CHEAT SHEET

A concise guide for identifying and managing suspicious Windows services.

1 Key Indicators

Be aware of these indicators

- Unusual Service Names
- Unexpected Locations
- Unknown Publishers
- Unusual Resource Usage
- Inconsistent behaviour
- Network Activity
- Autostart Mechanisms
- Lack of Documentations
- Modification of System documents
- Resistance to Analysis

2 Types of Window Services

Local Services

Provide functionalities specific to user accounts, often without network-wide impact or requirements.

Network Services

Manage data exchange and communication across networked systems, ensuring connectivity and access.

System Services

Critical for system stability and operation, running essential processes and maintenance tasks.

Third-party Services

Added by non-Windows software, offering additional features or enhancing existing functionalities.

3 Comparison Table

Legitimate Service Name	Legitimate Service Name	Reason for Suspicion
svchost.exe	svch0st.exe	Zero instead of ‘o’
lsass.exe	Isass.exe	Capital ‘I’ instead of ‘l’
services.exe	service.exe	Missing ‘s’ at the end
winlogon.exe	winlogin.exe	‘i’ replaced with ‘o’
smss.exe	sms.exe	Missing ‘s’ at the end

Legitimate Service Name	Legitimate Service Name	Reason for Suspicion
csrss.exe	cssrs.exe	Transposed letters
spoolsv.exe	spoolvs.exe	Transposed letters
explorer.exe	iexplorer.exe	Added ‘i’ at the beginning
ctfmon.exe	ctfmoon.exe	Added ‘o’ in the name
userinit.exe	userlnit.exe	Transposed letters

4 Best practices

Managing tips to ensure system security

- Routinely check services for new, changed, or unusual activities.
- Use automated tools for real-time detection of suspicious services.
- Keep systems updated to close vulnerabilities exploited by malicious services.
- Restrict service management to prevent unauthorized changes and mitigate risks.
- Have a clear plan for responding to and investigating alerts.

Like Comment Repost

http://blackperldfir.com

https://academy.blackperldfir.com

CHEAT SHEET

A concise guide for identifying and managing suspicious Windows services.

5 Event IDs for Threat Hunting

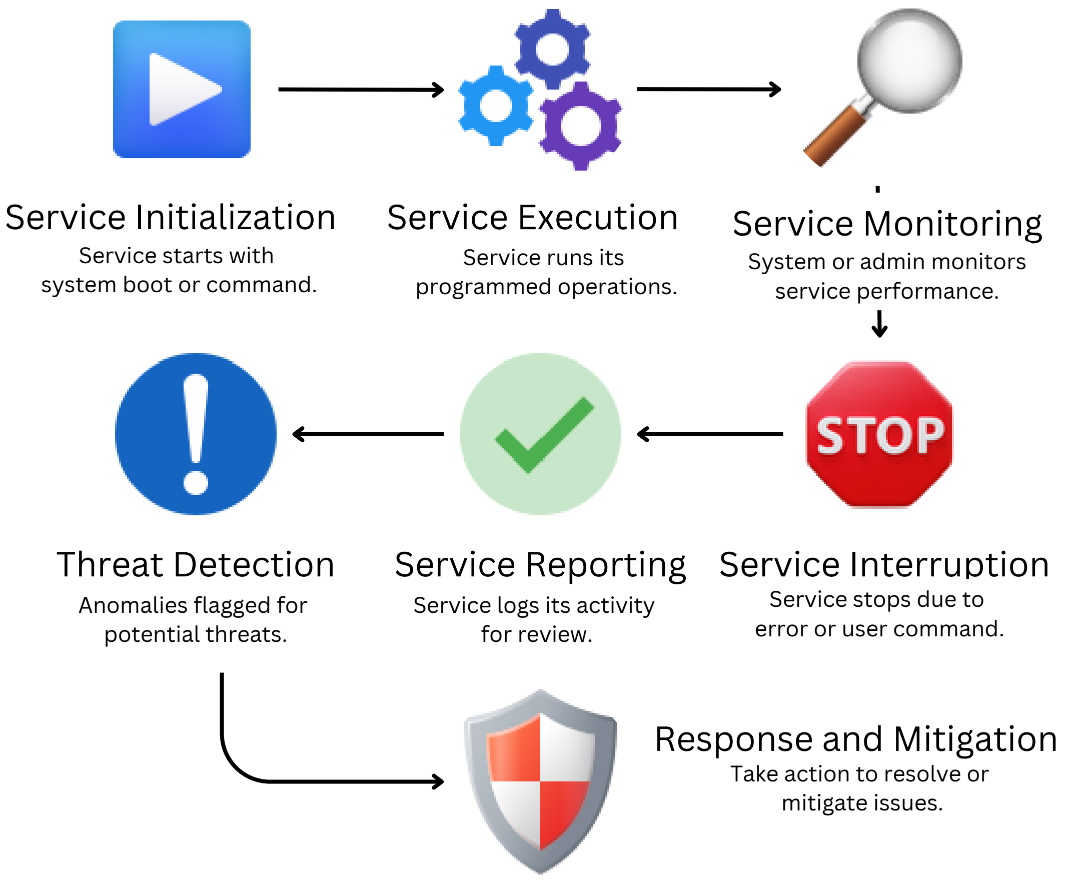
List of Windows Event IDs that are significant for threat hunting

Event ID	Description
4697	A service was installed in the system.
7045	Created when new services are created on the local Windows machine.
7034	The service terminated unexpectedly.
7036	Indicates a service entered the stopped state or the running state.
1102	The audit log was cleared.
4771	Failed Kerberos pre-authentication.

● critical events
● informational events
● security-related events

6 Understanding Process Loads

How potential threats are detected and handled.



Service Initialization
Service starts with system boot or command.

Service Execution
Service runs its programmed operations.

Service Monitoring
System or admin monitors service performance.

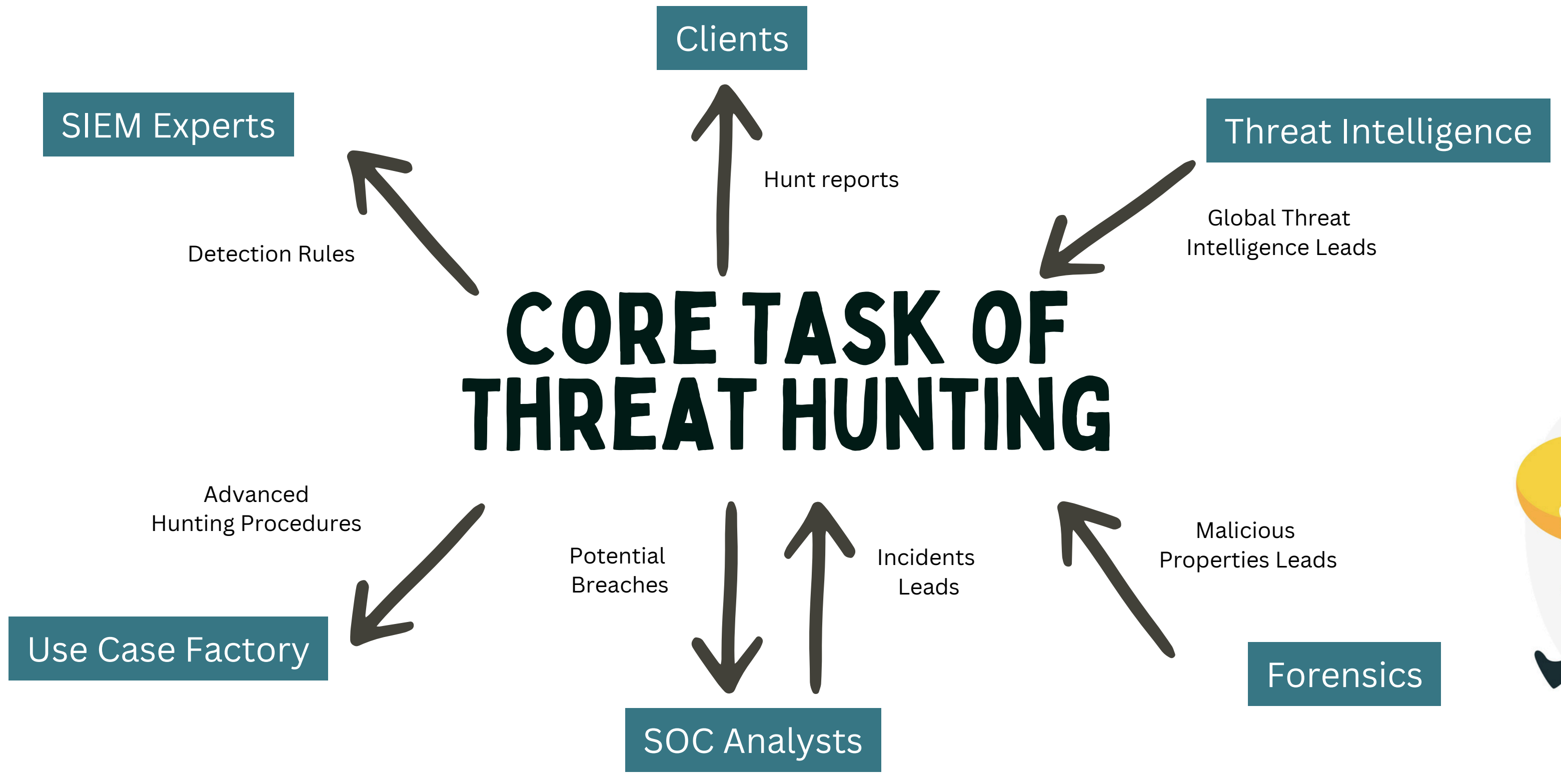
Service Interruption
Service stops due to error or user command.

Service Reporting
Service logs its activity for review.

Threat Detection
Anomalies flagged for potential threats.

Response and Mitigation
Take action to resolve or mitigate issues.

7 Threat Hunting Strategies



CORE TASK OF THREAT HUNTING

Clients — Hunt reports

SIEM Experts — Detection Rules

Threat Intelligence — Global Threat Intelligence Leads

Use Case Factory — Advanced Hunting Procedures

SOC Analysts — Potential Breaches — Incidents Leads

Forensics — Malicious Properties Leads

Like Comment Repost

http://blackperldfir.com

https://academy.blackperldfir.com