safous

MITRE ATT&CK MITIGATION CHECKLIST

Mitigate ATT&CK Techniques With Safous Privileged Remote Access

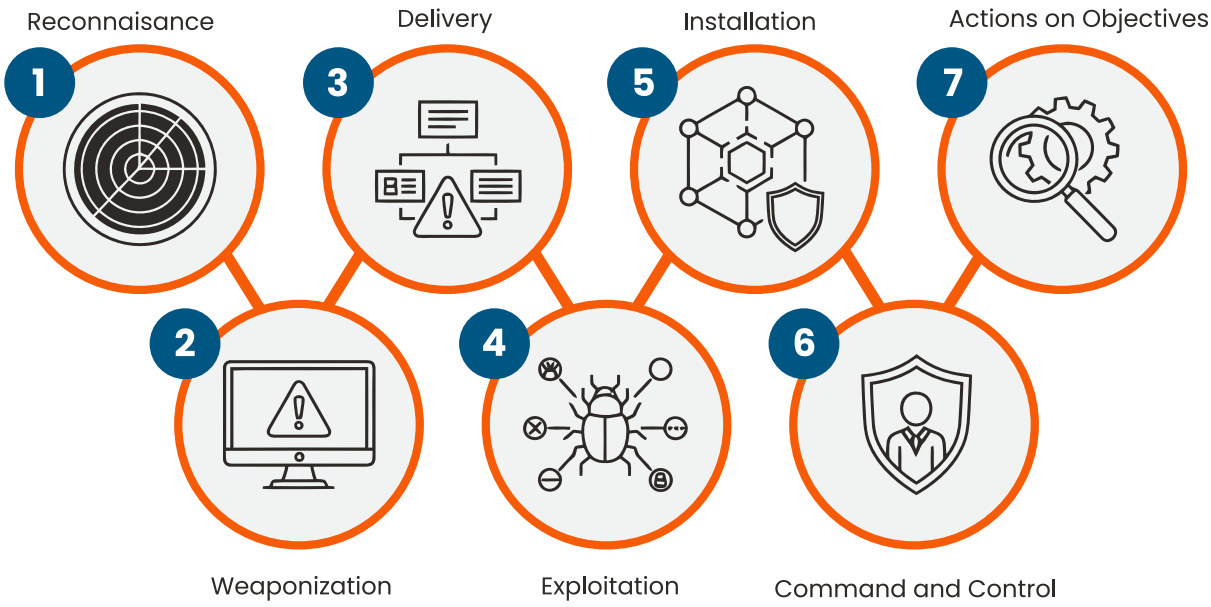
MITRE ATT&CK is a knowledge base of attacker tactics and techniques based on real-world observations. It's not a product taxonomy but a structured framework for adversary behavior that outlines attackers' goals, methods, and the conditions under which attacks succeed or fail.

Privileged remote access is a critical attack vector in both Enterprise and ICS environments, with adversaries typically targeting unprotected remote administration tools, third-party and vendor access, and vulnerabilities in IT/OT systems.

MITRE ATT&CK defines different tactic structures for Enterprise and ICS environments. Tactic names, emphasis, and tactical groupings do not map 1:1 between environments. But while the framework defines different tactical structures for these environments, many attacker techniques – especially those involving privileged remote access – are shared across both.

This checklist is designed to help organizations understand how Safous Privileged Remote Access mitigates real-world attacker behaviors described in the MITRE ATT&CK framework. It is not a compliance or certification checklist. It is an ATT&CK-informed, behavior-based mitigation checklist showing how Safous helps reduce the likelihood of attacker techniques succeeding through misuse of privileged remote access in both Enterprise and ICS environments.

The Cyber Kill Chain



This Cyber Kill Chain diagram provides a high-level illustrative flow. MITRE ATT&CK complements it by describing detailed adversary behaviors (tactics and techniques) that may occur in different orders, repeat, or be skipped depending on the attack.

Safous × MITRE ATT&CK for Enterprise

ATT&CK Tactic	ATT&CK Technique	Attacker Objective	Safous Mitigation
Reconnaissance Note: *Reconnaissance is addressed indirectly through attack surface reduction and Zero Trust access hiding. Safous does not detect reconnaissance activities, but prevents them from yielding actionable entry points.*	**T1593 –** Search Open Websites / Domains	Identify exposed IT remote access entry points	Hides remote access entry points, so they're not discoverable from the internet.
	T1046 – Network Service Discovery	Enumerate reachable services	No VPN gateways or exposed remote management endpoints exist.
Initial Access	**T1133 –** External Remote Services	Gain access via VPN/RDP/SSH	Remote access does not rely on VPN or network-level connectivity.
	T1078 – Valid Accounts	Log in using stolen credentials	Requires identity, device, and contextual verification for all access requests.
Execution	**T1059 –** Command-Line Interface	Execute commands after login	Limits remote sessions to approved applications only.
Persistence	**T1098 –** Account Manipulation	Maintain long-term privileged access	Grants access only when needed; supports just-in-time access.
	T1136 – Create Account	Establish backdoor admin accounts	New account creation requires approval and audit logging.
Privilege Escalation	**T1068 –** Exploitation for Privilege Escalation	Gain elevated privileges	Supports task- and role-specific privileged access policies.
	T1078 – Valid Accounts	Use existing high-privilege accounts	Separates high-privilege accounts from standard user accounts.
Lateral Movement	**T1021 –** Remote Services	Move across internal systems	Access to one system does not imply access to others.
Command and Control	**T1071 –** Application Layer Protocol	Control systems covertly	Remote sessions are fully visible and auditable.
Exfiltration Note: *Safous mitigates exfiltration risks specifically within privileged remote access sessions, rather than providing full data loss prevention across all network channels.*	**T1041 –** Exfiltration Over C2 Channel	Steal data via remote access tunnel	Restricts, controls, and audits file transfer activities within privileged sessions, preventing unauthorized data exfiltration over command-and-control channels.

Safous × MITRE ATT&CK for ICS

ATT&CK Tactic	ATT&CK Technique	Attacker Objective	Safous Mitigation
Initial Access	**T1133 –** External Remote Services	Access control systems via vendor remote connections	Vendor remote access is not permanently exposed.
	T1078 – Valid Accounts	Use shared or vendor credentials	Requires identity, device, and contextual verification for all access requests.

ATT&CK Tactic	ATT&CK Technique	Attacker Objective	Safous Mitigation
Execution	**T1021 –** Remote Services	Perform engineering or control actions	Limits remote sessions to approved systems and applications.
	T1059 – Command-Line Interface	Execute control logic modifications	Only permits explicitly approved commands and actions.
Persistence	**T1078 –** Valid Accounts	Retain long-term maintenance access	Eliminates permanent vendor and engineer access.
	T1098 – Account Manipulation	Preserve access across maintenance cycles	Grants access only when needed; supports just-in-time access.
Privilege Escalation	**T1078 –** Valid Accounts	Obtain engineering-level privileges	Supports task- and role-specific privileged access policies.
	T0820 – Abuse Elevation Control Mechanism	Bypass safety interlocks	Escalation to control-critical functions requires explicit approval.
Lateral Movement	**T1021 –** Remote Services	Pivot from IT to OT environments	Prevents network-wide reachability between IT and OT.
	T1078 – Valid Accounts	Move across engineering networks	Isolates access by system, function, and role.
Command and Control	**T1021 –** Remote Services	Control systems via legitimate management paths	All privileged sessions are recorded and auditable.
Inhibit Response Function	**T0831 –** Modify Control Logic	Disable alarms or safety responses	Only permits explicitly approved maintenance actions.
Impact	**T0827 –** Loss of Control	Cause physical or operational impact	Access restrictions block unauthorized control actions.

***Note:** The Attacker Objective column represents attacker behaviors defined by the MITRE ATT&CK framework, while the Safous Mitigation column describes enforced security conditions that prevent those behaviors from succeeding. This mapping is ATT&CK-informed and intended as a behavior-based mitigation reference, not a compliance or coverage claim.*

Mitigate ATT&CK-Relevant Threats in Enterprise and ICS Environments

MITRE ATT&CK describes how real attackers operate. Many of their highest-impact techniques in both Enterprise and ICS environments – initial access, persistence, lateral movement, and command and control – depend on privileged remote access.

Safous Privileged Remote Access helps organizations mitigate these tactics with:

- **Removing internet-visible entry points** and minimizing exposed attack surface, reducing reconnaissance effectiveness.
- **Enforcing Zero Trust access,** including identity verification, device posture checks, and contextual verification.
- **Eliminating standing privileged access** with JIT, granting privileges only when needed and revoking them after use.

With Safous, organizations gain environment-specific controls to help stop ATT&CK-defined attack paths in practice, not just on paper.

Contact us today to get started.

EXPLORE SAFOUS