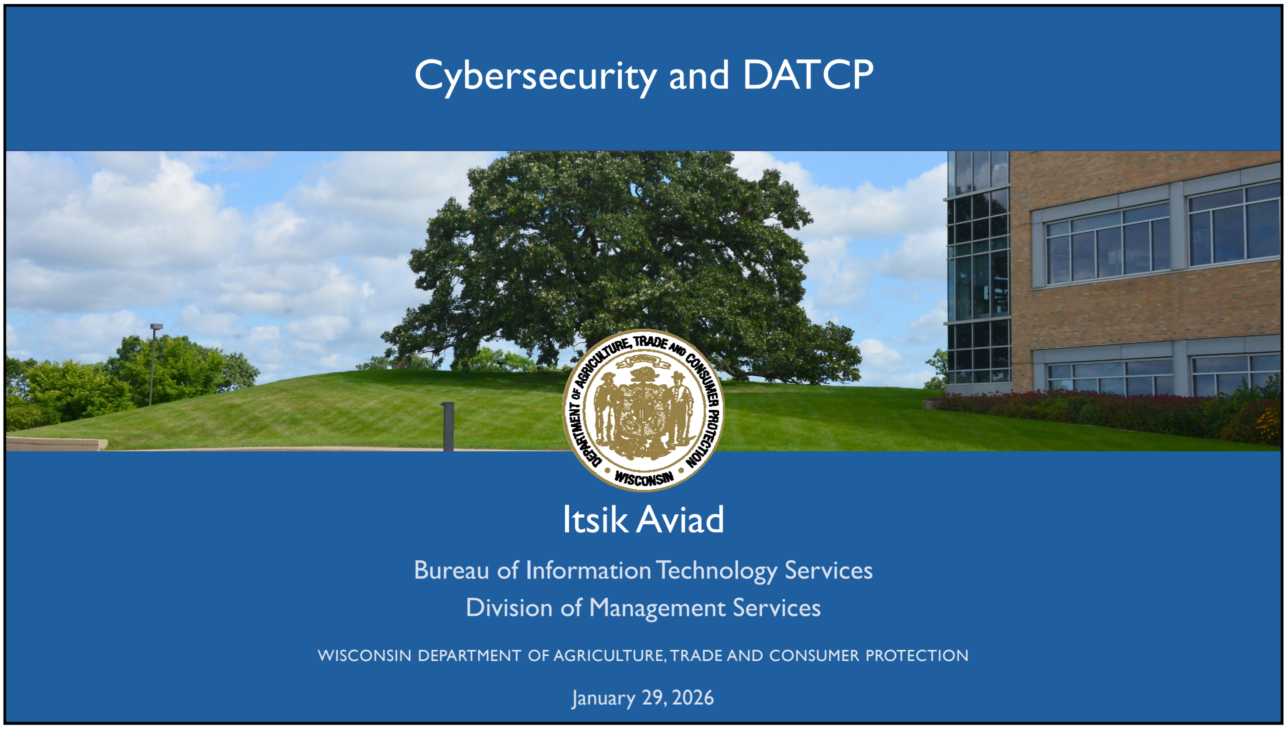


Cybersecurity and DATCP

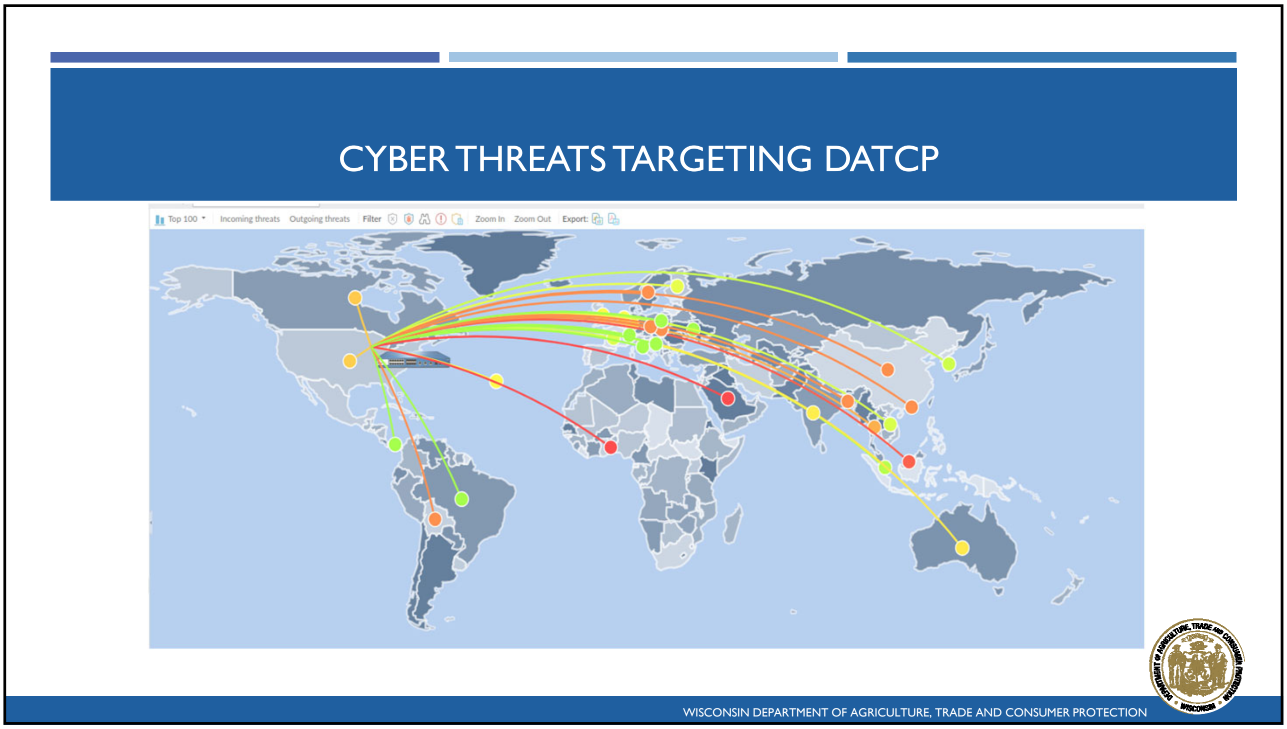
Itsik Aviad

Bureau of Information Technology Services
Division of Management Services

WISCONSIN DEPARTMENT OF AGRICULTURE, TRADE AND CONSUMER PROTECTION

January 29, 2026

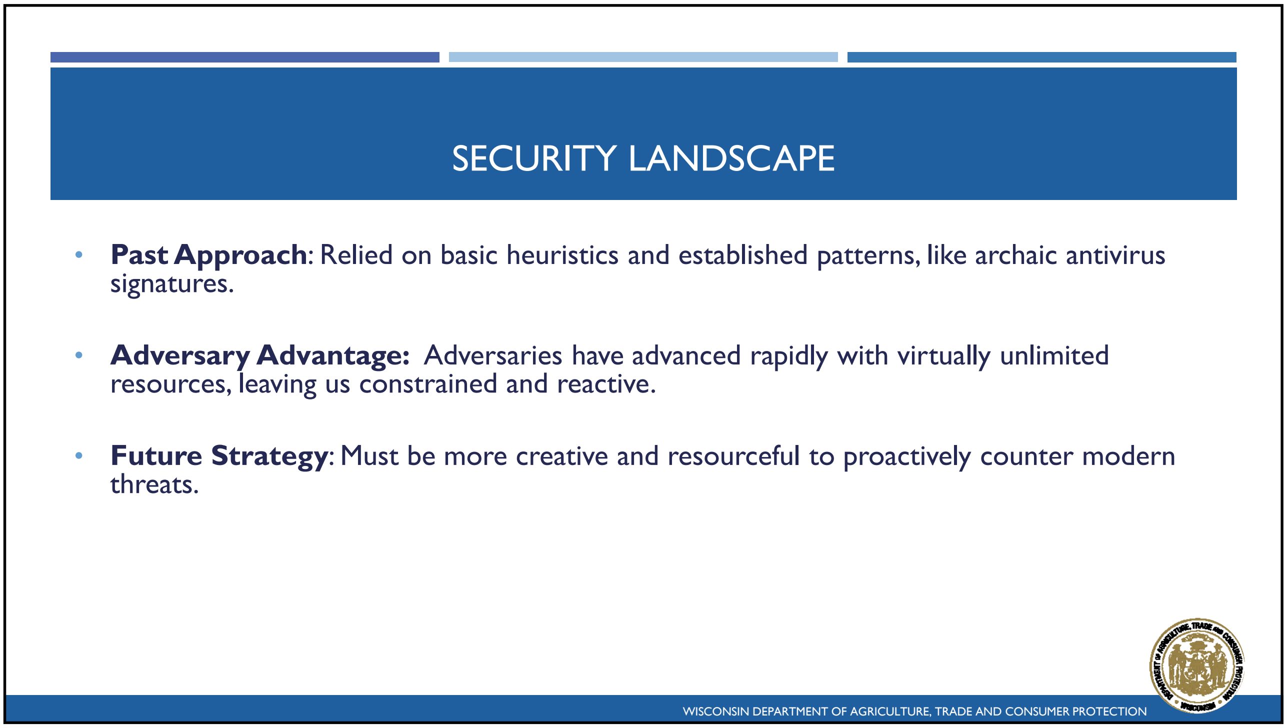
1



CYBER THREATS TARGETING DATCP

WISCONSIN DEPARTMENT OF AGRICULTURE, TRADE AND CONSUMER PROTECTION

2

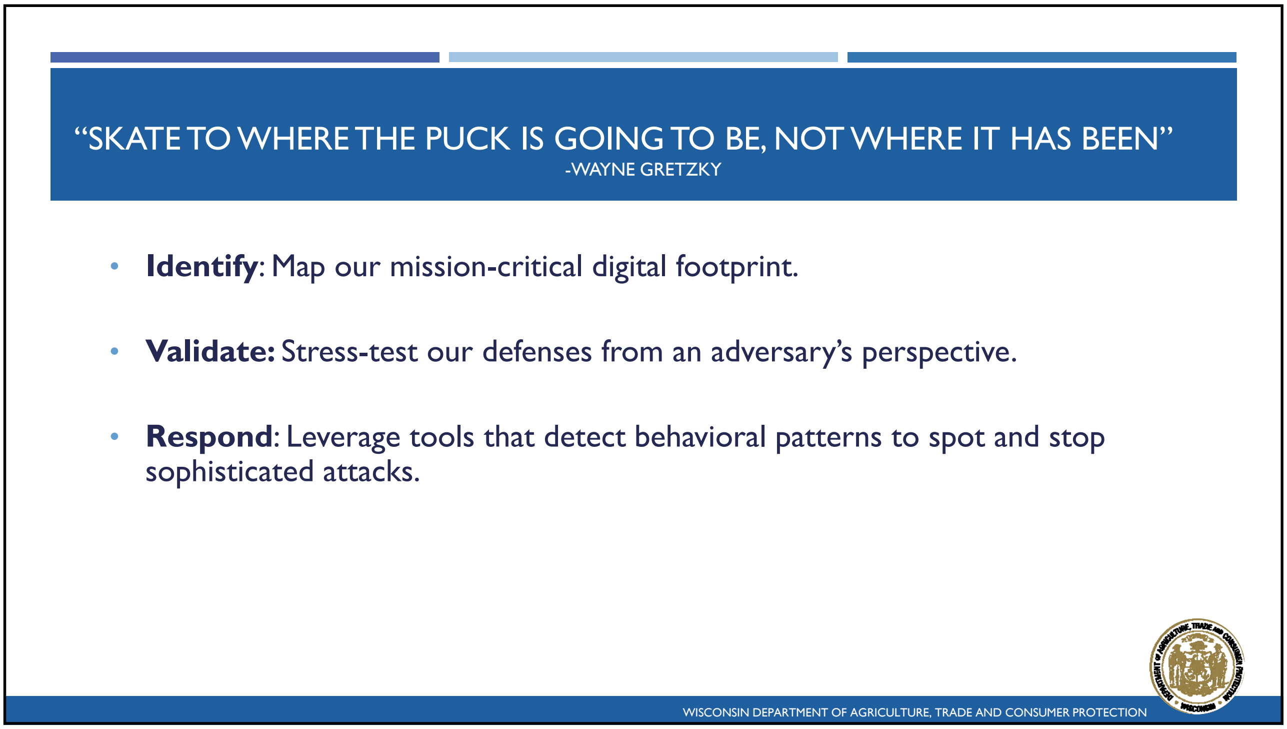


SECURITY LANDSCAPE

- **Past Approach**: Relied on basic heuristics and established patterns, like archaic antivirus signatures.
- **Adversary Advantage:** Adversaries have advanced rapidly with virtually unlimited resources, leaving us constrained and reactive.
- **Future Strategy**: Must be more creative and resourceful to proactively counter modern threats.

WISCONSIN DEPARTMENT OF AGRICULTURE, TRADE AND CONSUMER PROTECTION

3



"SKATE TO WHERE THE PUCK IS GOING TO BE, NOT WHERE IT HAS BEEN"

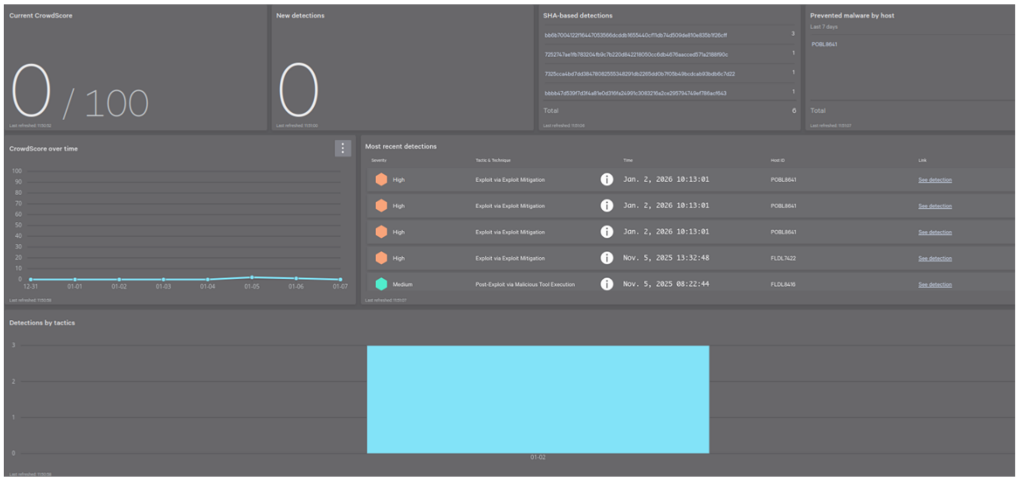
-WAYNE GRETZKY

- **Identify**: Map our mission-critical digital footprint.
- **Validate:** Stress-test our defenses from an adversary's perspective.
- **Respond**: Leverage tools that detect behavioral patterns to spot and stop sophisticated attacks.

WISCONSIN DEPARTMENT OF AGRICULTURE, TRADE AND CONSUMER PROTECTION

4

DATCP'S ENDPOINT DASHBOARD



Current CrowdScore

0 / 100

Last refreshed: 11:50:52

New detections

0

Last refreshed: 11:51:00

SHA-based detections

bb6b7004122f16447053566dcddb1655440cf11db74d509de810e835b1f26cff	3
7252747ae1fb783204fb9c7b220d842218050cc6db4676aacced571a2188f90c	1
7325cca4bd7dd38478082555348291db2265dd0b7f05b49bcdcab93bdb6c7d22	1
bbbb47d539f7d3f4a81e0d316fa24991c3083216a2ce295794749ef786acf643	1
Total	6

Last refreshed: 11:51:06

Prevented malware by host

Last 7 days

POBL8641

Total

Last refreshed: 11:51:07

CrowdScore over time

Last refreshed: 11:50:58

Most recent detections

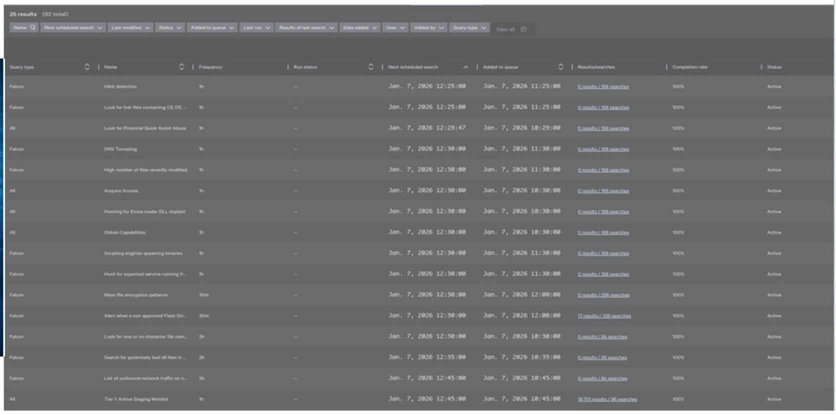
Severity	Tactic & Technique	Time	Host ID	Link
High	Exploit via Exploit Mitigation	Jan. 2, 2026 10:13:01	POBL8641	See detection
High	Exploit via Exploit Mitigation	Jan. 2, 2026 10:13:01	POBL8641	See detection
High	Exploit via Exploit Mitigation	Jan. 2, 2026 10:13:01	POBL8641	See detection
High	Exploit via Exploit Mitigation	Nov. 5, 2025 13:32:48	FLDL7422	See detection
Medium	Post-Exploit via Malicious Tool Execution	Nov. 5, 2025 08:22:44	FLDL8416	See detection

Last refreshed: 11:51:07

Detections by tactics

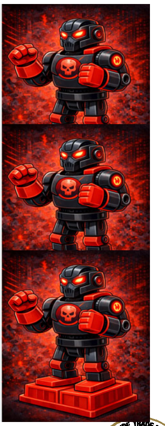
Last refreshed: 11:50:58

ALWAYS-ON PROTECTION

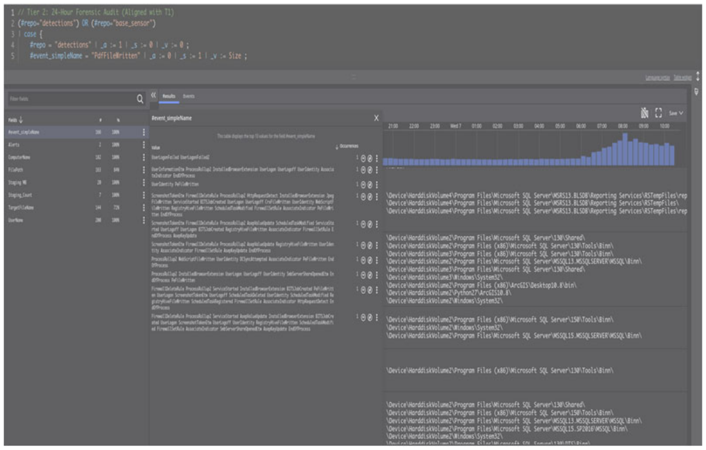


25 results (92 total)

Query type	Name	Frequency	Run status	Next scheduled search	Added to queue	Results/searches	Completion rate	Status
Falcon	Hikit detection	1h	–	Jan. 7, 2026 12:25:00	Jan. 7, 2026 11:25:00	0 results / 168 searches	100%	Active
Falcon	Look for link files containing CS, DS, ...	1h	–	Jan. 7, 2026 12:25:00	Jan. 7, 2026 11:25:00	0 results / 168 searches	100%	Active
All	Look for Potential Quick Assist Abuse	1h	–	Jan. 7, 2026 12:29:47	Jan. 7, 2026 10:29:00	0 results / 168 searches	100%	Active
Falcon	DNS Tunneling	1h	–	Jan. 7, 2026 12:30:00	Jan. 7, 2026 11:30:00	0 results / 168 searches	100%	Active
Falcon	High number of files recently modified	1h	–	Jan. 7, 2026 12:30:00	Jan. 7, 2026 11:30:00	0 results / 168 searches	100%	Active
All	Acquire Access	1h	–	Jan. 7, 2026 12:30:00	Jan. 7, 2026 10:30:00	0 results / 168 searches	100%	Active
All	Hunting for Evora loader DLL implant	1h	–	Jan. 7, 2026 12:30:00	Jan. 7, 2026 10:30:00	0 results / 168 searches	100%	Active
All	Obtain Capabilities	1h	–	Jan. 7, 2026 12:30:00	Jan. 7, 2026 10:30:00	0 results / 168 searches	100%	Active
Falcon	Scripting engines spawning binaries	1h	–	Jan. 7, 2026 12:30:00	Jan. 7, 2026 11:30:00	0 results / 168 searches	100%	Active
Falcon	Hunt for expected service running fr...	1h	–	Jan. 7, 2026 12:30:00	Jan. 7, 2026 11:30:00	0 results / 168 searches	100%	Active
Falcon	Mass file encryption patterns	30m	–	Jan. 7, 2026 12:30:00	Jan. 7, 2026 12:00:00	0 results / 336 searches	100%	Active
Falcon	Alert when a non approved Flash Dri...	30m	–	Jan. 7, 2026 12:30:00	Jan. 7, 2026 12:00:00	17 results / 336 searches	100%	Active
Falcon	Look for one or no character file nam...	2h	–	Jan. 7, 2026 12:30:00	Jan. 7, 2026 10:30:00	0 results / 84 searches	100%	Active
Falcon	Search for potentially bad dll files in ...	2h	–	Jan. 7, 2026 12:35:00	Jan. 7, 2026 10:35:00	0 results / 85 searches	100%	Active
Falcon	List of outbound network traffic on n...	2h	–	Jan. 7, 2026 12:45:00	Jan. 7, 2026 10:45:00	0 results / 84 searches	100%	Active
All	Tier 1: Active Staging Monitor	1h	–	Jan. 7, 2026 12:45:00	Jan. 7, 2026 10:45:00	18,701 results / 96 searches	100%	Active



PROACTIVE ANOMALY DETECTION



```
// Tier 2: 24-Hour Forensic Audit (Aligned with T1)
(#repo="detections") OR (#repo="base_sensor")
| case {
    #repo = "detections" | _o := 1 | _s := 0 | _v := 0 ;
    #event_simpleName = "PdfFileWritten" | _o := 0 | _s := 1 | _v := Size ;
```

Fields	#	%
#event_simpleName	166	100%
Alerts	2	100%
ComputerName	182	100%
FilePath	183	84%
Staging_MB	28	100%
Staging_Count	7	100%
TargetFileName	144	72%
UserName	200	100%

#event_simpleName

This table displays the top 10 values for the field #event_simpleName

Value	Occurrences
UserLogonFailed UserLogonFailed2	1
UserInformationEtw ProcessRollup2 InstalledBrowserExtension UserLogon UserLogoff UserIdentity AssociateIndicator EndOfProcess	1
UserIdentity PeFileWritten	1
ScreenshotTakenEtw FirewallDeleteRule ProcessRollup2 HttpRequestDetect InstalledBrowserExtension JpegFileWritten ServiceStarted BITSJobCreated UserLogon UserLogoff CrxFileWritten UserIdentity WebScriptFileWritten RegistryHiveFileWritten ScheduledTaskModified FirewallSetRule AssociateIndicator PeFileWritten EndOfProcess	1
ScreenshotTakenEtw FirewallDeleteRule ProcessRollup2 AsepValueUpdate ScheduledTaskModified ServiceStarted UserLogoff UserLogon BITSJobCreated RegistryHiveFileWritten AssociateIndicator FirewallSetRule EndOfProcess AsepKeyUpdate	1
ScreenshotTakenEtw FirewallDeleteRule ProcessRollup2 AsepValueUpdate RegistryHiveFileWritten UserIdentity AssociateIndicator FirewallSetRule AsepKeyUpdate EndOfProcess	1
ProcessRollup2 WebScriptFileWritten UserIdentity DCSyncAttempted AssociateIndicator PeFileWritten EndOfProcess	1
ProcessRollup2 InstalledBrowserExtension UserLogon UserLogoff UserIdentity SmbServerShareOpenedEtw EndOfProcess PeFileWritten	1
FirewallDeleteRule ProcessRollup2 ServiceStarted InstalledBrowserExtension BITSJobCreated PeFileWritten UserLogon ScreenshotTakenEtw UserLogoff ScheduledTaskDeleted UserIdentity ScheduledTaskModified RegistryHiveFileWritten ScheduledTaskRegistered FirewallSetRule AssociateIndicator HttpRequestDetect EndOfProcess	1
FirewallDeleteRule ProcessRollup2 ServiceStarted AsepValueUpdate InstalledBrowserExtension BITSJobCreated UserLogon ScreenshotTakenEtw UserLogoff UserIdentity RegistryHiveFileWritten ScheduledTaskModified FirewallSetRule AssociateIndicator SmbServerShareOpenedEtw AsepKeyUpdate EndOfProcess	1

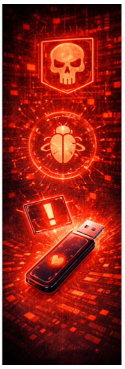
```
\Device\HarddiskVolume4\Program Files\Microsoft SQL Server\MSRS13.BLSDB\Reporting Services\RSTempFiles\rep
\Device\HarddiskVolume4\Program Files\Microsoft SQL Server\MSRS13.BLSDB\Reporting Services\RSTempFiles\
\Device\HarddiskVolume4\Program Files\Microsoft SQL Server\MSRS13.BLSDB\Reporting Services\RSTempFiles\rep

\Device\HarddiskVolume2\Program Files\Microsoft SQL Server\130\Shared\
\Device\HarddiskVolume2\Program Files (x86)\Microsoft SQL Server\130\Tools\Binn\
\Device\HarddiskVolume3\Program Files (x86)\Microsoft SQL Server\130\Tools\Binn\
\Device\HarddiskVolume2\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Binn\
\Device\HarddiskVolume3\Program Files\Microsoft SQL Server\130\Shared\
\Device\HarddiskVolume3\Windows\System32\
\Device\HarddiskVolume2\Program Files (x86)\ArcGIS\Desktop10.8\bin\
\Device\HarddiskVolume2\Python27\ArcGIS10.8\
\Device\HarddiskVolume2\Windows\System32\

\Device\HarddiskVolume2\Program Files (x86)\Microsoft SQL Server\150\Tools\Binn\
\Device\HarddiskVolume2\Windows\System32\
\Device\HarddiskVolume2\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Binn\

\Device\HarddiskVolume2\Program Files (x86)\Microsoft SQL Server\130\Tools\Binn\

\Device\HarddiskVolume2\Program Files\Microsoft SQL Server\130\Shared\
\Device\HarddiskVolume2\Program Files (x86)\Microsoft SQL Server\150\Tools\Binn\
\Device\HarddiskVolume2\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Binn\
\Device\HarddiskVolume2\Program Files\Microsoft SQL Server\MSSQL15.SP2016\MSSQL\Binn\
\Device\HarddiskVolume2\Windows\System32\
\Device\HarddiskVolume2\Program Files\Microsoft SQL Server\130\DTS\Binn\
```



WISCONSIN DEPARTMENT OF AGRICULTURE, TRADE AND CONSUMER PROTECTION

7

Itsik Aviad

Bureau of Information Technology Services

datcp.wi.gov

01/29/2026

8