THREAT CARD T-01

PHISHING CAMPAIGN

STEP: INITIAL COMPROMISE
VECTOR: SOCIAL ENGINEERING

CLUE FOR THREAT ORCHESTRATOR

"Your security team reports that several employees have received emails claiming to be from your IT department requesting password resets. One user has already clicked the link. Email headers show the domain is spoofed."

WHY THIS WORKS

Phishing exploits human psychology rather than technical vulnerabilities. Attackers use social engineering to create urgency and bypass technical controls. With email authentication (DMARC/SPF) and user training, this attack is highly preventable.

THREAT CARD T-02

WATERING HOLE ATTACK

STEP: INITIAL COMPROMISE
VECTOR: WEB EXPLOIT

CLUE FOR THREAT ORCHESTRATOR

"A popular industry blog your employees frequently visit has been compromised. Logs show that your users' browsers were redirected to a malicious domain hosting an exploit kit targeting unpatched browsers."

WHY THIS WORKS

Watering hole attacks target trusted third-party sites to infect specific user groups. They bypass email filters and exploit browser vulnerabilities. Defense requires rapid patching and endpoint monitoring.

THREAT CARD T-03

COMPROMISED CREDENTIALS

STEP: INITIAL COMPROMISE
VECTOR: CREDENTIAL ABUSE

CLUE FOR THREAT ORCHESTRATOR

"Your SIEM has detected a successful VPN login from an unusual geographic location at 3 AM. The username belongs to an employee who is currently on vacation. The login attempt came from an IP in a known cybercrime hosting provider."

WHY THIS WORKS

Credential stuffing uses passwords leaked from third-party breaches. If employees reuse passwords, their work accounts become compromised. Multi-factor authentication (MFA) is the primary defense.

THREAT CARD T-04

LATERAL MOVEMENT VIA SMB

STEP: PIVOT & ESCALATE
VECTOR: NETWORK

CLUE FOR THREAT ORCHESTRATOR

"Network segmentation alerts show unusual SMB traffic between a compromised workstation and your file server. Suspicious named pipe activity detected. The attacker appears to be enumerating shares and attempting to access restricted resources."

WHY THIS WORKS

SMB (Server Message Block) is a legitimate protocol, so traffic blends in. Flat network architecture allows attackers to move freely. Without micro-segmentation and strong authentication, lateral movement is easy.

THREAT CARD T-05

PRIVILEGE ESCALATION VIA KERNEL EXPLOIT

STEP: PIVOT & ESCALATE
VECTOR: MALWARE

CLUE FOR THREAT ORCHESTRATOR

"EDR telemetry shows a low-privilege process loading a proof-of-concept exploit for an unpatched local privilege escalation vulnerability in the Windows kernel. Seconds later, the same process spawned a child running as SYSTEM. Patch reports show this host is three months behind on kernel updates."

WHY THIS WORKS

Kernel exploits abuse memory- corruption or logic flaws (think Dirty Pipe or win32k CVEs) to jump from a standard user to SYSTEM or root. Public PoC code often appears within days of disclosure, so unpatched hosts are easy targets. Rapid patching, EDR behavioral detection, and least privilege limit the damage.

THREAT CARD T-06

MIMIKATZ CREDENTIAL DUMPING

STEP: PIVOT & ESCALATE
VECTOR: CREDENTIAL ABUSE

CLUE FOR THREAT ORCHESTRATOR

"Memory forensics analysis on the Domain Controller reveals suspicious LSASS process manipulation. A tool has dumped credential hashes from memory. Several cached domain admin credentials have been extracted. Attacker now has credentials to move to critical systems."

WHY THIS WORKS

Mimikatz attacks Windows LSASS (Local Security Authority Subsystem) memory to extract credentials. Without proper Credential Guard and memory protection, domain admin credentials become compromised, enabling full infrastructure access.

THREAT CARD T-07

SCHEDULED TASK PERSISTENCE

STEP: PERSISTENCE
VECTOR: MALWARE

CLUE FOR THREAT ORCHESTRATOR

"Log analysis shows a scheduled task created by the compromised account. The task is set to execute every 6 hours and runs a script from a hidden directory. The activity occurs outside normal business hours. Timestamp metadata indicates advanced timestomping."

WHY THIS WORKS

Scheduled tasks run with privileges of the owner account and survive reboots. They blend in with legitimate administrative tasks. Windows Event Logs may not be forwarded centrally, allowing this persistence mechanism to hide.

THREAT CARD T-08

REGISTRY RUN KEY PERSISTENCE

STEP: PERSISTENCE
VECTOR: MALWARE

CLUE FOR THREAT ORCHESTRATOR

"Registry analysis detects a new entry under HKLM\Software\Microsoft\Windows\CurrentVersion\Run pointing to an executable in an unusual location. The binary has obfuscated metadata and a fake digital signature. It executes at every system startup."

WHY THIS WORKS

Registry Run keys execute at startup with persistence across reboots. They're difficult to distinguish from legitimate startup programs. Endpoint detection solutions must actively monitor registry writes.

THREAT CARD T-09

BEACONING TO C2 SERVER

STEP: C2 & EXFIL
VECTOR: NETWORK

CLUE FOR THREAT ORCHESTRATOR

"Your threat intelligence feed alerts on suspicious outbound HTTPS connections to a domain associated with known malware. Netflow shows regular 3-minute intervals of encrypted traffic. The pattern matches documented C2 beaconing behavior."

WHY THIS WORKS

Beaconing establishes command and control communication with the attacker's infrastructure. Encrypted HTTPS makes payload inspection difficult. Threat intelligence and behavioral analysis (unusual timing) are required for detection.


THREAT

THREAT

THREAT

THREAT

THREAT

THREAT

THREAT

THREAT

THREAT

THREAT CARD T-10

SQL DATABASE EXFILTRATION

STEP: C2 & EXFIL
VECTOR: DATA EXFIL

CLUE FOR THREAT ORCHESTRATOR

"Database audit logs show a large SELECT query executed by a service account retrieving customer data. Results (500k+ records) were piped to a temporary file. System logs show this file was copied to cloud storage via encrypted connection."

WHY THIS WORKS

Database exfiltration bypasses endpoint controls. Attackers use legitimate protocols (HTTPS, SFTP) to trusted services (S3, Dropbox). Without DLP (Data Loss Prevention), and egress filtering, detection is nearly impossible.

THREAT CARD T-11

RANSOMWARE PAYLOAD DEPLOYMENT

STEP: C2 & EXFIL
VECTOR: MALWARE

CLUE FOR THREAT ORCHESTRATOR

"EDR alerts spike as multiple processes begin encrypting files on the file server. Hundreds of files change extension to '.locked'. A ransom note appears on all administrative workstations. Network traffic shows exfil before encryption began (double extortion tactic)."

WHY THIS WORKS

Modern ransomware exfiltrates data first (to extort payment), then encrypts. Fast detection during the exfil phase is critical. Once file encryption begins, recovery becomes difficult. Segmentation and backups are essential.

THREAT CARD T-12

BROWSER EXTENSION BACKDOOR

STEP: C2 & EXFIL
VECTOR: DATA EXFIL

CLUE FOR THREAT ORCHESTRATOR

"Browser logs show installation of a suspicious extension claiming to be a productivity tool. Traffic analysis reveals the extension is capturing keystrokes and session cookies. User login credentials for sensitive portals are being sent to a server in a high-risk country."

WHY THIS WORKS

Browser extensions run with full access to user activity. They can capture credentials, intercept HTTPS traffic (before encryption), and persist across browser updates. Extension vetting and endpoint protection are critical defenses.

DEFENSE CARD D-01

EMAIL AUTHENTICATION SETUP

TIER: BASIC - 10 Budget
COUNTERMEASURE: SOCIAL ENGINEERING

DESCRIPTION

Deploy SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain Message Authentication, Reporting & Conformance) to prevent email spoofing. Implement enforcement policies to reject spoofed emails.

EFFECT

Blocks phishing emails claiming to be from your domain. Requires attackers to find alternative vectors. Also provides reporting on spoofing attempts.

DEFENSE CARD D-02

USER SECURITY TRAINING

TIER: BASIC - 10 Budget
COUNTERMEASURE: SOCIAL ENGINEERING

DESCRIPTION

Conduct phishing awareness training for all staff. Teach recognition of suspicious links, sender spoofing, urgency tactics, and credential harvesting attempts. Run simulated phishing campaigns.

EFFECT

Reduces successful phishing rate by 70-80%. Users become your first line of defense. Works best when combined with technical controls.

DEFENSE CARD D-03

WINDOWS UPDATE PATCHING

TIER: BASIC - 10 Budget
COUNTERMEASURE: WEB EXPLOIT

DESCRIPTION

Deploy automated Windows Update management across all systems. Establish patch deployment timelines (critical = 48 hours, high = 2 weeks). Audit compliance with patch reporting.

EFFECT

Closes browser and kernel vulnerabilities. Prevents watering hole and exploit kit attacks. Should be combined with vulnerability scanning to identify gaps.

DEFENSE CARD D-04

NETWORK FIREWALL RULES

TIER: BASIC - 10 Budget
COUNTERMEASURE: NETWORK

DESCRIPTION

Deploy perimeter firewall rules to block unauthorized outbound protocols. Default-deny for unusual ports and known malware C2 domains. Whitelist only necessary business traffic.

EFFECT

Prevents early-stage lateral movement and C2 beaconing. Slows attacker reconnaissance. Must be maintained with threat intelligence feeds.

DEFENSE CARD D-05

LOG CENTRALIZATION

TIER: BASIC - 10 Budget
COUNTERMEASURE: MALWARE

DESCRIPTION

Deploy centralized log aggregation (syslog, Splunk, ELK). Forward Windows Event Logs, firewall logs, DNS queries, and proxy logs to central SIEM. Configure syslog integrity protection.

EFFECT

Makes local log tampering difficult. Provides investigative visibility into attacker activities. Foundation for threat hunting and compliance.

DEFENSE CARD D-06

BASIC ANTIVIRUS DEPLOYMENT

TIER: BASIC - 10 Budget
COUNTERMEASURE: MALWARE

DESCRIPTION

Deploy signature-based antivirus across all endpoints. Enable automatic definition updates (daily). Configure real-time file and email scanning.

EFFECT

Catches known malware variants. Does not detect zero-day or polymorphic malware. Useful as part of defense-in-depth but insufficient as primary defense.


THREAT


THREAT


THREAT


DEFENSE


DEFENSE


DEFENSE


DEFENSE


DEFENSE


DEFENSE

DEFENSE CARD D-19

BACKUP & DISASTER RECOVERY

TIER: BASIC - 10 Budget
COUNTERMEASURE: MALWARE

DESCRIPTION

Implement the 3-2-1 backup strategy: 3 copies of data, 2 different storage types, 1 offsite copy. Test restore procedures quarterly.

EFFECT

Enables rapid recovery from ransomware. Ensures data availability even if primary systems are compromised. Critical for business continuity.

DEFENSE CARD D-23

IR PROGRAM & RUNBOOKS

TIER: BASIC - 10 Budget
COUNTERMEASURE: NETWORK

DESCRIPTION

Establish an incident response program with detailed runbooks for common scenarios: malware infection, data exfiltration, ransomware, insider threats, supply chain compromise. Include roles, responsibilities, and communication plans.

EFFECT

Enables faster, more coordinated response when incidents occur. Reduces confusion during high- pressure situations. Improves incident containment and recovery time.

DEFENSE CARD D-07

MULTI-FACTOR AUTHENTICATION (MFA)

TIER: ADVANCED - 15 Budget
COUNTERMEASURE: CREDENTIAL ABUSE

DESCRIPTION

Deploy MFA for all remote access (VPN, RDP), email, and admin portals. Use authenticator apps or hardware tokens (not SMS). Enforce MFA on sensitive user accounts.

EFFECT

Makes compromised credentials useless without the second factor. Blocks credential stuffing attacks. Most effective single security measure against account takeover.

DEFENSE CARD D-08

EDR (ENDPOINT DETECTION & RESPONSE)

TIER: ADVANCED - 15 Budget
COUNTERMEASURE: MALWARE

DESCRIPTION

Deploy EDR agent on all endpoints. Monitor process execution, file creation, registry modifications, and memory injection attempts. Enable behavioral analytics and automated response.

EFFECT

Detects living-off-the-land attacks (PowerShell, cmd, scheduled tasks). Enables fast incident response and threat hunting. Provides deep visibility into attack progression.

DEFENSE CARD D-09

NETWORK SEGMENTATION

TIER: ADVANCED - 15 Budget
COUNTERMEASURE: NETWORK

DESCRIPTION

Implement VLANs and microsegmentation to separate user workstations from servers. Deploy firewall rules between segments. Implement zero- trust network access controls.

EFFECT

Prevents lateral movement via SMB and other internal protocols. Limits blast radius of compromise. Forces attackers to find alternate paths. Combined with MFA, highly effective.

DEFENSE CARD D-10

SIEM CORRELATION RULES

TIER: ADVANCED - 15 Budget
COUNTERMEASURE: NETWORK

DESCRIPTION

Create SIEM rules to detect attack patterns: failed login spikes, privilege escalation attempts, unusual process creation, scheduled task creation, and data exfil indicators.

EFFECT

Correlates events across logs to detect multi-step attacks. Reduces alert fatigue through smart aggregation. Enables faster investigation and response.

DEFENSE CARD D-11

DATA LOSS PREVENTION (DLP)

TIER: ADVANCED - 15 Budget
COUNTERMEASURE: DATA EXFIL

DESCRIPTION

Deploy DLP to monitor outbound data transfers. Classify sensitive data (customer PII, source code, trade secrets). Block or alert on unauthorized transfers to cloud storage, email, USB, or external networks.

EFFECT

Prevents SQL database exfiltration and bulk data theft. Detects unusual data access patterns. Enforces data security policies. Works best with strong authentication and encryption.

DEFENSE CARD D-12

PASSWORD MANAGER & VAULT

TIER: ADVANCED - 15 Budget
COUNTERMEASURE: CREDENTIAL ABUSE

DESCRIPTION

Deploy enterprise password vault (CyberArk, HashiCorp Vault). Enforce strong unique passwords. Implement password rotation policies for service accounts. Enable audit logging for credential access.

EFFECT

Prevents credential reuse attacks. Makes credential stuffing difficult. Provides audit trail for compliance and incident investigation.

DEFENSE CARD D-18

INTRUSION PREVENTION SYSTEM (IPS)

TIER: ADVANCED - 15 Budget
COUNTERMEASURE: WEB EXPLOIT

DESCRIPTION

Deploy network-based IPS with exploit signatures. Monitor for known CVE exploitation patterns. Configure WAF (Web Application Firewall) rules for SQL injection, XSS, and other OWASP Top 10 attacks.

EFFECT

Blocks exploitation attempts in transit. Prevents watering hole and web exploit attacks. Most effective when combined with patching.


D E F E N S E


D E F E N S E


D E F E N S E


D E F E N S E


D E F E N S E


D E F E N S E


D E F E N S E


D E F E N S E


D E F E N S E

DEFENSE CARD D-24

THREAT INTELLIGENCE INTEGRATION

TIER: ADVANCED - 15 Budget
COUNTERMEASURES: NETWORK, DATA EXFIL

DESCRIPTION

Subscribe to threat intelligence feeds (MISP, VirusTotal, AlienVault OTX). Integrate IOCs (Indicators of Compromise) into firewall, SIEM, and proxy. Participate in information sharing communities.

EFFECT

Enables faster detection of known malicious IPs and domains. Identifies emerging threats targeting your industry. Reduces detection time from days to minutes.

DEFENSE CARD D-13

THREAT HUNTING PROGRAM

TIER: ELITE - 25 Budget
COUNTERMEASURE: MALWARE

DESCRIPTION

Establish proactive threat hunting using MITRE ATT&CK framework. Hunt for living-off-the-land techniques, anomalous processes, suspicious registry changes, and memory injection. Use automated tools (OSQuery, Velociraptor).

EFFECT

Finds advanced attacks that bypass signature-based detection. Detects LSASS dumping, scheduled task persistence, and registry backdoors. Reduces dwell time significantly.

DEFENSE CARD D-14

MEMORY FORENSICS

TIER: ELITE - 25 Budget
COUNTERMEASURE: MALWARE

DESCRIPTION

Deploy memory capture and analysis (Volatility, Memoryze). Create memory images of suspicious systems. Analyze for credential dumping, injected code, and rootkits. Extract evidence for incident response.

EFFECT

Detects Mimikatz attacks and credential harvesting. Reveals attacker activities hidden from disk forensics. Critical for identifying advanced persistence mechanisms.

DEFENSE CARD D-15

DECEPTION TECHNOLOGY (HONEYPOTS)

TIER: ELITE - 25 Budget
COUNTERMEASURE: NETWORK

DESCRIPTION

Deploy decoy systems (fake file servers, databases, credentials) to detect lateral movement. Create canary tokens that alert when accessed. Deploy honeypots for web exploit detection.

EFFECT

Any access to honeypots indicates active compromise. Detects lateral movement with zero false positives. Slows attacker progress and forces reconnaissance, increasing detection time.

DEFENSE CARD D-16

CREDENTIAL GUARD & SECURE BOOT

TIER: ELITE - 25 Budget
COUNTERMEASURE: CREDENTIAL ABUSE

DESCRIPTION

Enable Windows Credential Guard to isolate LSASS in virtualized container. Implement UEFI Secure Boot to prevent bootkit attacks. Enable TPM attestation for device integrity validation.

EFFECT

Makes Mimikatz credential dumping ineffective. Prevents bootloader manipulation. Ensures firmware integrity. Blocks entire classes of attacks targeting early boot stage.

DEFENSE CARD D-17

ADVANCED MALWARE SANDBOX

TIER: ELITE - 25 Budget
COUNTERMEASURE: MALWARE

DESCRIPTION

Deploy advanced sandboxing solution (Cuckoo, Detonate, hybrid-analysis). Analyze suspicious files/URLs in isolated environments. Generate behavioral indicators and YARA rules. Share IOCs with threat intel.

EFFECT

Detects zero-day malware and unknown exploits. Analyzes evasion tactics. Generates detection rules for SIEM. Prevents spread of novel malware.

DEFENSE CARD D-20

ZERO TRUST ACCESS CONTROL

TIER: ELITE - 25 Budget
COUNTERMEASURE: CREDENTIAL ABUSE

DESCRIPTION

Implement zero-trust architecture: verify every access request regardless of source. Deploy device identity, user identity, and behavior analytics. Implement conditional access policies.

EFFECT

Eliminates implicit trust based on network location. Even compromised devices cannot access sensitive resources without proper authentication and behavior validation.

DEFENSE CARD D-21

CONTAINER SECURITY & ORCHESTRATION

TIER: ELITE - 25 Budget
COUNTERMEASURE: MALWARE

DESCRIPTION

Deploy container runtime security (Falco, Sysdig). Implement image scanning for vulnerabilities. Use policy enforcement engines (OPA/ Gatekeeper). Implement network policies for container segmentation.

EFFECT

Detects container escape attempts. Prevents vulnerable images from running. Limits lateral movement within containerized environments. Critical for modern cloud applications.

DEFENSE CARD D-22

SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)

TIER: ELITE - 25 Budget
COUNTERMEASURE: NETWORK

DESCRIPTION

Deploy enterprise SIEM (Splunk, ELK, QRadar). Centralize logs from all sources. Implement automated correlation rules, threat intelligence integration, and incident response workflows.

EFFECT

Provides centralized visibility into all security events. Enables rapid threat detection and investigation. Foundation for a mature incident response program.


D E F E N S E

D E F E N S E

D E F E N S E

D E F E N S E

D E F E N S E

D E F E N S E

D E F E N S E

D E F E N S E

D E F E N S E