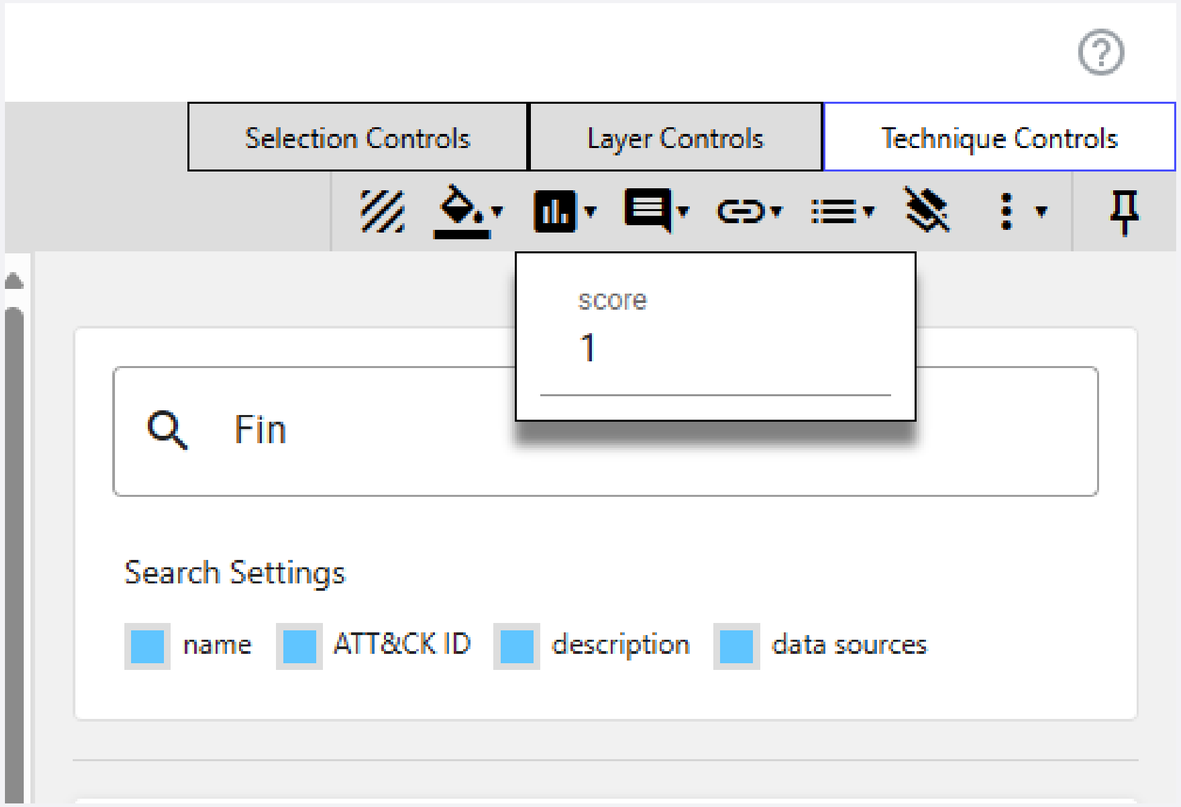


SIKICH®

SIKICH.COM

THE MITRE ATTACK® Navigator

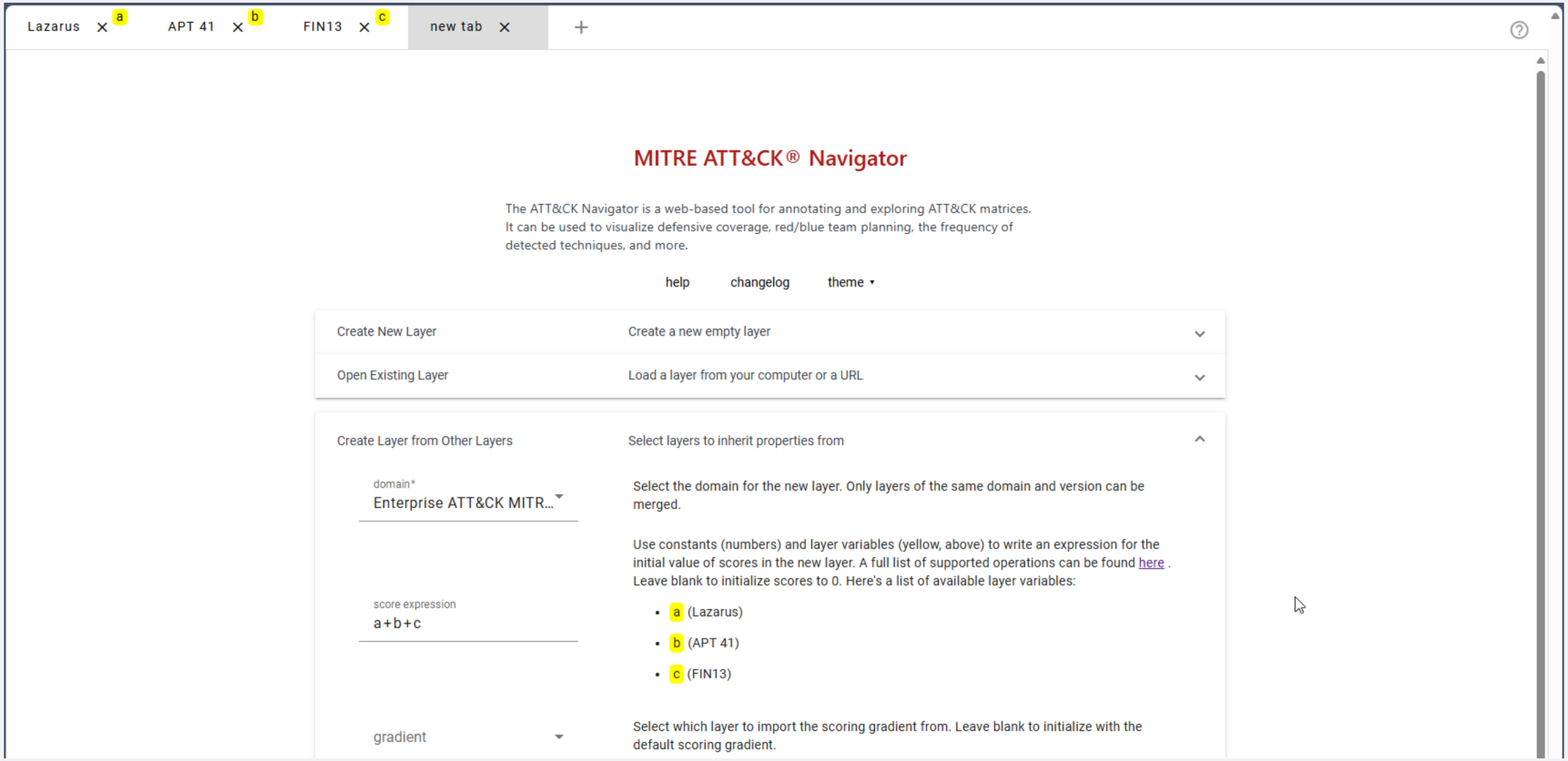




SIKICH®

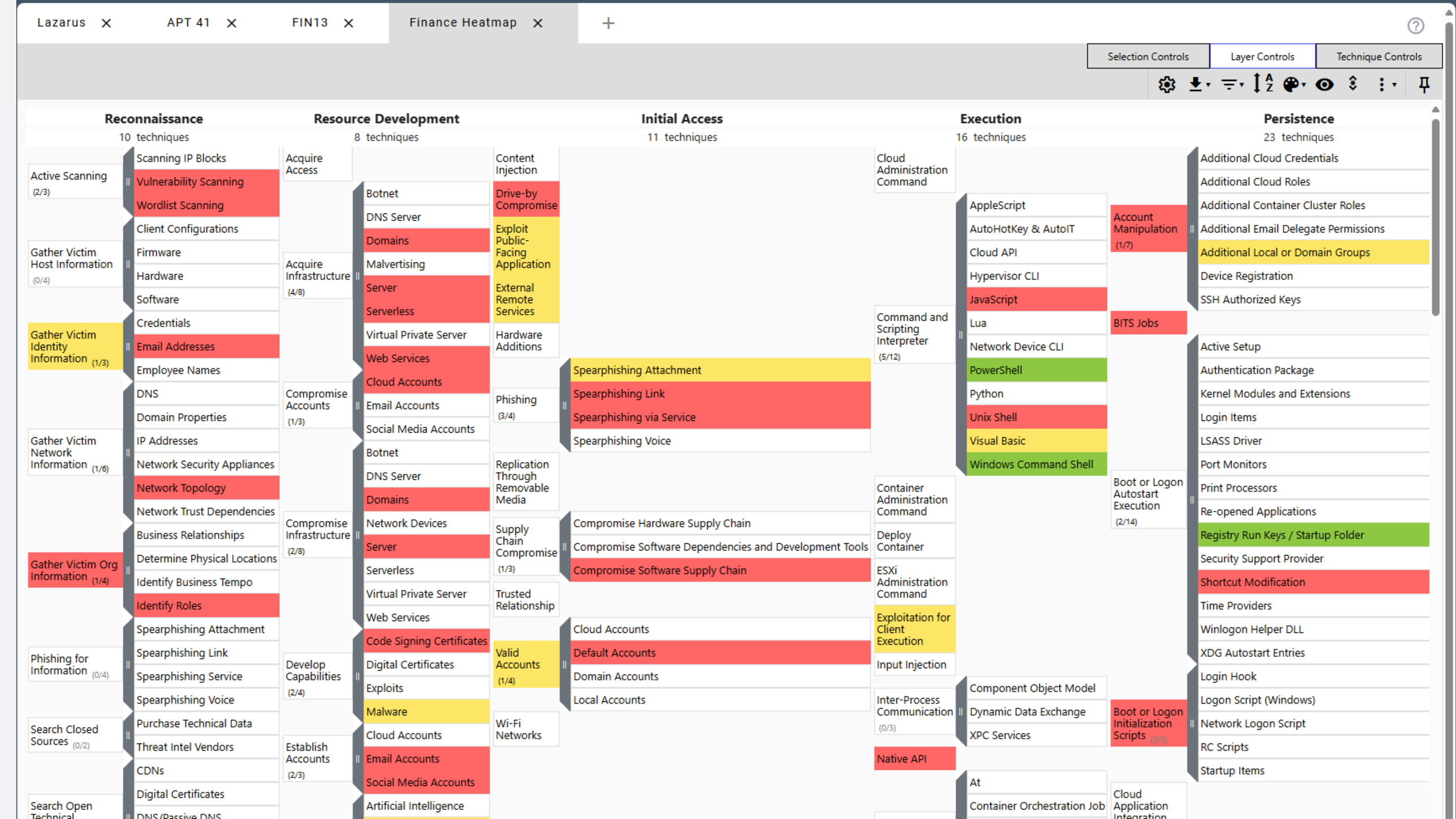
SIKICH.COM

THE MITRE ATTACK® Navigator



SIKICH®

SIKICH.COM


Lazarus
APT 41
FIN13
Finance Heatmap
Selection Controls
Layer Controls
Technique Controls
Reconnaissance
10 techniques
Active Scanning (2/3)
Scanning IP Blocks
Vulnerability Scanning
Wordlist Scanning
Gather Victim Host Information (0/4)
Client Configurations
Firmware
Hardware
Software
Gather Victim Identity Information (1/3)
Credentials
Email Addresses
Employee Names
Gather Victim Network Information (1/6)
DNS
Domain Properties
IP Addresses
Network Security Appliances
Network Topology
Network Trust Dependencies
Gather Victim Org Information (1/4)
Business Relationships
Determine Physical Locations
Identify Business Tempo
Identify Roles
Phishing for Information (0/4)
Spearphishing Attachment
Spearphishing Link
Spearphishing Service
Spearphishing Voice
Search Closed Sources (0/2)
Purchase Technical Data
Threat Intel Vendors
Search Open Technical
CDNs
Digital Certificates
DNS/Passive DNS
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (4/8)
Botnet
DNS Server
Domains
Malvertising
Server
Serverless
Virtual Private Server
Web Services
Compromise Accounts (1/3)
Cloud Accounts
Email Accounts
Social Media Accounts
Compromise Infrastructure (2/8)
Botnet
DNS Server
Domains
Network Devices
Server
Serverless
Virtual Private Server
Web Services
Develop Capabilities (2/4)
Code Signing Certificates
Digital Certificates
Exploits
Malware
Establish Accounts (2/3)
Cloud Accounts
Email Accounts
Social Media Accounts
Artificial Intelligence
Initial Access
11 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (3/4)
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Spearphishing Voice
Replication Through Removable Media
Supply Chain Compromise (1/3)
Compromise Hardware Supply Chain
Compromise Software Dependencies and Development Tools
Compromise Software Supply Chain
Trusted Relationship
Valid Accounts (1/4)
Cloud Accounts
Default Accounts
Domain Accounts
Local Accounts
Wi-Fi Networks
Execution
16 techniques
Cloud Administration Command
Command and Scripting Interpreter (5/12)
AppleScript
AutoHotKey & AutoIT
Cloud API
Hypervisor CLI
JavaScript
Lua
Network Device CLI
PowerShell
Python
Unix Shell
Visual Basic
Windows Command Shell
Container Administration Command
Deploy Container
ESXi Administration Command
Exploitation for Client Execution
Input Injection
Inter-Process Communication (0/3)
Component Object Model
Dynamic Data Exchange
XPC Services
Native API
At
Container Orchestration Job
Persistence
23 techniques
Account Manipulation (1/7)
Additional Cloud Credentials
Additional Cloud Roles
Additional Container Cluster Roles
Additional Email Delegate Permissions
Additional Local or Domain Groups
Device Registration
SSH Authorized Keys
BITS Jobs
Active Setup
Authentication Package
Kernel Modules and Extensions
Login Items
LSASS Driver
Port Monitors
Print Processors
Boot or Logon Autostart Execution (2/14)
Re-opened Applications
Registry Run Keys / Startup Folder
Security Support Provider
Shortcut Modification
Time Providers
Winlogon Helper DLL
XDG Autostart Entries
Boot or Logon Initialization Scripts (0/5)
Login Hook
Logon Script (Windows)
Network Logon Script
RC Scripts
Startup Items
Cloud Application Integration

MAF – REMEDIATION ENTERPRISE TECHNIQUES / D3FEND **WALK THROUGH**

SIKICH®

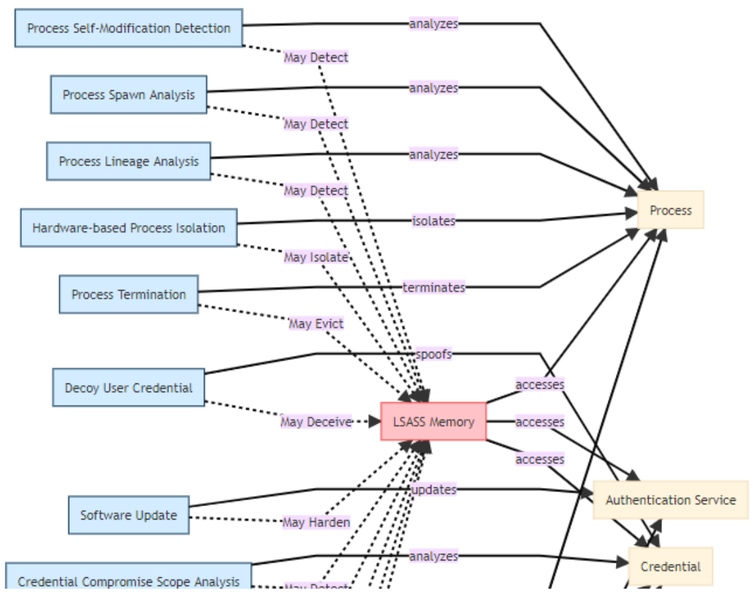
THE MITRE ATTACK®

LSASS Memory - T1003.001

(ATT&CK® Technique)

D3FEND Inferred Relationships

Browse the D3FEND knowledge graph by clicking on the nodes below.



SIKICH®

SIKICH.COM

MAF – POST TEST ANALYSIS
DISCUSSION

SIKICH®

THE MITRE ATTACK®

1. CORRELATE THE FINDINGS
with the tactics, techniques and procedures
that revealed the vulnerabilities.
2. ALIGN CONTROLS
so that you detect and properly respond to
the corresponding attacks

SIKICH®

TIPS
BEST PRACTICE

SIKICH®

TIPS

- **ATTACK NARRATIVE:** Required if you are going to effectively use MAF.
- **REPORTS:** Break narrative up to reflect specific TTPs.
- **ATTACK NAVIGATOR:** Use layers to create custom maps of attack chains.
  - **PEN TEST ANALYSIS:** Use layers to show TTPs from the pentest.
  - **APT ANALYSIS:** Use layers to show specific APT groups.
  - **HEATMAPS:** Create a new layer combining previous layers to highlight most common attacks.
  - **EXPORT:** Export to SVG and EXCEL for reporting purposes

RESOURCES

- **MITRE ATT&CK®**
  https://attack.mitre.org/
- **ATT&CK® Navigator (mitre-attack.github.io)**
  https://mitre-attack.github.io/attack-navigator/
- **ATTACK-Tools: Utilities for MITRE™ ATT&CK (github.com)**
  https://github.com/nshalabi/ATTACK-Tools
- **Insider Threat Tactics, Techniques, and Procedures (TTP) Knowledge Base**
  https://github.com/center-for-threat-informed-defense/insider-threat-ttp-kb
- **MITRE D3FEND™ – A knowledge graph of cybersecurity countermeasures**
  https://d3fend.mitre.org/
- **MITRE ATT&CK Windows Logging Cheat Sheets**
  https://github.com/MalwareArchaeology/ATTACK
- **Best Practices for MITRE ATT&CK® Mapping (cisa.gov)**
  https://www.cisa.gov/uscert/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf
- **CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™) (mitre.org)**
  https://capec.mitre.org/
- **CWE - Common Weakness Enumeration (mitre.org)**
  https://cwe.mitre.org/

THANK YOU

FOR YOUR TIME

Thomas Freeman, CISSP, CISM, CISA, GPEN, GCIH, GCIA, GCWN

SIKICH®

SIKICH®

ACCOUNTING TECHNOLOGY ADVISORY

LinkedIn: www.linkedin.com/company/sikich
Facebook: www.facebook.com/sikichllp
Twitter: www.twitter.com/sikichllp
Blog: www.sikich.com/insights

SIKICH.COM