Understanding the MITRE ATT&CK Framework: a Comprehensive Guide

Cybersecurity teams today face a constantly shifting threat landscape. Attackers are refining their methods, automating exploitation, and targeting identity systems with increasing precision. As a result, traditional perimeter-based defenses are no longer adequate. Organizations must adopt a more structured, intelligence-led approach to threat detection and response.

The MITRE ATT&CK Framework provides that structure. It is a globally recognized knowledge base of tactics and techniques, derived from real-world observations. The framework maps the entire attack lifecycle across 14 core tactics, each representing a specific objective an attacker seeks to accomplish. These tactics include actions like gaining access, executing code, escalating privileges, evading defenses, and causing impact. Together, they form the foundation of the ATT&CK Enterprise Matrix, which security teams can use to analyze and defend against attacks with greater clarity and purpose.

For CISOs, the MITRE ATT&CK Framework offers a strategic look into how attackers operate. It allows leaders to prioritize investments, measure security program effectiveness, and communicate technical risk in business terms. The framework also helps align security initiatives with broader enterprise risk and resilience goals.

For security operations teams, MITRE ATT&CK is a tactical playbook. It breaks down each phase of an attack into observable techniques that can be monitored, hunted, or blocked. Security analysts can use this intelligence to fine-tune detections, close visibility gaps, and respond more effectively when incidents occur. The matrix becomes a blueprint for building mature, threat-informed defense capabilities.

For compliance officers, the framework supports proactive alignment with regulatory and audit expectations. By demonstrating coverage across known attacker behaviors, organizations can provide evidence that they have implemented reasonable and informed security controls. The use of MITRE ATT&CK also strengthens documentation for risk assessments, security governance, and technical safeguard validation.

This white paper introduces the full structure and significance of the MITRE ATT&CK Framework and explores each of its 14 core tactics in detail. Every section is organized from a stakeholder perspective, offering tailored insight for CISOs, security operations teams, and compliance officers. The goal is to provide each with actionable guidance they can use to improve detection, accelerate response, and harden their organization's overall cyber resilience.

The 14 tactics of the ATT&CK Enterprise Matrix: *Choose a tactic:*

Reconnaissance

Overview

Reconnaissance is where attackers gather intelligence on a target organization. This information helps them shape their attack strategies, identifying potential entry points, valuable assets, employee structures, and system vulnerabilities. Activities in this stage can include collecting email addresses, mapping public-facing infrastructure, monitoring job postings for technical information, or analyzing DNS records. While often passive and difficult to detect, reconnaissance is essential to the success of later stages and should not be underestimated.

For CISOs: Risk & Impact

Reconnaissance represents a silent threat, one that's often missed until it's too late. Attackers studying your environment are laying the groundwork for phishing campaigns, credential stuffing, or targeted exploits. While this activity may not trigger security alerts, its impact is strategic: an informed attacker is a far more dangerous one.

To mitigate the risk, CISOs must reduce the amount of sensitive data available publicly. This includes controlling what employees share online, ensuring asset inventories are complete and accurate, and implementing external threat monitoring to flag when the organization appears in attacker forums or intelligence feeds. Ultimately, the goal is to harden the organization's external posture and reduce its visibility as a viable target.

For Security Operations Teams: Detection & Response

Security Operations teams face a unique challenge with reconnaissance, it often leaves no fingerprints within internal systems. However, there are ways to detect certain forms of active reconnaissance. Suspicious DNS queries, unusual web traffic to public resources, automated scanning of IP ranges, or spikes in login attempts against web portals can all point to probing activity.

Security operation teams should also leverage threat intelligence feeds to identify when their brand or domains are being mentioned in malicious infrastructure or phishing kits. While the security operations team may not be able to respond directly to passive reconnaissance, early awareness of targeting behavior enables better readiness, such as tightening phishing rules or geofencing access to sensitive services.

For Compliance Officers: Controls & Audit Relevance

Although reconnaissance itself does not constitute a breach, it intersects with compliance when it reveals organizational exposure that should have been mitigated. Regulations like GDPR, HIPAA, and SOX require the implementation of reasonable security measures to protect sensitive data. If an attacker uses publicly available information to later access protected systems, auditors may question whether your preventative controls were sufficient.

Compliance officers should ensure that asset inventories are up to date, public-facing services are documented, and employee policies include training on limiting oversharing of technical or organizational details online. Monitoring and reducing the attack surface is not just a security concern, it's increasingly a compliance expectation.

Conclusion

Though stealthy and often external, reconnaissance is where attackers begin to shape their campaigns. Organizations that understand their public exposure, and proactively manage it, are significantly less likely to become targets. By aligning strategic oversight, technical detection, and compliance obligations, companies can reduce the success of reconnaissance and make it harder for attackers to gather the intelligence they need to proceed.

Resource Development

Overview

In the Resource Development phase, attackers establish the tools, infrastructure, and assets they need to conduct future attacks. This may involve acquiring domains for phishing, creating fake identities, developing malware, or compromising third-party systems to use as launch points. This phase is where attackers prepare the foundation for the upcoming attack. Although largely external, this stage provides critical opportunities for defenders to intercept and disrupt the adversary's plans.

For CISOs: Risk & Impact

CISOs must recognize that attackers often invest time and resources before ever launching an attack. When attackers register domains resembling your company name, create social media personas mimicking employees, or deploy malware frameworks tailored to your environment, they signal commitment and intent. Left unmonitored, this infrastructure becomes the launching pad for phishing campaigns, credential harvesting, and supply chain attacks.

Strategically, this underscores the importance of brand protection, domain monitoring, and threat intelligence. A mature security program doesn't just react to breaches; it actively monitors attacker preparations and neutralizes them early. CISOs should view this phase as an opportunity to erode attacker confidence by disrupting their readiness.

For Security Operations Teams: Detection & Response

For Security operations teams, Resource Development activities offer a window into adversary behavior before direct engagement. Monitoring certificate transparency logs, domain registrations that mimic corporate brands, or the proliferation of custom malware across threat actor toolkits can all provide insight into impending campaigns. If malware command-and-control infrastructure is discovered in the wild that references internal systems or lures, it may signal that an organization is being actively targeted.

Security analysts should collaborate with threat intel teams to identify attacker infrastructure and indicators of compromise before they're used. By analyzing attacker tooling, such as new variants of known backdoors, teams can build detections and preventive controls that will pay off during the attack execution stage.

For Compliance Officers: Controls & Audit Relevance

While Resource Development is often an external activity, its implications affect compliance domains. Regulators increasingly expect organizations to demonstrate proactive risk management, not just technical safeguards, but also environmental awareness. If attackers are allowed to spoof brands, register fake domains, or prepare phishing infrastructure using a company's identity without challenge, compliance reviewers may raise red flags.

Officers should ensure that policies include brand protection strategies, social engineering readiness, and third-party risk monitoring. Domain impersonation and phishing readiness are especially relevant for compliance frameworks like PCI DSS and GDPR, which focus on the protection of customer data and accountability for indirect breaches.

Conclusion

Resource Development is where attackers gear up for the fight. But it also offers a unique opportunity for defenders to act early, before the first email is sent or vulnerability exploited. By monitoring external infrastructure, staying ahead of attacker tooling, and tightening compliance expectations around brand and identity protection, organizations can put attackers on the defensive before an intrusion ever begins.

Initial Access

Overview

Initial Access represents the critical first step in an attacker's access into an organization's environment. At this stage, attackers attempt to gain entry through a variety of means, including phishing, exploiting public-facing applications, or leveraging stolen credentials. While the specific techniques vary, the overarching goal is the same: establish a foothold from which to move deeper into the network. Because all subsequent attacker behavior relies on gaining initial access, this phase carries strategic significance across security, operational, and compliance domains.

For CISOs: Risk and Impact

Initial Access introduces a high-risk threshold due to its potential to trigger a cascade of security failures. A single compromised user account, especially one with elevated privileges, can lead to lateral movement, data exfiltration, or widespread ransomware deployment within hours. This phase often exposes the effectiveness (or absence) of phishing defenses, security awareness training, and patch management programs.

The business implications are considerable. If attackers gain access through a social engineering campaign or an unpatched application, the organization risks not only financial damage but also reputational harm, especially if customer data is involved. Furthermore, regulatory scrutiny may increase if it is found that basic security hygiene, such as multi-factor authentication (MFA) or timely vulnerability remediation, was not enforced.

CISOs must therefore champion a proactive strategy that includes reducing the attack surface, investing in employee education to reduce social engineering success rates, and driving accountability for patch cycles. At the board level, this means articulating risk in terms of business continuity and potential regulatory fines stemming from a preventable breach.

For Security Operations Teams: Detection & Response

Security operations teams are on the front line when attackers attempt to establish initial access. Techniques such as spearphishing attachments, exploitation of internet-facing systems, or the use of previously compromised credentials are all common in this phase. Detection relies on vigilance across email, endpoint, and network activity.

Analysts must be familiar with patterns such as users launching PowerShell scripts from Office applications or web servers exhibiting unusual access patterns or error codes, which could indicate exploitation attempts. Valid account usage also requires attention, especially when a legitimate account is observed authenticating from an unfamiliar IP address, device, or region.

Response during this phase is especially time sensitive. If Initial Access is caught early, containment is often limited to isolating a single user or machine. But delays allow attackers to entrench themselves, making eradication significantly more complex. Security operations workflows should include enrichment of alerts with geolocation, behavioral context, and known tactics mapped to MITRE ATT&CK techniques to help analysts assess severity and urgency.

Threat hunting teams can also improve visibility by proactively looking for signs of Initial Access, such as Office macros executing scripts, credential use outside normal hours, or spikes in authentication failures. The faster these patterns are identified, the more likely the intrusion can be contained before escalation occurs.

For Compliance Officers: Controls & Audit Relevance

For compliance officers, the Initial Access phase is tightly bound to mandated protections around unauthorized access, credential misuse, and exposure of sensitive systems. Frameworks like HIPAA, PCI DSS, and SOX all impose requirements that overlap directly with this stage of the attack lifecycle. If attackers gain entry through preventable gaps, such as missing MFA, lack of

patching, or inadequate training, organizations may face significant regulatory penalties.

Auditors typically look for proof that safeguards are not only in place but actively monitored and maintained. This includes records of vulnerability scanning, patch management policies, email filtering configurations, and evidence of periodic security awareness training. Multi-factor authentication is a recurring control point and a common area of deficiency in audit findings, particularly for remote access and privileged accounts.

To remain compliant, organizations must demonstrate that they are continuously reducing their exposure. This means ensuring public-facing applications are regularly assessed, remote access is tightly controlled, and user behaviors are routinely reviewed for anomalies. Moreover, aligning these efforts with frameworks such as NIST CSF or ISO 27001 not only supports compliance but also creates consistency in security posture across departments.

Conclusion:

Understanding and defending against Initial Access is not only foundational to stopping attacks early but also critical to ensuring broader resilience across the organization. By viewing this tactic through the lenses of strategic oversight, technical defense, and regulatory compliance, stakeholders can align around a shared objective: to minimize the opportunities attackers have to gain a foothold in the first place. Whether by hardening external systems, refining detection workflows, or demonstrating due diligence during audits, the collective effort to disrupt Initial Access is the first and most crucial step in breaking the attacker's chain of progression.

Execution

Overview

Execution is the phase where attackers run malicious code on a target system. Techniques in this phase include scripting, command-line interfaces, user execution such as launching a malicious document, and exploitation of applications to run code. Execution can be triggered remotely or locally and is a necessary step for establishing persistence, collecting data, or carrying out lateral movement.

For CISOs: Risk and Impact

Execution often marks the point of no return. If successful, it means attackers are now actively operating inside your environment. It is a strong indicator that other stages, such as Initial Access, were not only attempted but succeeded. This raises the risk of business disruption, data loss, or full compromise.

CISOs must focus on reducing the organization's exposure to executable threats. This includes policies that restrict script execution, enforce application allow-listing, and apply software restriction policies. Investment in user awareness, endpoint protection platforms, and endpoint detection and response technologies are critical. Executable control should be monitored and reported as a core part of the security posture.

Execution is also where insider threats and social engineering succeed if controls are weak. Therefore, CISOs should ensure that technical defenses are augmented by well-tested playbooks and security training that can identify and contain incidents early in this phase.

For Security Operations Teams: Detection and Response

Security Operations teams must be highly attuned to signs of Execution. These can include PowerShell usage with obfuscated arguments, execution of binaries from unusual directories, Office documents spawning command shells, or lateral script executions.

Effective detections depend on understanding the surrounding context. Analysts should assess whether the script was signed, whether it was run at an unusual time, whether it spawned a network connection, or whether it attempted credential access. Analysts should correlate logs to identify anomalies. Behavioral analytics and baselining of normal system activity provide critical context to distinguish legitimate administrative actions from malicious ones.

Automation is essential. Security operations workflows should trigger containment actions such as isolating a host when confirmed or highly suspicious execution behaviors are detected. Playbooks should guide analysts on triage steps including collecting volatile memory, identifying parent-child process relationships, and escalating based on mapped MITRE ATT&CK techniques.

For Compliance Officers: Controls and Audit Relevance

Execution ties directly into compliance via controls over authorized software, employee training, and malware prevention. Regulations such as PCI DSS, HIPAA, and NIST 800-53 require mechanisms to prevent unauthorized code execution and detect malware.

Compliance officers must ensure the organization enforces strong configuration management. This includes maintaining approved software inventories, enforcing execution policies via Group Policy or third-party tools, and providing ongoing evidence of endpoint security measures.

Audit readiness involves not only showing that anti-malware tools are deployed but also proving they are functioning, updated, and monitored. Logging and alerting on events must be demonstrable. For regulated environments, failure to detect or prevent malware execution is frequently considered negligence.

Conclusion

Execution is the turning point where attackers move from preparation to active interference. Organizations that monitor this phase closely can detect and respond to attacks before significant harm occurs. By integrating control, detection, and compliance oversight, stakeholders can limit the ability of malicious code to run and ensure that all attempts are rapidly detected and contained.

Persistence

Overview

Persistence refers to the techniques attackers use to maintain their foothold within a compromised environment. Once they gain access, attackers do not want to lose it after a reboot or credential change. They may create new user accounts, implant malware that reactivates on startup, or abuse legitimate services to maintain access over time. This tactic ensures that even if the initial compromise is detected, the attacker retains a way to re-enter the environment.

For CISOs: Risk and Impact

Persistence turns a single intrusion into a long-term threat. Attackers who successfully maintain access can return repeatedly, even after containment measures are applied. This stage introduces serious business risks by enabling prolonged data exposure, repeated disruptions, and deeper penetration into sensitive systems.

CISOs must ensure that identity governance, endpoint controls, and logging are configured to identify unauthorized account creation, service modifications, and registry tampering. Leadership should recognize that effective response to persistence attempts requires both continuous monitoring and fast, decisive containment.

Routine review of accounts, AutoStart mechanisms, and remote access paths should be standard operating procedure. Without

visibility into persistent access techniques, organizations are at risk of sustained compromise with minimal warning signs.

For Security Operations Teams: Detection and Response

Persistence techniques often mimic legitimate behavior, which makes detection difficult. Security operations teams must look for unusual use of trusted binaries, unauthorized registry changes, and system modifications that survive reboot. Indicators of persistence include:

- Abnormal scheduled task creation
- Use of startup folders by unauthorized accounts
- WMI event subscriptions with suspicious triggers
- Newly created or duplicated local administrator accounts

Detection efforts should focus on identifying changes to AutoStart locations, malware patterns, and scripting. Endpoint protection tools and baseline deviation alerts are essential for spotting the subtle changes attackers depend on.

Security operations teams should also conduct regular sweeps of system logs, registry entries, and services to uncover dormant persistence mechanisms. Incident playbooks should include validation steps after containment to ensure that the attacker cannot reestablish access through previously deployed tools.

For Compliance Officers: Controls and Audit Relevance

Persistence challenges an organization's ability to detect and remove malicious presence. Many regulatory frameworks, including HIPAA, PCI DSS, and NIST SP 800-53, require that organizations demonstrate their ability to contain and eliminate threats effectively.

Compliance officers must confirm that endpoint protection platforms are active and up to date, and that change control mechanisms monitor and alert on unauthorized configuration changes. Policies should support the removal of inactive accounts, enforcement of least privilege, and documentation of periodic reviews for startup entries and administrative privileges.

Auditors often expect proof of detection tools capable of identifying persistence behaviors. Compliance is supported by demonstrating that preventive controls are actively monitored and that systems are routinely checked for hidden or unauthorized changes.

Conclusion

Persistence allows attackers to maintain access long after the initial breach. If left undetected, these techniques give adversaries time to escalate privileges, steal data, or launch additional attacks. Organizations that continuously verify system integrity, monitor changes, and follow structured protocols will be in a stronger position to eliminate long-term threats.

Privilege Escalation

Overview

Privilege Escalation refers to techniques used by attackers to gain higher levels of access within a compromised environment. This often involves moving from a standard user account to one with administrative or system-level privileges. Escalated access allows attackers to disable defenses, move laterally, exfiltrate data, or establish persistence with greater control.

For CISOs: Risk and Impact

Privilege Escalation marks a major shift in attacker capability. With elevated access, attackers can take control of sensitive assets, modify security settings, or erase traces of activity. It often signals that initial security failures have led to a broader compromise.

CISOs must ensure privilege escalation paths are minimized through access controls, patching, and privilege audits. Role-based access, just-in-time permissions, and multi-factor authentication for privileged accounts are essential safeguards. This tactic exposes critical gaps in identity and access management programs that should be continuously assessed and improved.

The business risk increases when attackers can access confidential systems, modify key configurations, or impersonate high-privilege users. Privilege Escalation can be the doorway to data loss, operational disruption, and reputational damage.

For Security Operations Teams: Detection and Response

Security Operations teams must detect indicators of privilege escalation such as:

- Use of built-in tools like PsExec or RunAs
- Modifications to group memberships or access control lists
- Abnormal use of service accounts
- Execution of processes under system-level permissions

Detection requires correlation of authentication logs, event logs, and endpoint telemetry. Analysts should track access token use, logon patterns, and command execution that deviates from expected behavior. Suspicious privilege increases should be escalated immediately.

Security Operations teams must also simulate known privilege escalation techniques in their environment to validate alerting mechanisms. Automated responses such as account disablement or session termination can stop attacks in progress. Threat hunting should focus on finding dormant or misconfigured accounts that may allow privilege abuse.

For Compliance Officers: Controls and Audit Relevance

Privilege Escalation maps directly to core access control and monitoring requirements in regulatory frameworks such as PCI DSS, HIPAA, SOX, and ISO 27001. Auditors want to see clear enforcement of least privilege, role separation, and real-time detection of unauthorized access changes.

Compliance officers should verify that all privileged access is approved, documented, and reviewed regularly. Logs of group membership changes, elevation events, and administrative account usage must be retained and reviewed. Tools that track and alert of privilege changes strengthen audit readiness.

Policy documentation should reflect procedures for granting, revoking, and validating privileged access. Evidence that privileged accounts are monitored and periodically reauthorized supports both compliance goals and overall security posture.

Conclusion

Privilege Escalation enables attackers to expand control, bypass defenses, and increase the severity of an incident. Preventing and detecting this tactic requires tightly controlled permissions, continuous monitoring, and collaboration between technical and governance teams. By closing gaps in privilege management, organizations reduce the likelihood and impact of high-level compromises.

Defense Evasion

Overview

Defense Evasion refers to the methods attackers use to avoid detection by security tools and processes. These techniques are designed to bypass antivirus software, endpoint detection systems, firewalls, and monitoring solutions. Common methods include code obfuscation, disabling security tools, clearing logs, and abusing trusted processes. This tactic is essential for maintaining stealth while conducting other stages of an attack.

For CISOs: Risk and Impact

Defense Evasion undermines the ability of security teams to identify and respond to attacks. It exposes weaknesses in tool coverage, configuration, and operational discipline. When attackers can hide their presence, they gain time to escalate privileges, spread laterally, or exfiltrate data without being noticed.

CISOs must drive investments in layered defense strategies. This includes defense-in-depth architecture, advanced endpoint protection, application control, and security analytics. Logging integrity, automated validation of sensor coverage, and regular control testing help reduce the risk of detection failures.

Defense Evasion also highlights the importance of secure configuration management. Tools must be hardened against tampering, and access to logs, monitoring agents, or security consoles must be tightly controlled. Business leaders should be made aware that a lack of detection is not proof of safety, and that evasion techniques often succeed by exploiting complacency.

For Security Operations Teams: Detection and Response

Security operations teams face significant challenges in detecting Defense Evasion. Indicators include:

- Security tools being disabled or uninstalled
- Log deletion or manipulation
- Unexpected changes to Group Policy or registry settings
- Use of signed but malicious binaries
- Processes running with hollowed memory or injected code

Security analysts must rely on behavioral detection, baseline deviations, and integrity checks to identify evasion attempts. Alerting on the failure of logging services, missing heartbeat signals from sensors, or unsigned driver loads can uncover stealth activity.

Response playbooks should include validation steps for the health and coverage of detection systems during incident triage. Analysts should investigate gaps in visibility and track which security controls were active at the time of the suspected evasion. Threat hunting should focus on uncovering unlogged activity, stealthy persistence mechanisms, and tampering with security configurations.

For Compliance Officers: Controls and Audit Relevance

Defense Evasion techniques directly threaten audit readiness by making detection and logging unreliable. Compliance frameworks such as NIST 800-53, ISO 27001, and PCI DSS require assurance that monitoring controls are in place, effective, and protected from manipulation.

Compliance officers should verify that log retention policies are enforced, logging mechanisms are monitored for integrity, and

that security controls are tested for resilience against tampering. Documented procedures for validating sensor health, system audit configurations, and access to forensic artifacts are essential to demonstrate readiness.

Auditors may request evidence that attempts to disable logging or evade detection are captured and responded to. Demonstrating visibility into system tampering and unauthorized configuration changes strengthens compliance posture and supports the organization's overall accountability model.

Conclusion

Defense Evasion enables attackers to operate undetected, often for extended periods. It allows them to escalate attacks without triggering alerts. By enforcing strong monitoring coverage, securing control infrastructure, and continuously validating the health of detection systems, organizations can reduce the effectiveness of evasion techniques and shorten the dwell time of active threats.

Credential Access

Overview

Credential Access refers to techniques used by attackers to steal usernames, passwords, authentication tokens, and other credentials from compromised systems. This enables unauthorized access to additional systems, services, and data. Common methods include keylogging, credential dumping, brute force, phishing, and accessing insecure credential storage locations such as LSASS or browser caches.

For CISOs: Risk and Impact

Credential Access is a gateway to widespread compromise. Once credentials are stolen, attackers can impersonate legitimate users, bypass authentication, and expand access to critical systems and cloud services. The risk compounds when privileged credentials are compromised, potentially allowing attackers to control entire environments.

CISOs must prioritize the protection of credential stores and reduce the exposure of high-value accounts. This includes deploying credential vaulting, enforcing strong password policies, implementing multifactor authentication, and limiting where credentials are stored in memory. Regular credential hygiene reviews and disabling unused accounts also reduce the attacker's opportunities.

Security programs should include simulation and red-teaming exercises to test credential protection controls. The business impact of stolen credentials can include data loss, regulatory violations, and prolonged dwell time due to the attacker's ability to move invisibly.

For Security Operations Teams: Detection and Response

Security operations teams must monitor for indicators of credential theft. These include:

- Access to LSASS memory
- Dumping of SAM or SECURITY registry hives
- Suspicious use of Mimikatz or similar tools
- Unusual logon attempts from new systems or locations
- Scripts that access credential stores or authentication tokens

Detection strategies should include endpoint monitoring, system audit policy enforcement, and logging of PowerShell and command-line usage. Analysts must correlate these with behavior-based indicators and look for abnormal access patterns that do not match user baselines.

Response actions should include isolating affected systems, rotating exposed credentials, and increasing logging and alerting thresholds for compromised accounts. Security operations teams should use threat intelligence to track toolsets commonly used for credential access and build detection rules accordingly.

For Compliance Officers: Controls and Audit Relevance

Credential theft has direct compliance implications, especially in environments governed by frameworks like HIPAA, SOX, PCI DSS, and NIST 800-53. These frameworks require controls around authentication, account management, and access monitoring.

Compliance officers should confirm that privileged account access is tightly controlled, monitored, and logged. Policies should mandate the use of multifactor authentication and prevent reuse of credentials across systems. Password policies, audit trails of authentication activity, and evidence of access reviews are essential components of audit readiness.

Regular penetration testing and credential audits should be documented and included in risk assessment materials. Evidence of automated detection and response to credential misuse helps demonstrate regulatory alignment and security maturity.

Conclusion

Credential Access enables attackers to impersonate legitimate users, making their actions harder to detect and stop. Organizations must adopt a layered defense strategy that limits access to credential stores, enforces strong authentication, and rapidly responds to signs of misuse. By treating credentials as high-value assets and monitoring them continuously, companies can reduce the likelihood and impact of this tactic.

Discovery

Overview

Discovery refers to the techniques attackers use to gather information about the internal environment after gaining initial access. This includes identifying domain controllers, network topology, user accounts, shared resources, security configurations, and active services. The purpose of this stage is to map the environment and identify targets for privilege escalation, lateral movement, or data collection.

For CISOs: Risk and Impact

Discovery allows attackers to turn a single compromised machine into a launchpad for deeper infiltration. Once an attacker understands the layout and structure of the environment, they can prioritize high-value systems, locate unprotected assets, and identify weak points in segmentation and privilege boundaries.

CISOs should ensure that discovery activity is monitored and limited through segmentation, least privilege access, and service isolation. Exposure of administrative shares, open directory services, and unfiltered system responses can greatly increase the speed and success of attacks. Investments in internal threat detection, anomaly detection, and strong access control policies are necessary to reduce this risk.

Discovery activity also reflects whether an organization is performing routine visibility audits. A mature security posture

includes continuous internal monitoring, data classification, and the ability to detect abnormal asset enumeration or account lookups.

For Security Operations Teams: Detection and Response

Security operations teams must be prepared to identify a wide range of discovery behaviors, including:

- Network scanning and port enumeration
- Active Directory enumeration using built-in commands or tools like BloodHound
- Net commands to list users, groups, and shares
- Querying system information or local security configurations
- NS lookups and reverse name resolution

Detection requires endpoint visibility, log collection from authentication systems, and monitoring of command-line and scripting activity. Analysts should baseline typical discovery behavior for IT operations and flag deviations that appear automated, out of hours, or sourced from suspicious accounts.

Security operations workflows should include correlation between system activity and user identity. Response playbooks must guide the containment of accounts and systems showing signs of internal reconnaissance. Threat hunting efforts should look for signs of silent scans, repeated name queries, and command output redirection.

For Compliance Officers: Controls and Audit Relevance

Discovery activity intersects with compliance requirements related to access controls, monitoring, and risk management. Frameworks such as NIST 800-53, ISO 27001, and CIS Controls require organizations to restrict unnecessary system information exposure and detect unauthorized queries.

Compliance officers should validate that systems do not expose excessive data to unauthenticated users, and that internal scanning activity is both logged and reviewed. Internal segmentation, access to administrative tools, and shared resource permissions should be regularly audited.

Logs from directory services, DNS, and network infrastructure are often requested during audits to demonstrate that monitoring is in place. Documentation of technical safeguards, alert thresholds, and network visibility controls can support compliance goals and demonstrate proactive risk management.

Conclusion

Discovery allows attackers to understand the landscape and plan their next move. Without proper visibility and access controls, even basic enumeration techniques can lead to privilege escalation and data access. Organizations that detect reconnaissance early, limit information exposure, and log internal queries position themselves to contain attacks before critical systems are compromised.

Lateral Movement

Overview

Lateral Movement involves techniques that attackers use to move through an environment after gaining initial access. The

goal is to reach additional systems, escalate privileges, and gain access to sensitive data or critical infrastructure. This stage often involves the use of stolen credentials, remote service protocols, remote desktop access, or administrative tools such as PsExec and Windows Management Instrumentation (WMI).

For CISOs: Risk and Impact

Lateral Movement allows attackers to expand their reach, compromise more systems, and deepen their control. A single compromised workstation can lead to domain-wide access if appropriate safeguards are not in place. The business risk increases substantially when lateral movement reaches systems containing customer data, financial records, or operational controls.

CISOs must implement strong segmentation policies, restrict administrative access, and monitor abnormal account behavior. Limiting lateral movement pathways reduces the attack surface and increases the chances of detection. Investments in user behavior analytics, just-in-time access control, and tiered network architecture help contain the spread of an intrusion.

Security awareness at the executive level is also important. Organizations must treat lateral movement as a sign that an attacker is actively exploiting the environment and that immediate containment actions are needed.

For Security Operations Teams: Detection and Response

Security operations teams must monitor for:

- Use of administrative tools across hosts
- Authentication attempts using compromised accounts
- Creation of remote services
- Unusual network traffic patterns between endpoints
- Logon sessions on systems unrelated to a user's normal behavior

Endpoint and network telemetry are essential. Analysts should track authentication events, session creation, and system access patterns. Lateral Movement often blends in with IT operations, so baselining and alert tuning are critical.

Detection rules should correlate account activity with system roles. For example, a marketing user authenticating to a domain controller may indicate malicious use of stolen credentials. Playbooks must include actions to isolate endpoints, revoke session tokens, and review system access logs.

Hunting teams should search for signs of credential abuse, script-based automation, and process execution chains that span multiple machines. Remote desktop usage, administrative share access, and execution of binaries from remote sources should be flagged for investigation.

For Compliance Officers: Controls and Audit Relevance

Lateral Movement impacts access control, logging, and segmentation requirements across nearly all regulatory frameworks. Standards such as NIST 800-53, PCI DSS, and ISO 27001 mandate monitoring of internal traffic, use of administrative accounts, and restrictions on unauthorized access between systems.

Compliance officers should confirm that policies address internal segmentation, use of privileged accounts, and system access audits. They must ensure that logs of remote access, user sessions, and inter-system communication are retained and reviewed regularly.

Documentation should demonstrate that lateral movement paths are limited through architectural controls and that security

teams are capable of detecting and responding to suspicious internal access. Controls that prevent excessive privilege accumulation and lateral authentication should be highlighted during audits.

Conclusion

Lateral Movement allows attackers to pivot from one system to another, increasing their access and impact. Organizations that implement strict access controls, monitor inter-system behavior, and respond quickly to abnormal authentication patterns will be better positioned to detect and contain attacks before they escalate.

Collection

Overview

Collection refers to the techniques used by attackers to gather and centralize data of interest within the environment. This includes harvesting sensitive documents, credentials, email archives, intellectual property, financial data, or configuration files. Collected data is often staged in preparation for exfiltration or used to facilitate further attacks.

For CISOs: Risk and Impact

Collection is a clear indicator that the attacker has achieved a stable presence and is pursuing tangible objectives. The exposure of sensitive or regulated data can lead to financial loss, regulatory violations, and long-term brand damage.

CISOs should prioritize identifying where sensitive data resides, limiting access to that data, and enforcing strict auditing. Data loss prevention (DLP), classification tools, and encryption should be deployed across endpoints, file shares, and cloud repositories. Business leaders must understand that failure to monitor and control data movement internally is a direct path to breach escalation.

This stage also reflects the effectiveness of internal segmentation and visibility. If attackers can gather data without being detected, then logging, access controls, and behavioral baselines are likely insufficient.

For Security Operations Teams: Detection and Response

Security operations teams must monitor for signs of data aggregation. Indicators include:

- Unusual file access across multiple systems
- Scripts that compress or archive large numbers of documents
- Collection of browser or system credentials
- Use of file synchronization tools not authorized in the environment
- Unauthorized access to email inboxes or shared drives

Detection should include monitoring for file access anomalies, large-scale read operations, and use of data staging directories. Analysts must investigate spikes in access volume, especially if initiated by service accounts or machines that do not typically access sensitive data.

Response procedures must include containment of the collection process, isolation of accounts or systems used for aggregation, and forensic imaging of involved devices. Coordination with data owners and privacy teams is essential when regulated data is involved.

Threat hunting can identify dormant scripts, malicious batch files, or unexpected file structures that may indicate data staging. Security operations teams should also scan for bulk access to endpoints that typically hold business-critical files.

For Compliance Officers: Controls and Audit Relevance

Collection tactics put data governance controls to the test. Regulatory frameworks such as GDPR, HIPAA, and CCPA require strong oversight of how personal and sensitive data is accessed, stored, and protected.

Compliance officers must verify that access to regulated data is logged, reviewed, and limited to authorized users. Data classification and protection policies should be clearly defined, implemented, and supported by automation where possible.

Evidence of file access monitoring, endpoint DLP, encryption enforcement, and access review processes must be documented. Audit trails should show how organizations identify and respond to large-scale access attempts or staging behavior.

Conclusion

Collection is the stage where attackers begin to extract value from a compromised environment. Without controls over internal data access, organizations leave themselves vulnerable to loss before data even leaves the network. Strong visibility, access management, and behavior monitoring are essential to detect and contain this phase of an attack.

Command and Control

Overview

Command and Control (C2) refers to the methods attackers use to communicate with compromised systems inside the target environment. These communications enable them to issue instructions, transfer data, update malware, and maintain access. Techniques vary widely and include use of legitimate services, encrypted channels, custom protocols, and commonly used ports to blend in with regular traffic.

For CISOs: Risk and Impact

Command and Control marks the point at which attackers shift from local compromise to remote operations. It allows them to maintain control, download additional payloads, and orchestrate complex activities from outside the environment.

CISOs must ensure outbound traffic is tightly monitored and restricted. Proxy filtering, DNS monitoring, firewall policies, and anomaly detection are essential defenses. Cloud-based C2 and use of trusted applications for command channels increase the difficulty of detection.

This phase highlights the need for rigorous egress controls and threat intelligence integration. Business leaders should understand that attackers can exfiltrate data, deploy ransomware, or trigger destructive actions through persistent C2 access.

For Security Operations Teams: Detection and Response

Security operations teams must look for C2 activity indicators such as:

- Outbound traffic to known malicious IP addresses or domains
- Use of uncommon protocols or ports for external communication
- Encrypted traffic to non-standard destinations

- Repeated failed DNS queries or beaconing behavior
- Connections to dynamic DNS services or anonymizing networks

Detection relies on deep packet inspection, DNS analysis, and correlation with threat intelligence feeds. Endpoint telemetry can also reveal unusual parent-child process behavior tied to C2 connections.

Response playbooks must include steps to isolate the communicating host, capture network traffic, and identify other endpoints using the same C2 infrastructure. Blocking the C2 channel must be coordinated with containment efforts to prevent fallback attempts.

Threat hunting should focus on persistence mechanisms tied to C2, script-based communication patterns, and unusual scheduling of network activity. Use of standard utilities like PowerShell or certutil for communication is increasingly common and must be monitored.

For Compliance Officers: Controls and Audit Relevance

C2 activity poses a serious challenge to maintaining audit readiness. Regulatory frameworks such as NIST 800-53, PCI DSS, and ISO 27001 require controls for detecting and responding to external command activity.

Compliance officers should confirm that egress filtering is documented, DNS logs are retained, and use of encryption is reviewed for legitimacy. Any detection of C2 activity must result in incident documentation and follow-up corrective actions.

Policy reviews should include verification that unauthorized outbound communications are blocked or flagged, and that intrusion detection systems are configured to detect known C2 patterns. Demonstrating awareness and response to remote control attempts supports regulatory expectations.

Conclusion

Command and Control gives attackers the ability to coordinate their operations and extract value over time. Without strong network monitoring and endpoint visibility, this activity can persist undetected. By implementing layered egress controls and investigating suspicious outbound traffic, organizations can detect and disrupt remote attacker control before it escalates.

Exfiltration

Overview

Exfiltration is the process by which attackers steal data from a compromised environment and transfer it to a system under their control. The goal is to extract sensitive or valuable information without detection. Attackers may use various methods including encrypted channels, cloud storage services, DNS tunneling, or common web protocols to mask their activity.

For CISOs: Risk and Impact

Exfiltration represents the realization of business risk. It converts a security incident into a data breach, triggering financial loss, legal exposure, and reputational harm. The damage increases significantly if the stolen data includes regulated information, intellectual property, or customer records.

CISOs must lead efforts to identify where sensitive data resides, who can access it, and how it is monitored. Data Loss Prevention (DLP), behavioral analytics, and tight egress controls form the foundation of an effective defense strategy. Encryption of data at rest and in transit helps reduce the impact of potential breaches.

Executive stakeholders must understand that exfiltration is not limited to obvious channels. USB drives, misused cloud accounts, and legitimate tools like Rclone or curl can be exploited by attackers. Prevention relies on both technical controls and user awareness.

For Security Operations Teams: Detection and Response

Security operations teams must monitor for indicators of exfiltration, including:

- Sudden spikes in outbound traffic volume
- Use of file transfer protocols during off hours
- Data being sent to unusual external domains or IPs
- Encrypted traffic leaving the network without a known business purpose
- Use of compression or encryption utilities immediately before transmission

Effective detection requires combining network monitoring, endpoint logging, and DLP telemetry. Analysts should investigate large file transfers, changes in traffic patterns, or repeated communication with cloud storage services from unexpected systems.

Response actions include isolating the involved endpoints, reviewing what data was accessed, and blocking the destination used for exfiltration. Security operations teams should work closely with data owners and legal teams to determine regulatory obligations following confirmed data theft.

Threat hunting should proactively examine past logs for missed signs of staged data, bulk access events, or unauthorized use of tools that enable transfer. Endpoint queries can detect artifacts such as compressed archives, script remnants, or alternate data streams.

For Compliance Officers: Controls and Audit Relevance

Exfiltration events are often subject to strict reporting requirements under laws such as GDPR, HIPAA, CCPA, and state-level data breach notification laws. Failure to detect and respond to exfiltration can result in substantial penalties.

Compliance officers must ensure that access to sensitive data is limited, logged, and reviewed. Controls should include outbound traffic monitoring, alerting on unauthorized transfers, and documented incident response procedures that address data theft.

Audit readiness depends on maintaining a defensible position regarding data movement controls. This includes demonstrating encryption enforcement, role-based access to files, alert logs for anomalous transfers, and documented responses to previous exfiltration attempts.

Conclusion

Exfiltration transforms an internal compromise into an external crisis. Preventing data theft requires visibility into where sensitive data resides, who accesses it, and how it leaves the network. Organizations that monitor outbound activity, enforce access controls, and act quickly on suspicious behavior will be better positioned to reduce the impact of data breaches.

Impact

Overview

Impact refers to the techniques attackers use to disrupt, damage, or manipulate systems and data after achieving their goals. This phase includes destroying data, encrypting files for ransom, disabling services, defacing assets, or sabotaging business operations. While some attacks are designed to steal data quietly, others aim to leave visible damage to force payments, send messages, or maximize disruption.

For CISOs: Risk and Impact

This stage marks the attacker's final objective. Impact can lead to widespread outages, lost revenue, loss of customer trust, and long-term operational consequences. It often affects business continuity and may result in regulatory investigations or public disclosure.

CISOs must ensure that recovery and containment plans are in place before an attack occurs. This includes implementing backup and restoration procedures, system hardening, offline data retention, and tested incident response plans. The ability to respond to ransomware, wiper malware, or destructive scripts depends on preparation.

Leaders should recognize that attackers may intentionally trigger damage even after being detected. Planning for worst-case outcomes is essential to ensure the organization can maintain operations and preserve its reputation.

For Security Operations Teams: Detection and Response

Security operations teams must prepare for scenarios where the attack becomes overt. Indicators include:

- Mass file encryption or deletion
- Disabling of services or scheduled tasks
- Unauthorized system reboots or shutdowns
- Overwrites of backup directories
- Alerts from anti-malware systems detecting wipers or ransomware

Detection requires file integrity monitoring, system health tracking, and correlation of endpoint alerts with behavioral signals. Analysts should be ready to initiate containment protocols and activate recovery procedures without delay.

Response steps include isolating affected systems, recovering from backups, coordinating with IT and disaster recovery teams, and preparing communications for leadership and external stakeholders. Security operations playbooks should outline how to triage critical systems first, preserve evidence for legal review, and prevent re-triggering of impact scripts.

Threat hunting can identify precursors to impact activity, such as staged destructive tools or test scripts on non-critical systems. Proactive detection of ransomware artifacts or persistence mechanisms improves readiness.

For Compliance Officers: Controls and Audit Relevance

Impact tactics present challenges for compliance teams because they may result in data loss, service unavailability, or compromised integrity of audit logs. Regulatory frameworks require resilience planning, incident handling policies, and proof of data recovery capabilities.

Compliance officers should verify that data is regularly backed up, that systems are covered by continuity planning, and that

controls exist to ensure timely response to disruptive events. Documentation of recovery testing and breach handling processes supports audit expectations.

Auditors may seek evidence that business-critical systems can be restored within required timeframes and that organizations have formalized impact assessment and communication strategies.

Conclusion

Impact is where the consequences of an attack become unavoidable. Whether through data destruction, encryption, or service disruption, this tactic tests an organization's preparedness. By planning, investing in recovery, and ensuring rapid detection and containment, organizations can limit the damage and maintain control in the face of destructive threats.

Definitions

1. Initial Access

Initial access techniques represent the methods attackers use to enter a target network. This could involve exploiting public-facing applications, phishing campaigns, or trusted relationships.

Key Techniques:

- Phishing (T1566)
- Exploit Public-Facing Application (T1190)
- Drive-by Compromise (T1189)

Defensive Measures:

- Employee phishing simulations and training
- Regular patching of internet-exposed systems
- Threat detection and network segmentation

---

2. Execution

Execution tactics involve running malicious code on a local or remote system. These actions allow attackers to execute programs or commands to achieve their objectives.

Key Techniques:

- PowerShell (T1059.001)
- Command and Scripting Interpreter (T1059)
- Scheduled Task/Job (T1053)

Defensive Measures:

- Script blocking policies
- Endpoint Detection and Response (EDR) monitoring
- AppLocker configuration

---

3. Persistence

Persistence techniques ensure an adversary can maintain access to systems even after restarts or credential changes. These footholds help in maintaining long-term control.

Key Techniques:

- Account Manipulation (T1098)
- Boot or Logon Autostart Execution (T1547)
- Create or Modify System Process (T1543)

Defensive Measures:

- Regular audits of user accounts and groups
- Monitoring autorun registry keys and services
- Logging scheduled tasks and startup items

---

4. Privilege Escalation

Once inside, attackers seek elevated privileges to access sensitive data and systems.

Key Techniques:

- Exploitation for Privilege Escalation (T1068)
- Valid Accounts (T1078)
- Bypass User Access Control (T1548.002)

Defensive Measures:

- Least privilege enforcement
- OS hardening and patch management
- Behavior analytics for anomalous privilege changes

5. Defense Evasion

These techniques are used to avoid detection throughout the attack lifecycle. Defense evasion is key to maintaining stealth and prolonging access.

Key Techniques:

- Obfuscated Files or Information (T1027)
- Impair Defenses (T1562)
- File and Directory Permissions Modification (T1222)

Defensive Measures:

- File integrity monitoring
- Antivirus and EDR with behavioral detection
- Audit policy enforcement

6. Credential Access

Credential access techniques aim to obtain credentials for account takeover and lateral movement.

Key Techniques:

- OS Credential Dumping (T1003)
- Brute Force (T1110)
- Credential Stuffing (T1110.004)

Defensive Measures:

- Multi-factor authentication (MFA)
- Account lockout policies
- Credential vaulting and lifecycle management

7. Discovery

Attackers explore the target environment to identify critical assets, services, and relationships.

Key Techniques:

- System Information Discovery (T1082)
- Network Service Scanning (T1046)
- Permission Groups Discovery (T1069)

Defensive Measures:

- Network segmentation
- Honeytokens and deceptive assets
- Alerting on abnormal network mapping behavior

8. Lateral Movement

Lateral movement allows attackers to navigate across systems within a network to locate high-value targets.

Key Techniques:

- Remote Services (T1021)
- Pass the Hash (T1550.002)
- Remote Desktop Protocol (RDP) Abuse (T1021.001)

Defensive Measures:

- RDP hardening
- SMB and WMI monitoring
- Lateral movement detection tools

9. Collection

These techniques involve gathering data relevant to the attacker's goals, often including documents, credentials, or screenshots.

Key Techniques:

- Screen Capture (T1113)
- Input Capture (T1056)
- Data from Local System (T1005)

Defensive Measures:

- DLP (Data Loss Prevention) tools
- Access controls on sensitive files
- Application logging and endpoint auditing

10. Command and Control (C2)

Command and control tactics enable attackers to communicate with compromised systems to issue commands and receive data.

Key Techniques:

- Application Layer Protocol (T1071)
- Encrypted Channel (T1573)
- Domain Fronting (T1090.004)

Defensive Measures:

- Network anomaly detection
- DNS monitoring and egress controls
- HTTPS decryption and inspection

11. Exfiltration

This tactic involves the extraction of data from the target network. Attackers may use compression and obfuscation to evade detection.

Key Techniques:

- Exfiltration Over Web Service (T1567.002)
- Scheduled Transfer (T1029)
- Archive Collected Data (T1560)

Defensive Measures:

- DLP policies
- Bandwidth usage monitoring
- External file transfer alerts

12. Impact

Impact techniques target system availability, integrity, or confidentiality, often to disrupt operations or coerce victims.

Key Techniques:

- Data Destruction (T1485)
- Disk Wipe (T1561)
- Defacement (T1491)

Defensive Measures:

- Regular backups and disaster recovery
- Immutable storage policies
- Monitoring for destructive commands

13. Reconnaissance

Pre-compromise techniques involving the identification of targets and vulnerabilities using open-source intelligence (OSINT).

Key Techniques:

- Search Open Websites/Domains (T1593)
- Gather Victim Identity Information (T1589)
- Phishing for Information (T1598)

Defensive Measures:

- Employee awareness training
- OSINT exposure assessments
- External threat intelligence integration

14. Resource Development

Attackers may develop or obtain resources like infrastructure, malware, and accounts before launching an attack.

Key Techniques:

- Acquire Infrastructure (T1583)
- Compromise Accounts (T1586)
- Establish Accounts (T1585)

Defensive Measures:

- Monitoring domain registrations and certificates
- Tracking suspicious infrastructure
- Blocking known malicious services

Conclusion

The MITRE ATT&CK Framework provides a structured approach to understanding adversarial behavior. By aligning security controls, detection strategies, and incident response with the ATT&CK matrix, organizations can enhance their security posture and proactively counter threats. Enterprises must adopt a layered defense, continuously improve visibility, and map detections to ATT&CK to stay ahead of today's sophisticated threat actors.

Appendix: MITRE ATT&CK Reference Links

- **attack.mitre.org**
- **mitre.org**

About Cygna Labs

Cygna Labs is a software developer and one of the top three global DDI vendors. Many Fortune 100 customers rely on Cygna Labs' DDI products and services, in addition to its industry-leading security and compliance solutions to detect and proactively mitigate data security threats, affordably pass compliance audits, and increase the productivity of their IT departments.

Cygna Labs Corp

sales@cygnalabs.com
Toll Free: 844.442.9462
Intl: +1 (305) 501-2430
www.cygnalabs.com

© 2025 Cygna Labs Corp. All Rights Reserved.