IOC Cheat Sheet for SOC Analysts

User Behavior IOCs

IOC	Description	Why It's Suspicious
Unusual login times	Logins during late nights or weekends	May indicate compromised accounts
Geographically impossible logins	Same user logging in from distant locations	Often sign of credential theft
High number of failed logins	Brute-force or password spray attack	Indicates an attempt to gain access
New admin accounts	Privileged accounts suddenly appear	May indicate attacker persistence

Network IOCs

IOC	Description	Why It's Suspicious
Beaconing behavior	Regular outbound traffic	Common for malware calling home
Unusual ports/protocols	E.g., SSH on port 8080	Used to bypass firewalls
Large data exfiltration	Unexpected data to external IPs	Sign of data theft
Connection to malicious IPs	Known bad IPs/domains	Evidence of malware communication

Host/System IOCs

IOC	Description	Why It's Suspicious
Unknown running processes	Processes with random names	Often malware trying to hide
Execution from odd directories	Like Temp or AppData	Indicators of staging tools
PowerShell with base64	Encoded script execution	Suspicious obfuscation
Disabled security tools	AV/logs turned off	Strong attacker sign

File-Related IOCs

IOC	Description	Why It's Suspicious
Known malware hashes	MD5, SHA-1, SHA-256	Confirms infection
Dropped files in odd locations	E.g., %TEMP%, %APPDATA%	Malware hiding spots
Unsigned or fake signed EXEs	Missing or fake digital signatures	Common in trojans
File masquerading	e.g., Invoice.docx.exe	Trick to fool users

Email/Phishing IOCs

IOC	Description	Why It's Suspicious
Suspicious sender domain	Misspelled domains	Often phishing

IOC Cheat Sheet for SOC Analysts

Embedded links	URL shorteners or redirections	May lead to malware
Attachments with macros	.docm, .xlsm files	Used to deliver payloads
Spoofed headers	Fake 'From' or relay servers	Social engineering signs