Sekurenetweb.com
csexams.com

Spot the Invisible:

A Quick Guide to Detecting Living Off the Land (LOTL) Attacks

Sekurenet

Unusual Use of Legitimate Tools

- ✓ Command-Line Utilities: Look for unexpected or unusual use of command-line tools like PowerShell, WMIC (Windows Management Instrumentation Command), or CertUtil. These tools are often used by attackers to execute scripts, download payloads, or perform reconnaissance.

- ✓ Fileless Execution: Be aware of processes running in memory without a corresponding file on disk. This could indicate the use of in-memory execution techniques.

Abnormal System Behavior

- ✓ Spikes in Network Activity: Unusual outbound traffic from typically low-traffic devices, or devices communicating with unknown IP addresses or domains.

- ✓ Unexpected Privilege Escalation: Monitor for accounts suddenly gaining elevated privileges without a clear justification.

Anomalous Process Relationships

- ✓ Process Spawning: Legitimate processes spawning child processes in an unusual manner (e.g., a web browser starting a PowerShell script).

- ✓ Parent-Child Process Mismatches: Detection of atypical parent-child process relationships, such as a text editor spawning a network connection.

Behavioral Analysis

- ✓ Heuristic-Based Detection: Employ behavior-based detection mechanisms that can spot deviations from normal operations, even if no malicious signature is present.

- ✓ User and Entity Behavior Analytics (UEBA): Monitor for deviations in user or system behavior, such as accessing resources at unusual times or from unusual locations.