INE– Cyber Sec

Incident Handling & Response Professional

Logging

Section 04 | Module 02

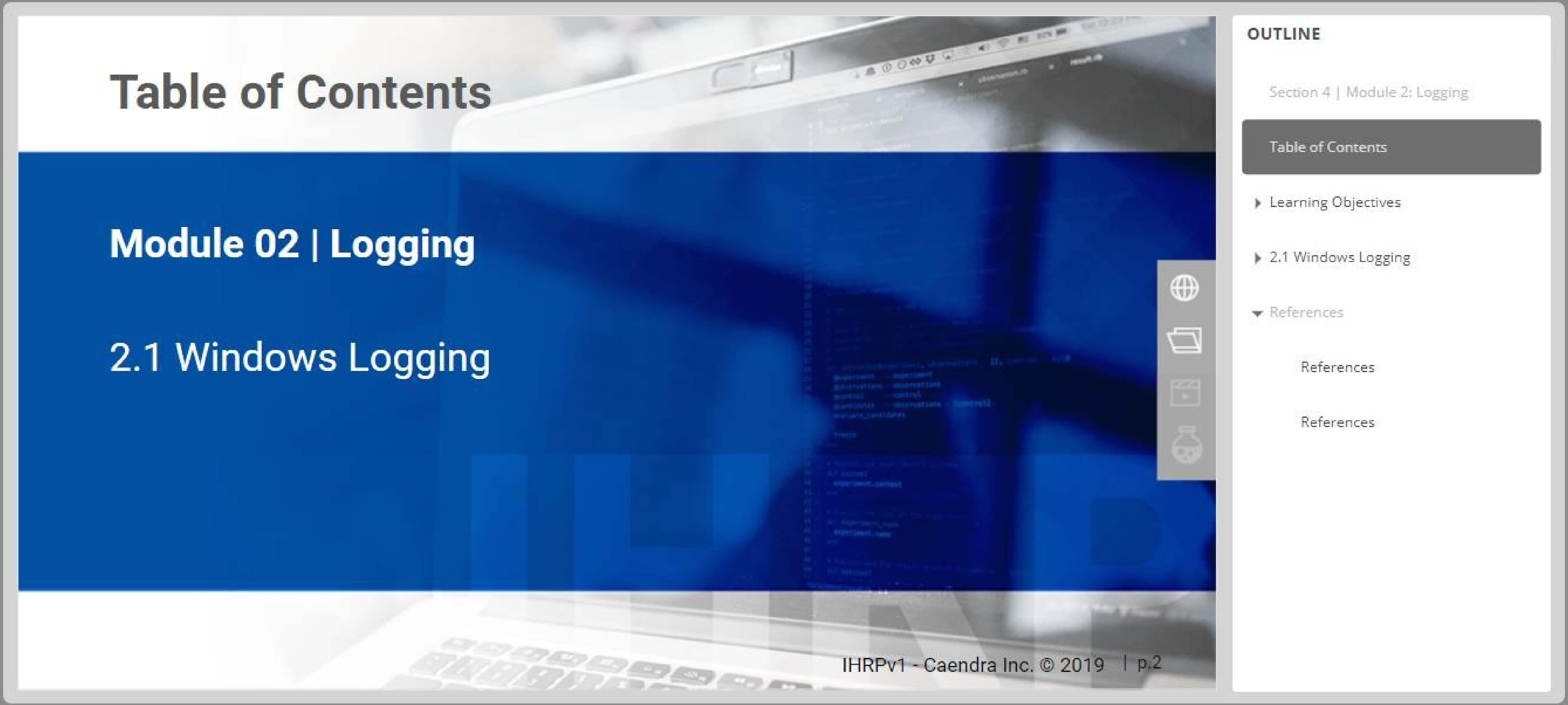
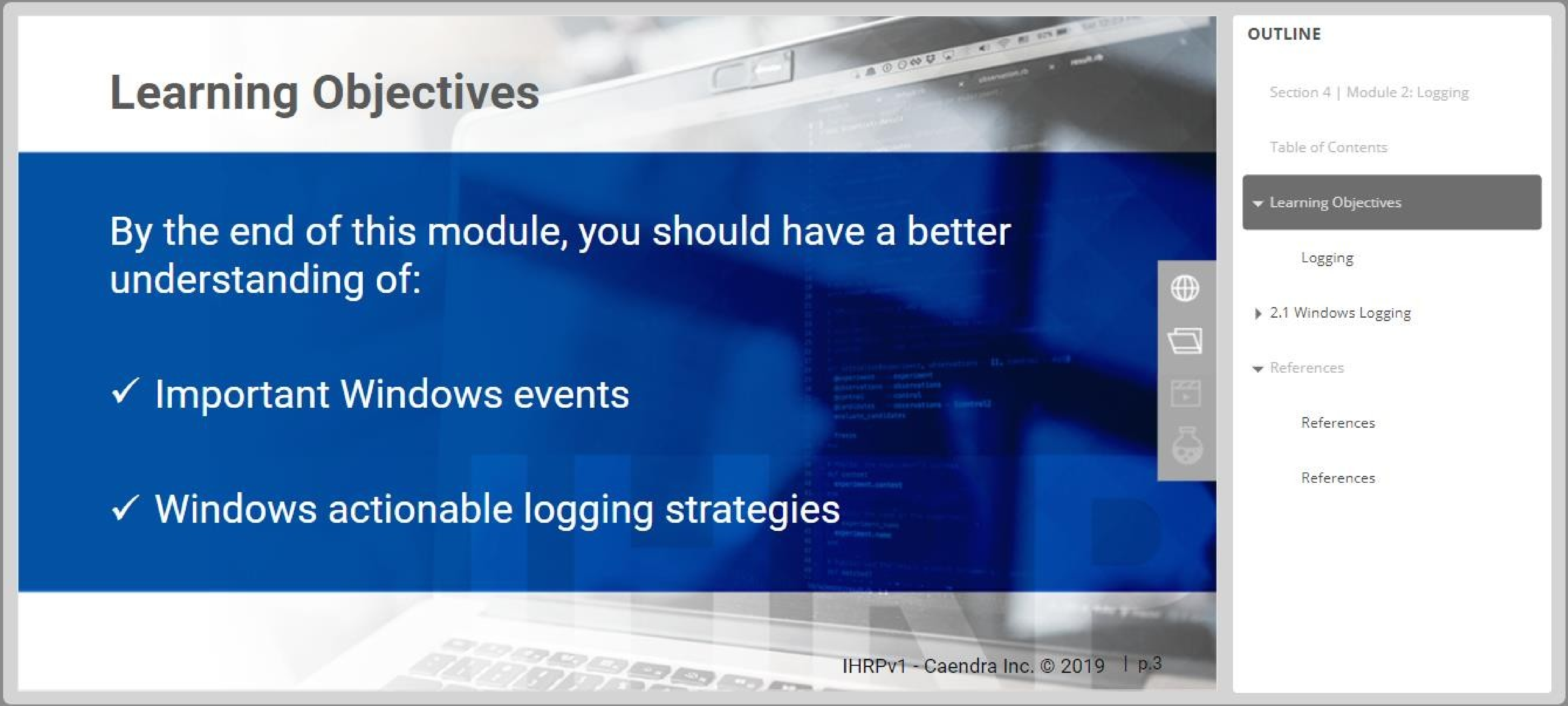


Table of Contents

Module 02 | Logging

2.1 Windows Logging



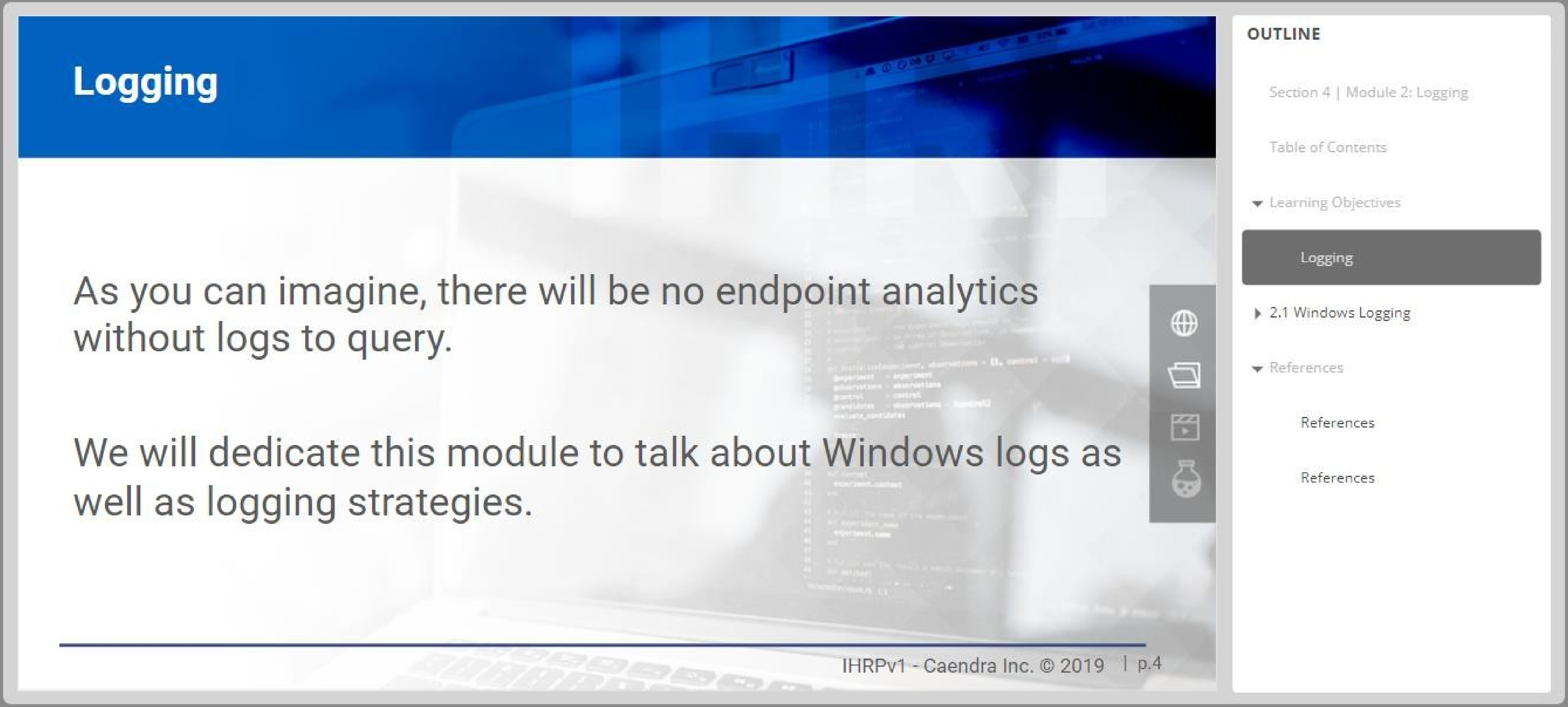
Learning Objectives

By the end of this module, you should have a better understanding of:

✓ Important Windows events

✓ Windows actionable logging strategies

OUTLINE



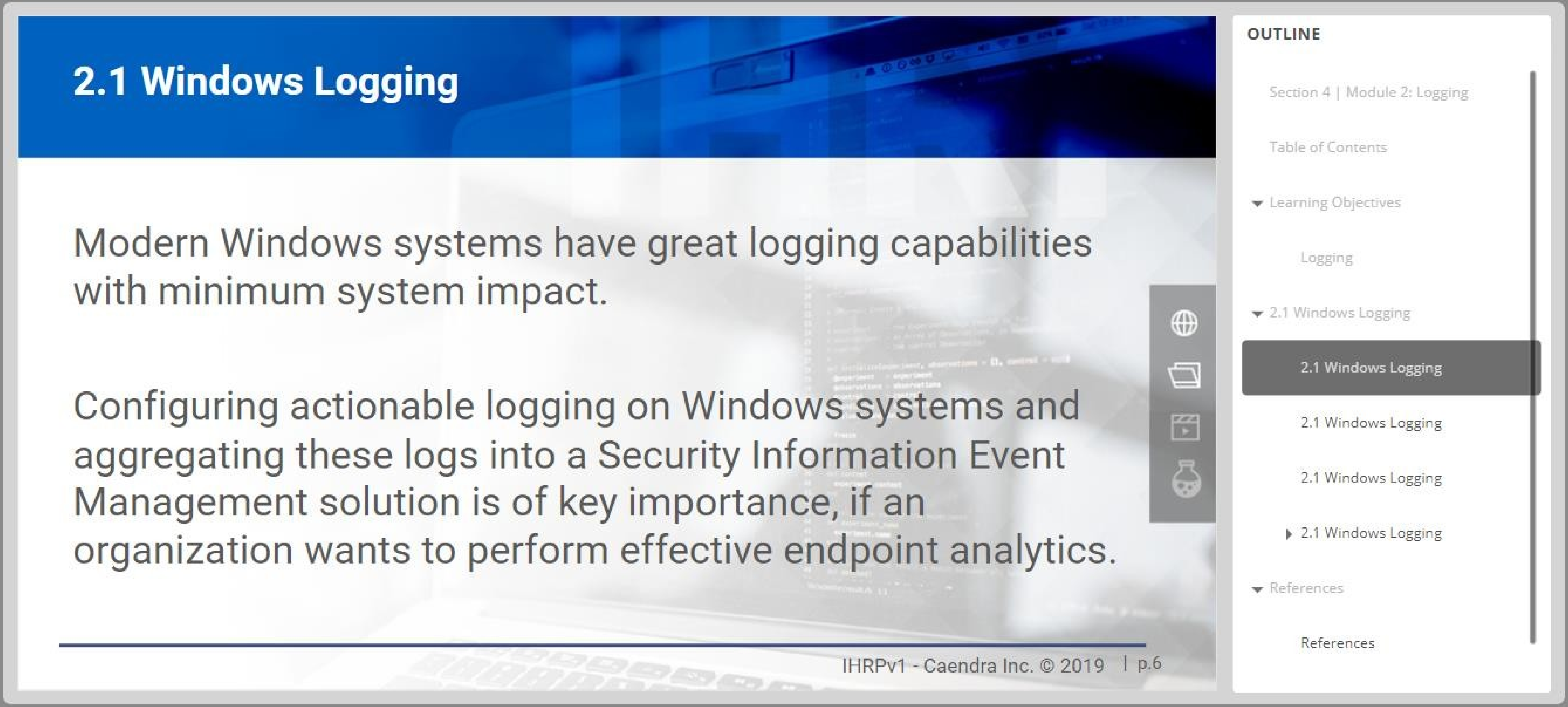
Logging

As you can imagine, there will be no endpoint analytics without logs to query.

We will dedicate this module to talk about Windows logs as well as logging strategies.

2.1

Windows Logging

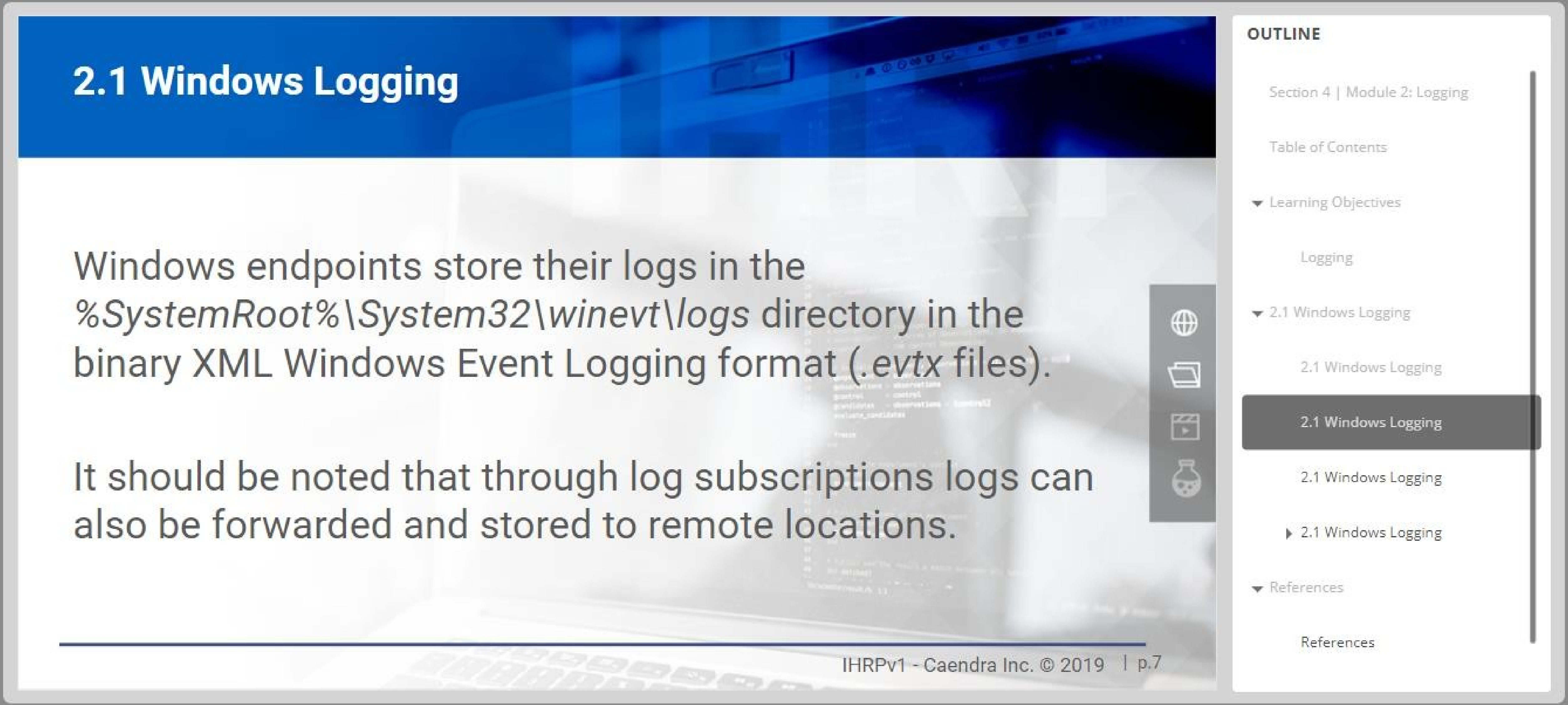


2.1 Windows Logging

Modern Windows systems have great logging capabilities with minimum system impact.

Configuring actionable logging on Windows systems and aggregating these logs into a Security Information Event Management solution is of key importance, if an organization wants to perform effective endpoint analytics.

OUTLINE

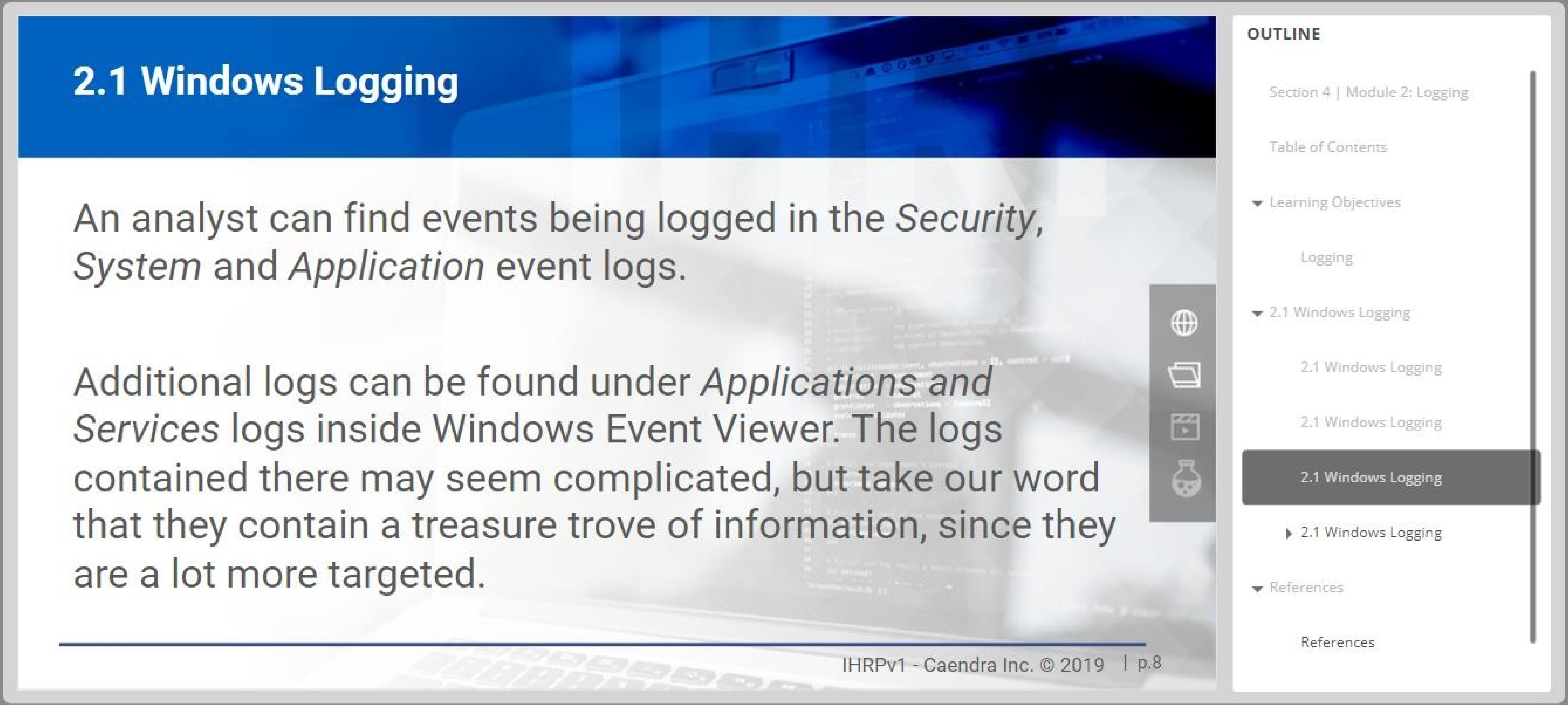


2.1 Windows Logging

Windows endpoints store their logs in the *%SystemRoot%\System32\winevt\logs* directory in the binary XML Windows Event Logging format (.*evtx* files).

It should be noted that through log subscriptions logs can also be forwarded and stored to remote locations.

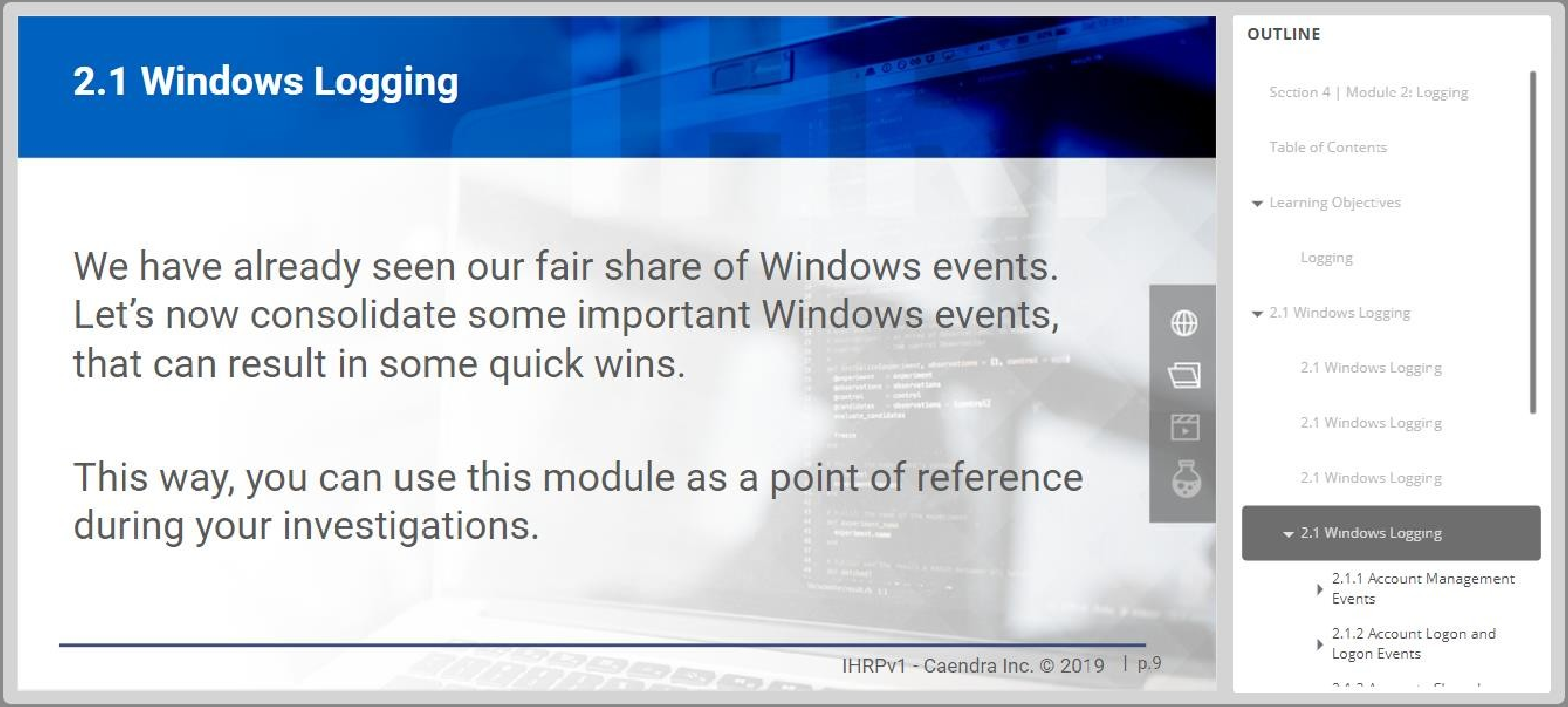
OUTLINE



2.1 Windows Logging

An analyst can find events being logged in the *Security*, *System* and *Application* event logs.

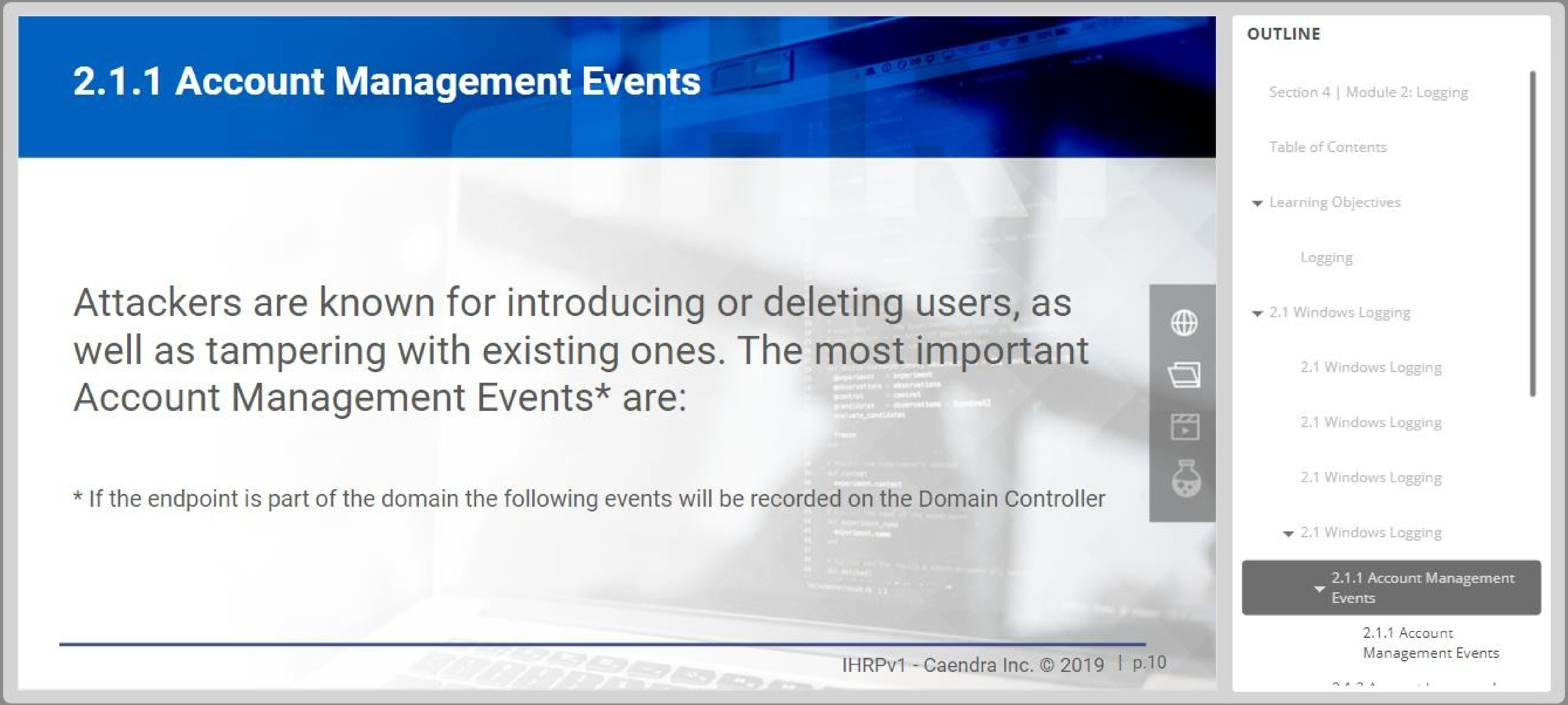
Additional logs can be found under *Applications and Services* logs inside Windows Event Viewer. The logs contained there may seem complicated, but take our word that they contain a treasure trove of information, since they are a lot more targeted.



2.1 Windows Logging

We have already seen our fair share of Windows events. Let’s now consolidate some important Windows events, that can result in some quick wins.

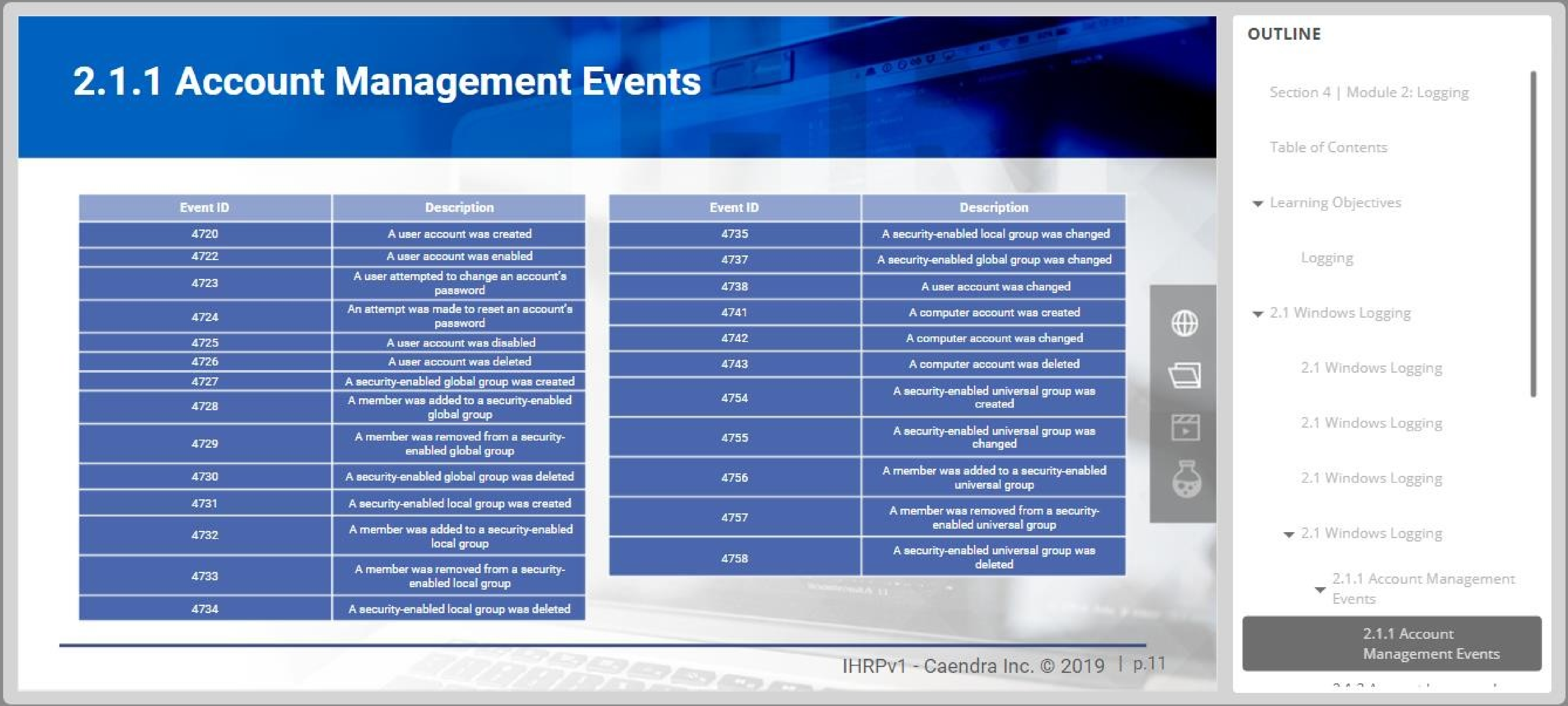
This way, you can use this module as a point of reference during your investigations.



2.1.1 Account Management Events

Attackers are known for introducing or deleting users, as well as tampering with existing ones. The most important Account Management Events* are:

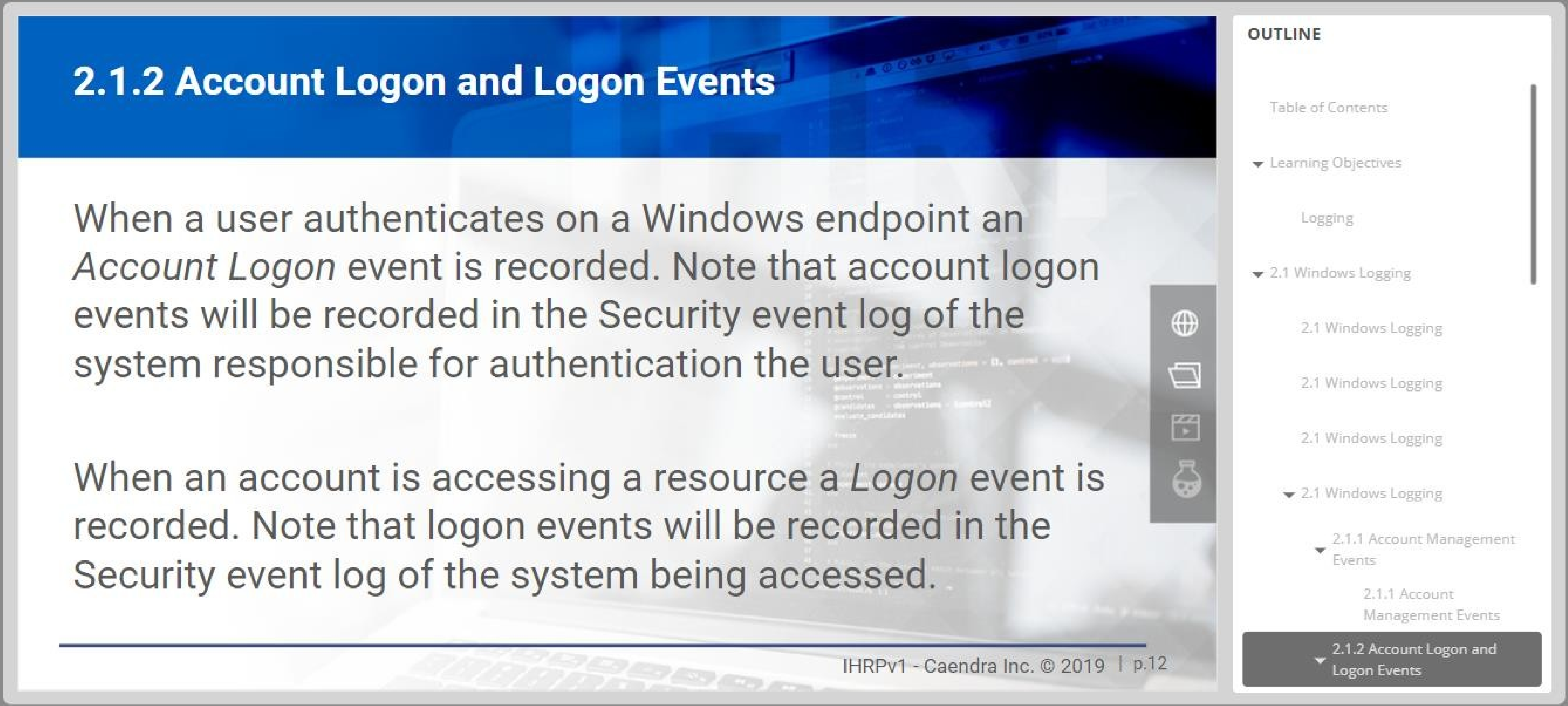
* If the endpoint is part of the domain the following events will be recorded on the Domain Controller



2.1.1 Account Management Events

Event ID	Description
4720	A user account was created
4722	A user account was enabled
4723	A user attempted to change an account's password
4724	An attempt was made to reset an account's password
4725	A user account was disabled
4726	A user account was deleted
4727	A security-enabled global group was created
4728	A member was added to a security-enabled global group
4729	A member was removed from a security-enabled global group
4730	A security-enabled global group was deleted
4731	A security-enabled local group was created
4732	A member was added to a security-enabled local group
4733	A member was removed from a security-enabled local group
4734	A security-enabled local group was deleted
4735	A security-enabled local group was changed
4737	A security-enabled global group was changed
4738	A user account was changed
4741	A computer account was created
4742	A computer account was changed
4743	A computer account was deleted
4754	A security-enabled universal group was created
4755	A security-enabled universal group was changed
4756	A member was added to a security-enabled universal group
4757	A member was removed from a security-enabled universal group
4758	A security-enabled universal group was deleted

OUTLINE

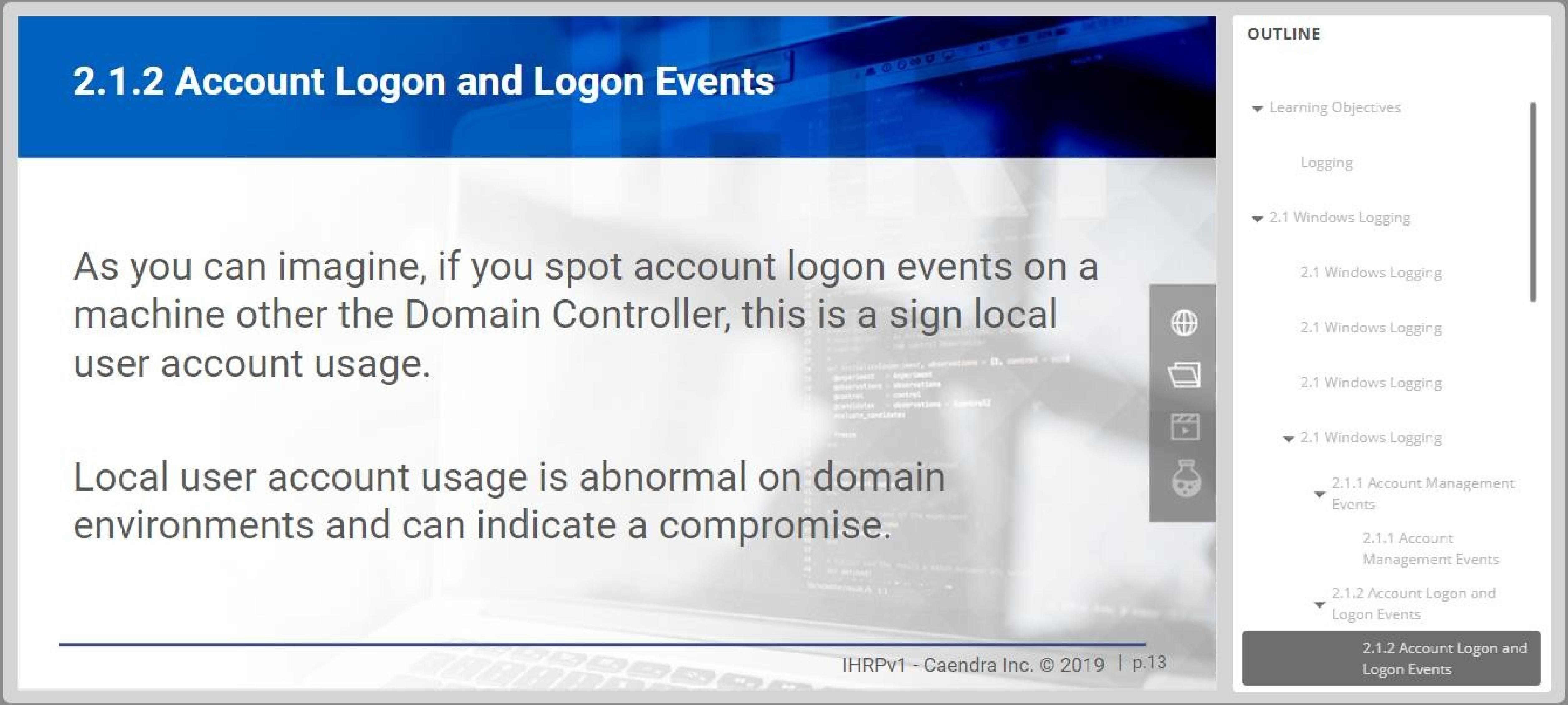


2.1.2 Account Logon and Logon Events

When a user authenticates on a Windows endpoint an *Account Logon* event is recorded. Note that account logon events will be recorded in the Security event log of the system responsible for authentication the user.

When an account is accessing a resource a *Logon* event is recorded. Note that logon events will be recorded in the Security event log of the system being accessed.

OUTLINE

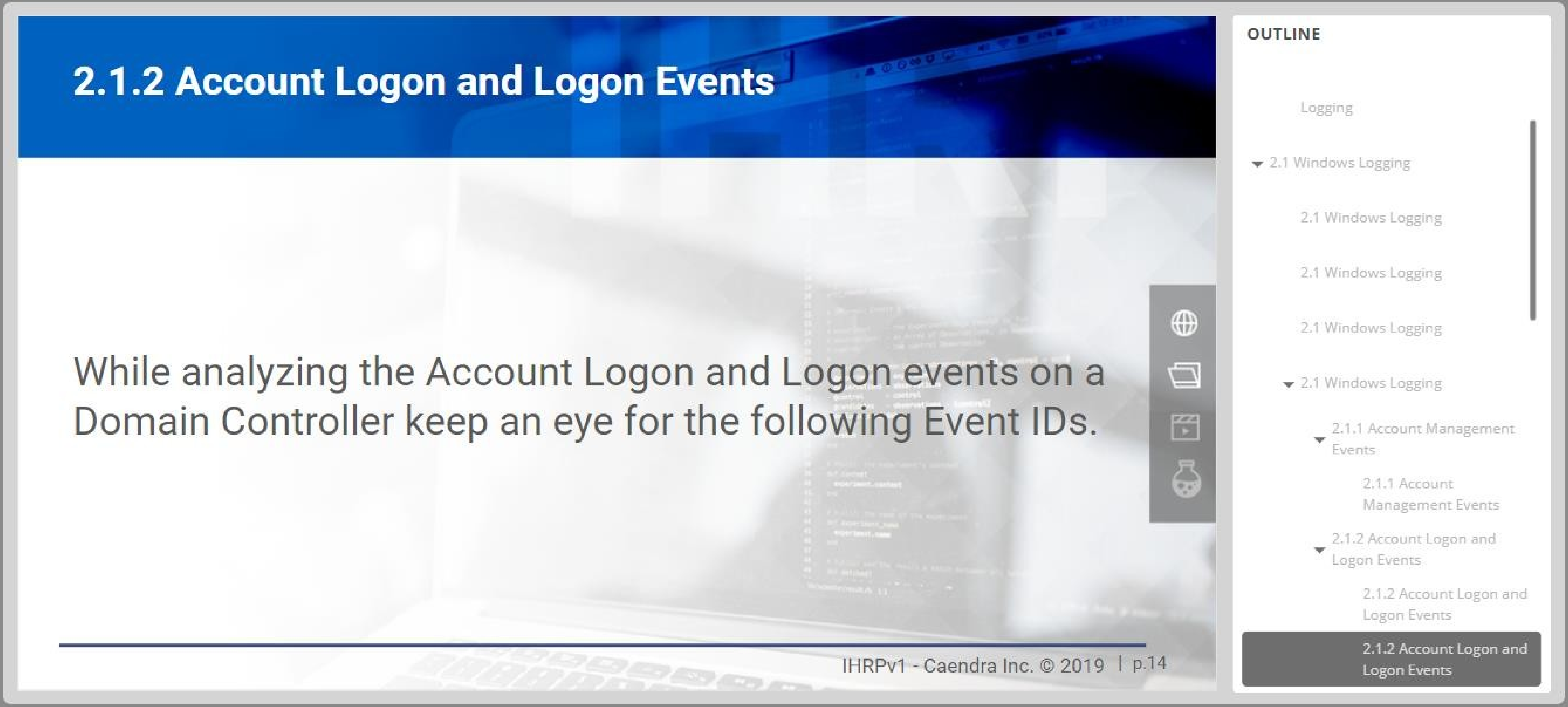


OUTLINE
Learning Objectives
Logging
2.1 Windows Logging
2.1 Windows Logging
2.1 Windows Logging
2.1 Windows Logging
2.1 Windows Logging
2.1.1 Account Management Events
2.1.1 Account Management Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

As you can imagine, if you spot account logon events on a machine other the Domain Controller, this is a sign local user account usage.

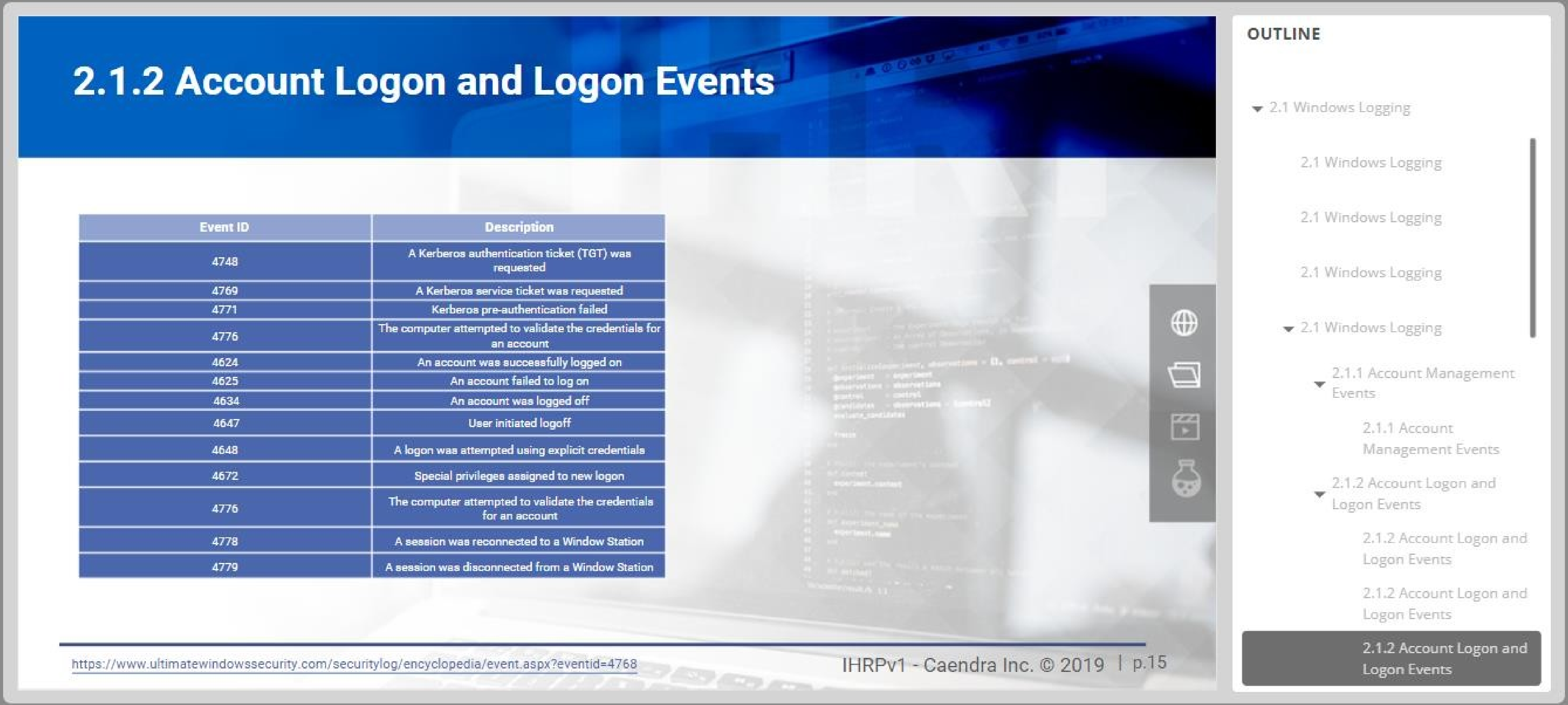
Local user account usage is abnormal on domain environments and can indicate a compromise.



2.1.2 Account Logon and Logon Events

While analyzing the Account Logon and Logon events on a Domain Controller keep an eye for the following Event IDs.

OUTLINE

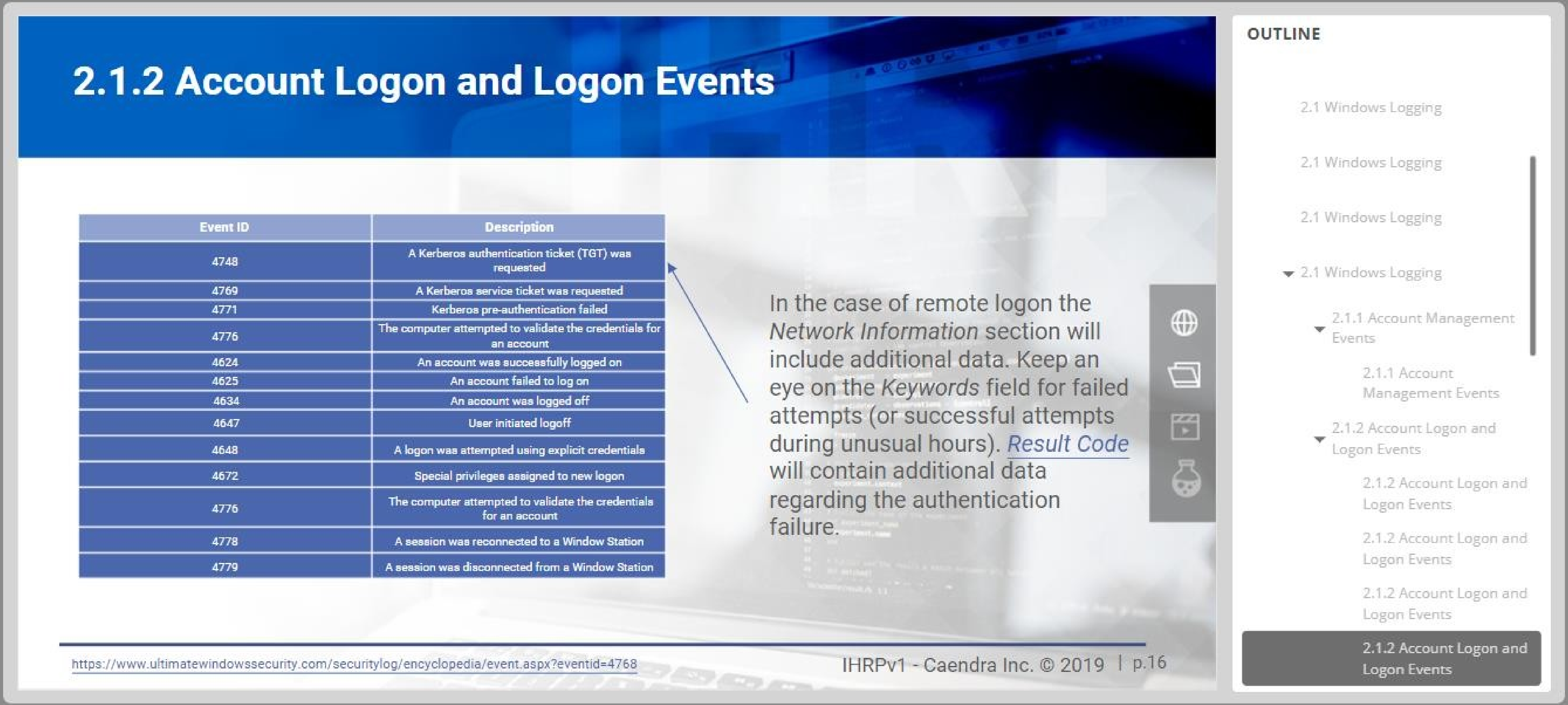


2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4768

OUTLINE
2.1 Windows Logging
2.1 Windows Logging
2.1 Windows Logging
2.1 Windows Logging
2.1 Windows Logging
2.1.1 Account Management Events
2.1.1 Account Management Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events



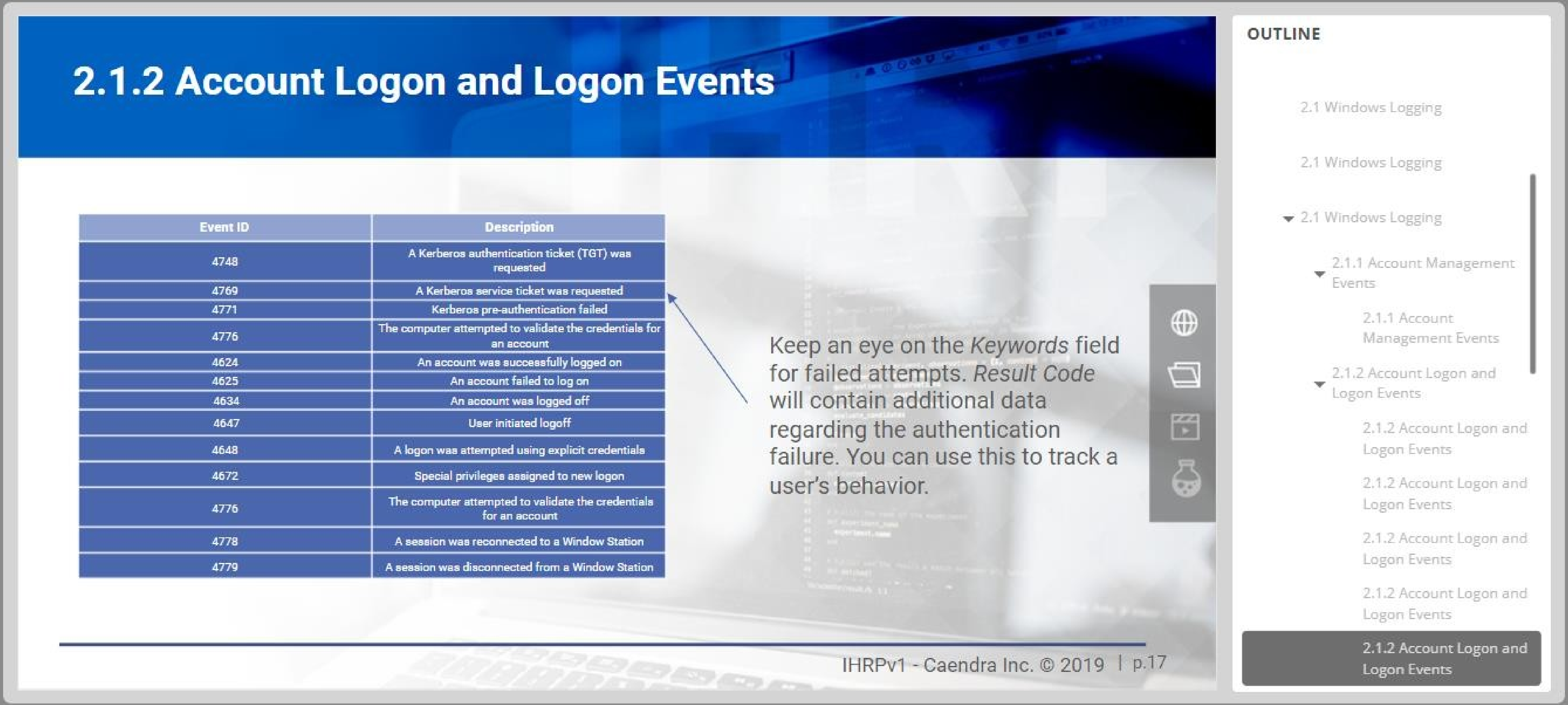
2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

In the case of remote logon the *Network Information* section will include additional data. Keep an eye on the *Keywords* field for failed attempts (or successful attempts during unusual hours). *Result Code* will contain additional data regarding the authentication failure.

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4768

OUTLINE

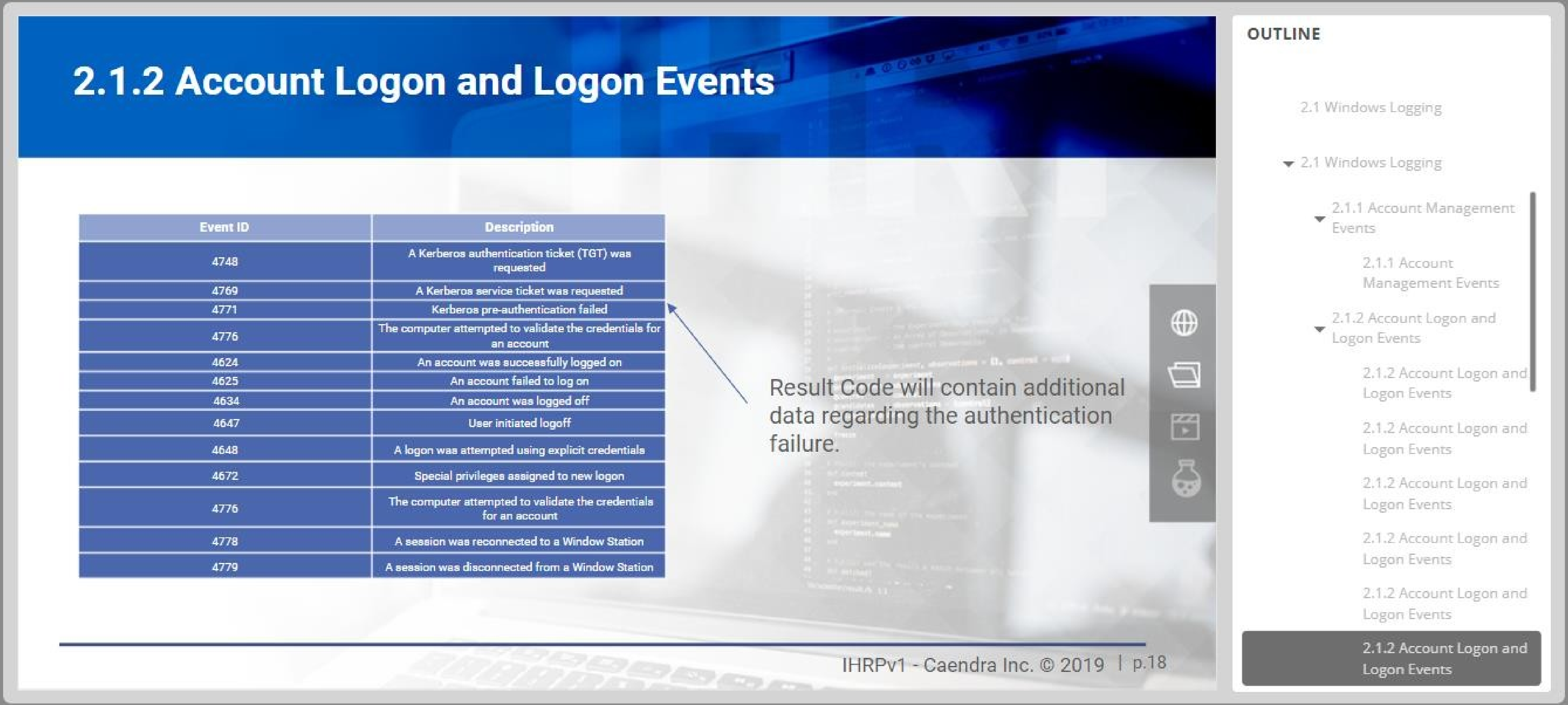


2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

Keep an eye on the *Keywords* field for failed attempts. *Result Code* will contain additional data regarding the authentication failure. You can use this to track a user's behavior.

OUTLINE

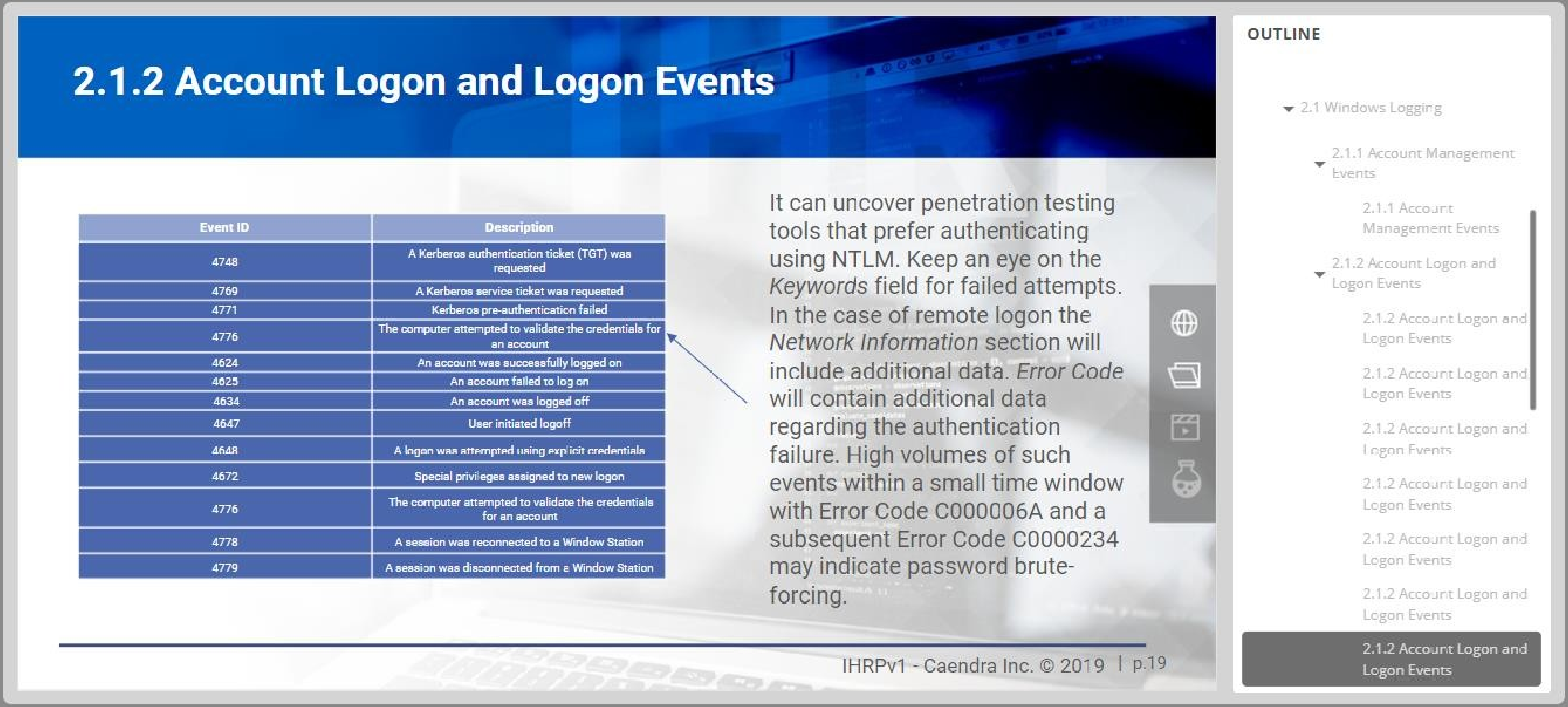


2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

Result Code will contain additional data regarding the authentication failure.

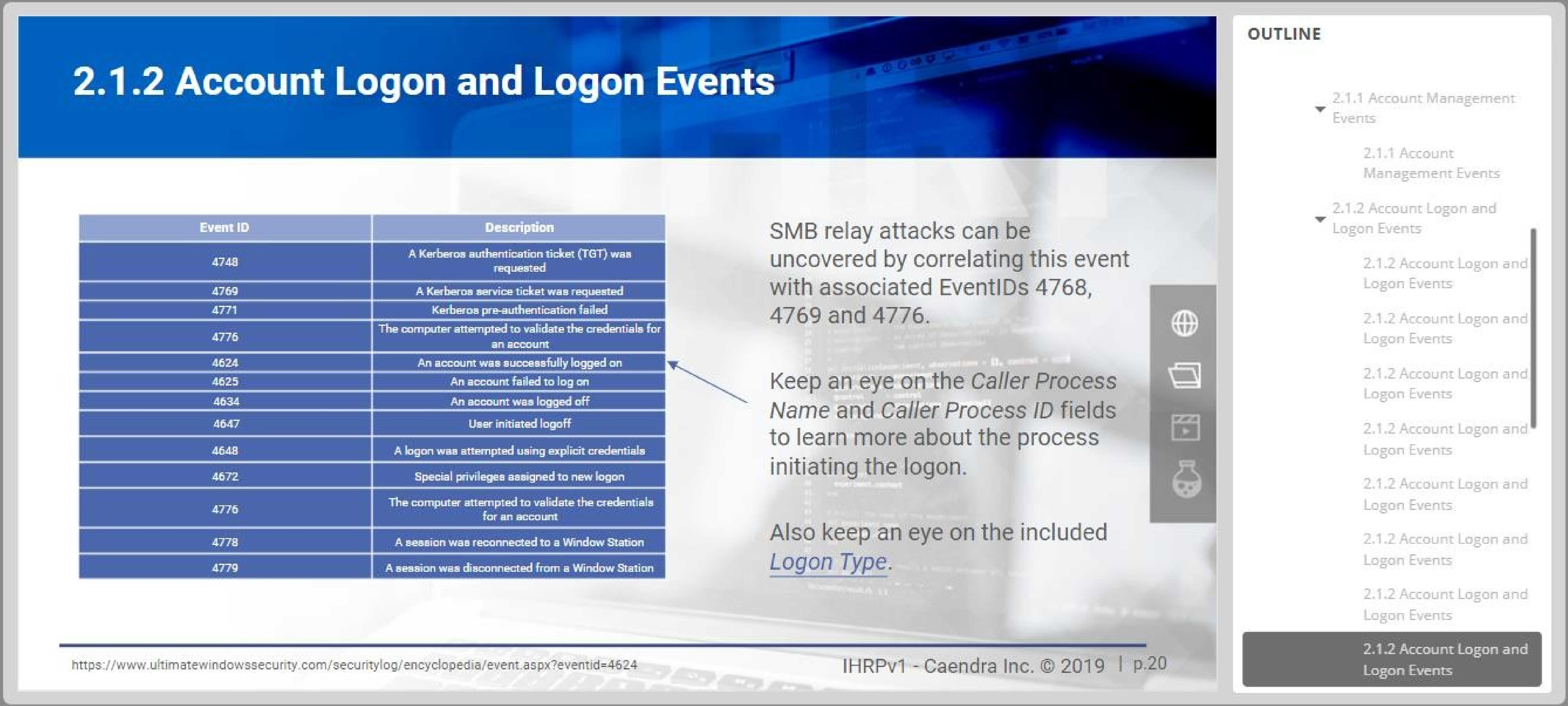
OUTLINE


OUTLINE
2.1 Windows Logging
2.1.1 Account Management Events
2.1.1 Account Management Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

It can uncover penetration testing tools that prefer authenticating using NTLM. Keep an eye on the *Keywords* field for failed attempts. In the case of remote logon the *Network Information* section will include additional data. *Error Code* will contain additional data regarding the authentication failure. High volumes of such events within a small time window with Error Code C000006A and a subsequent Error Code C0000234 may indicate password brute-forcing.



2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

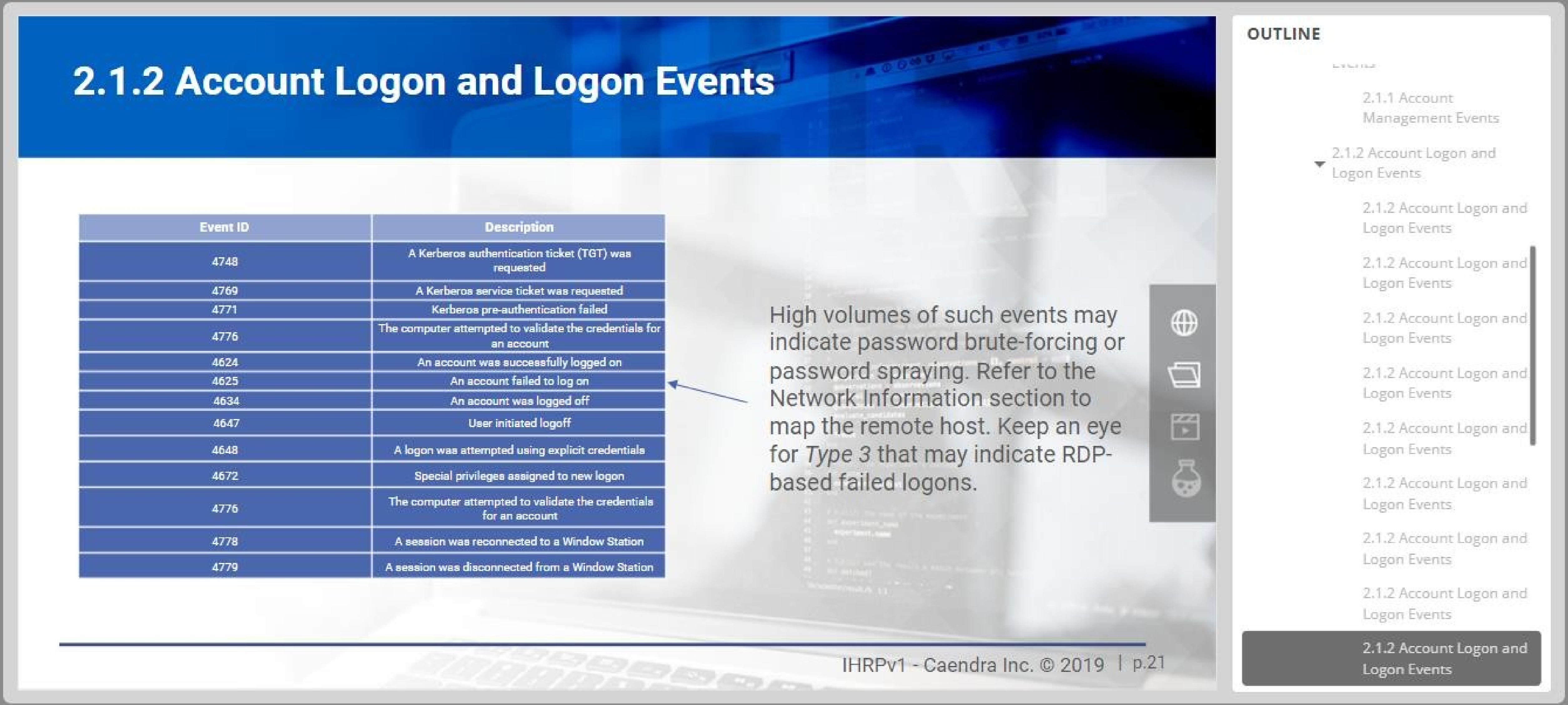
SMB relay attacks can be uncovered by correlating this event with associated EventIDs 4768, 4769 and 4776.

Keep an eye on the *Caller Process Name* and *Caller Process ID* fields to learn more about the process initiating the logon.

Also keep an eye on the included *Logon Type*.

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4624

OUTLINE

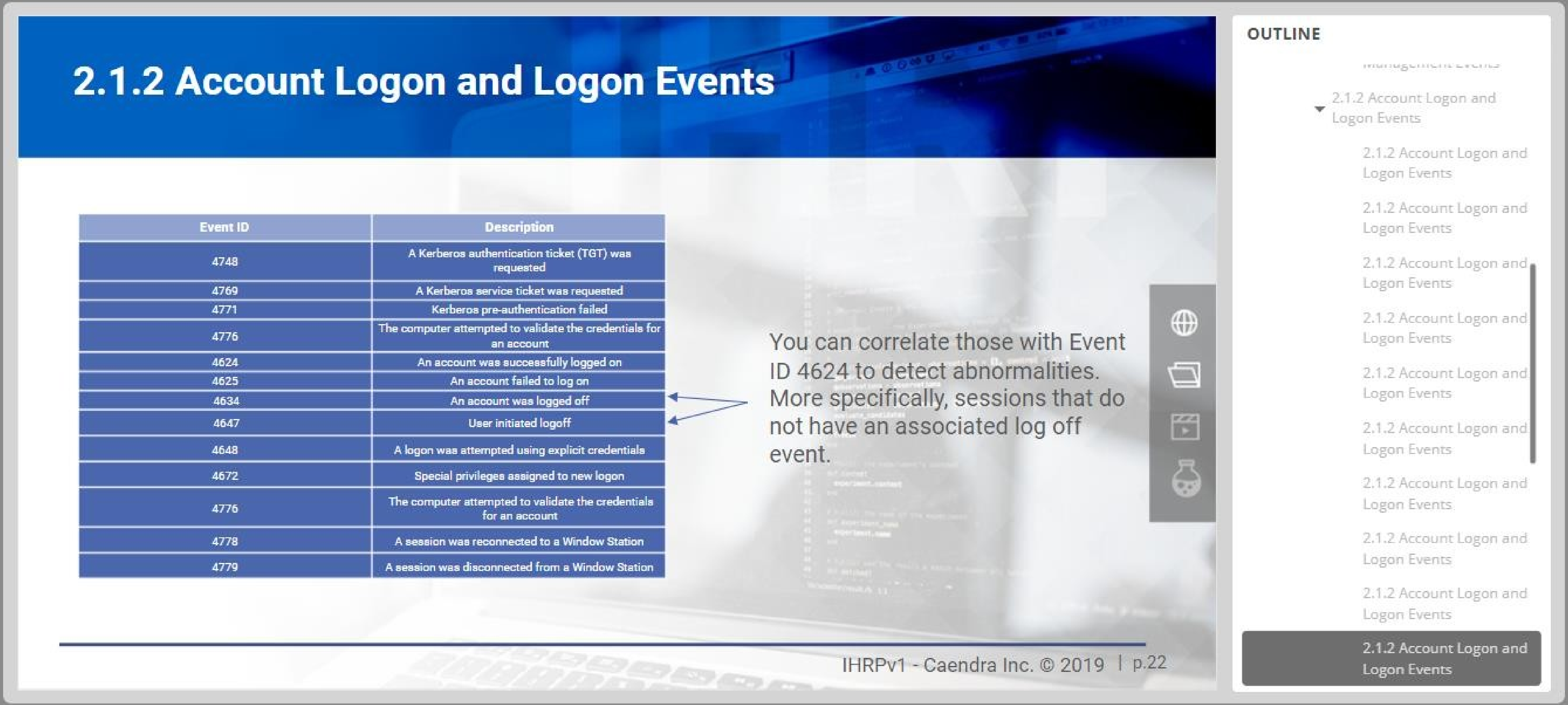


2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

High volumes of such events may indicate password brute-forcing or password spraying. Refer to the Network Information section to map the remote host. Keep an eye for *Type 3* that may indicate RDP-based failed logons.

OUTLINE

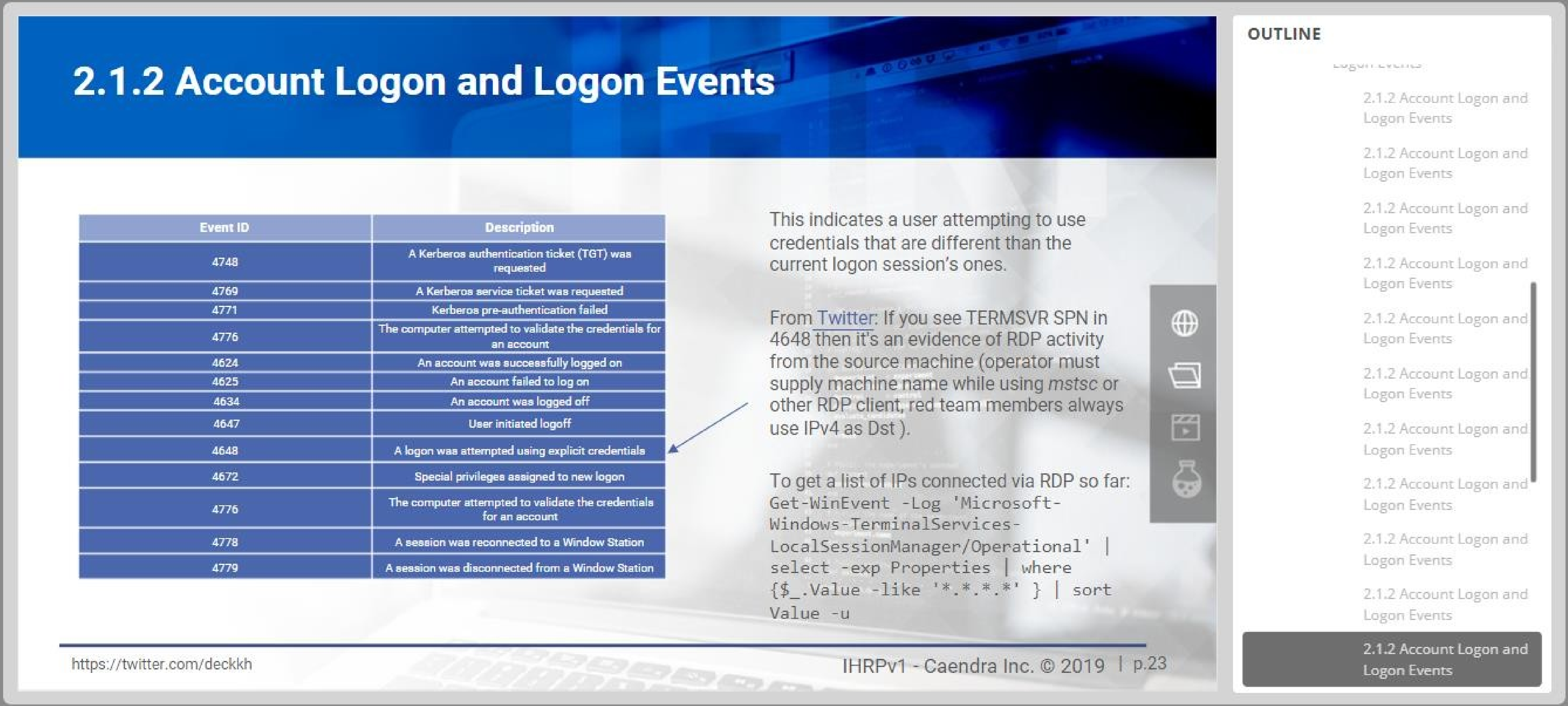


2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

You can correlate those with Event ID 4624 to detect abnormalities. More specifically, sessions that do not have an associated log off event.

OUTLINE
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events



2.1.2 Account Logon and Logon Events

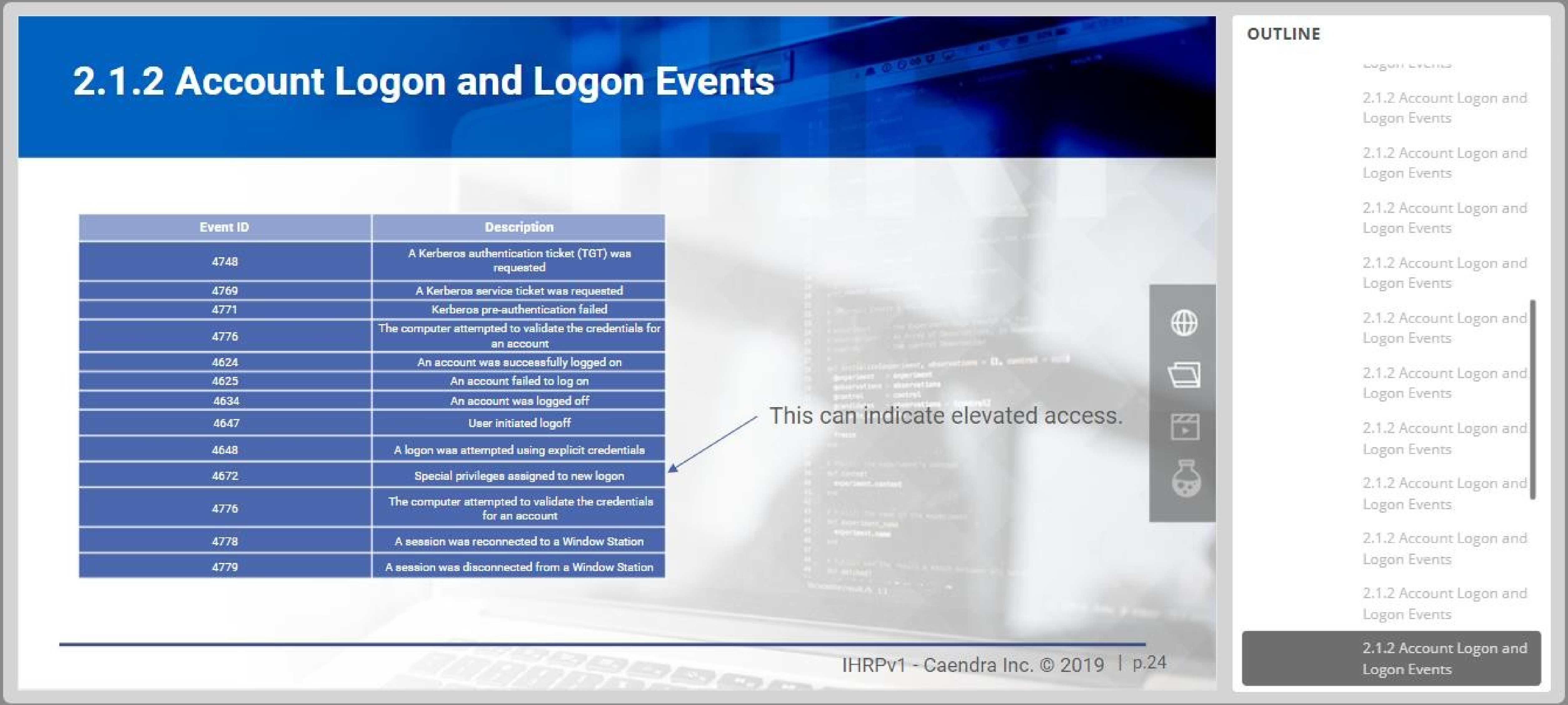
Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

This indicates a user attempting to use credentials that are different than the current logon session's ones.

From Twitter: If you see TERMSVR SPN in 4648 then it's an evidence of RDP activity from the source machine (operator must supply machine name while using *mstsc* or other RDP client, red team members always use IPv4 as Dst).

To get a list of IPs connected via RDP so far:

```
Get-WinEvent -Log 'Microsoft-
Windows-TerminalServices-
LocalSessionManager/Operational' |
select -exp Properties | where
{$_.Value -like '*.*.*.*' } | sort
Value -u
```

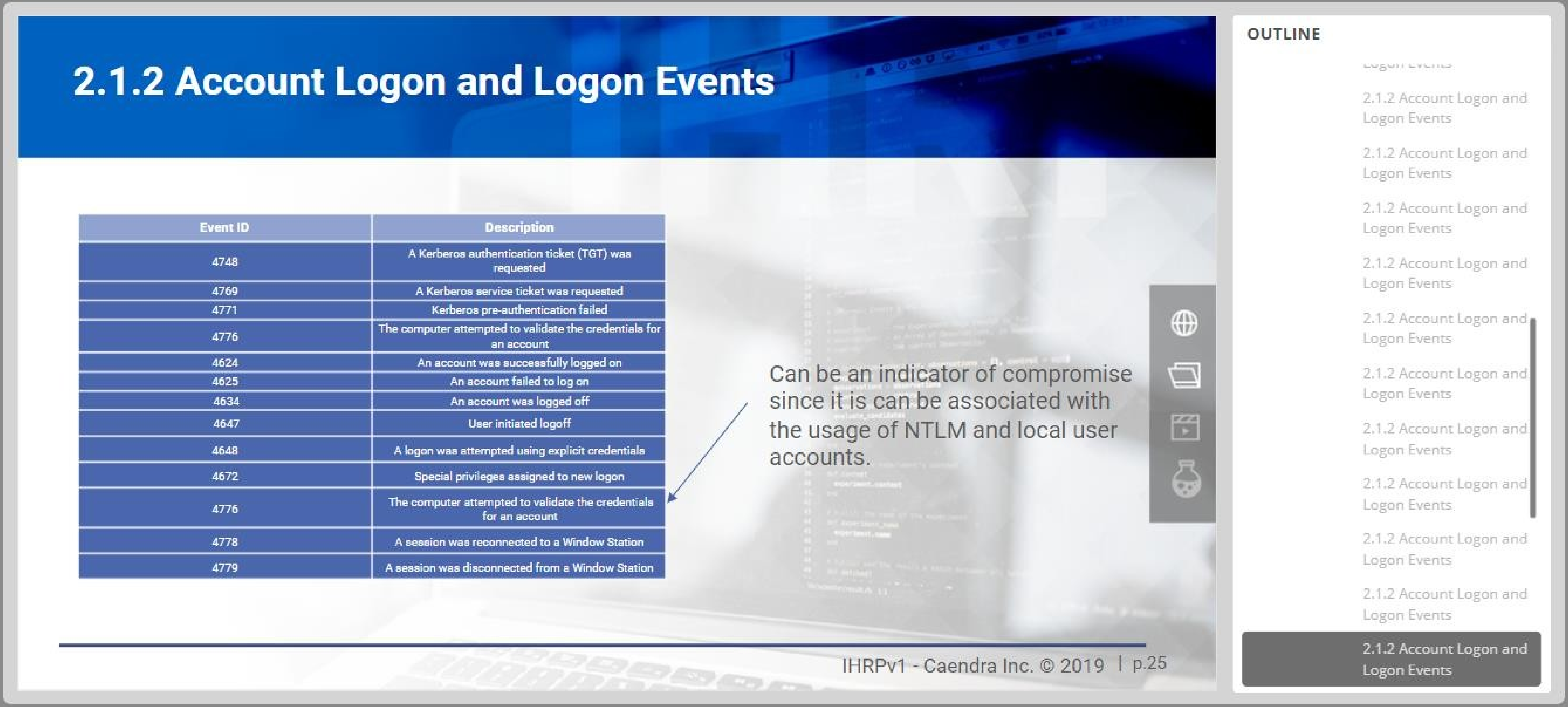


2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

This can indicate elevated access.

OUTLINE
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events

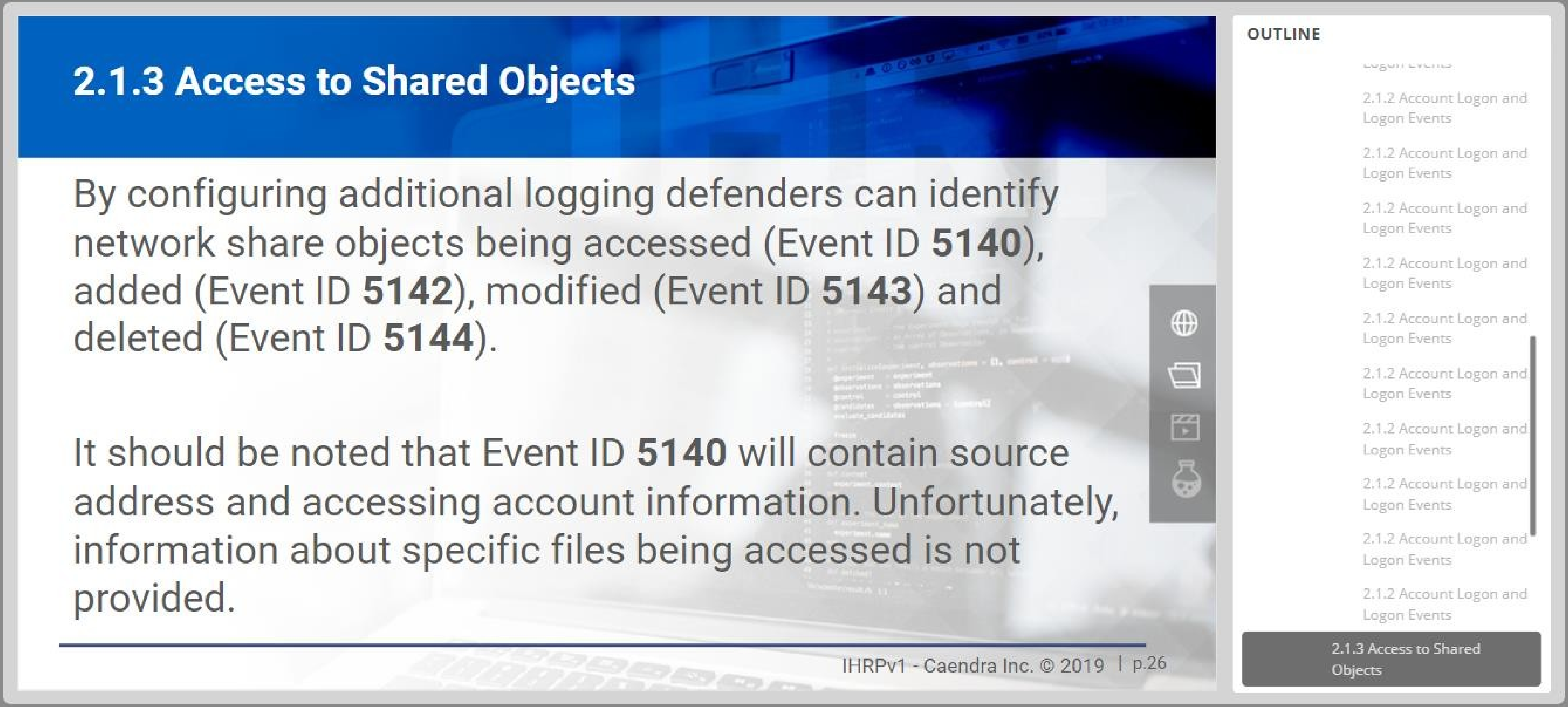


OUTLINE
Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

Can be an indicator of compromise since it is can be associated with the usage of NTLM and local user accounts.

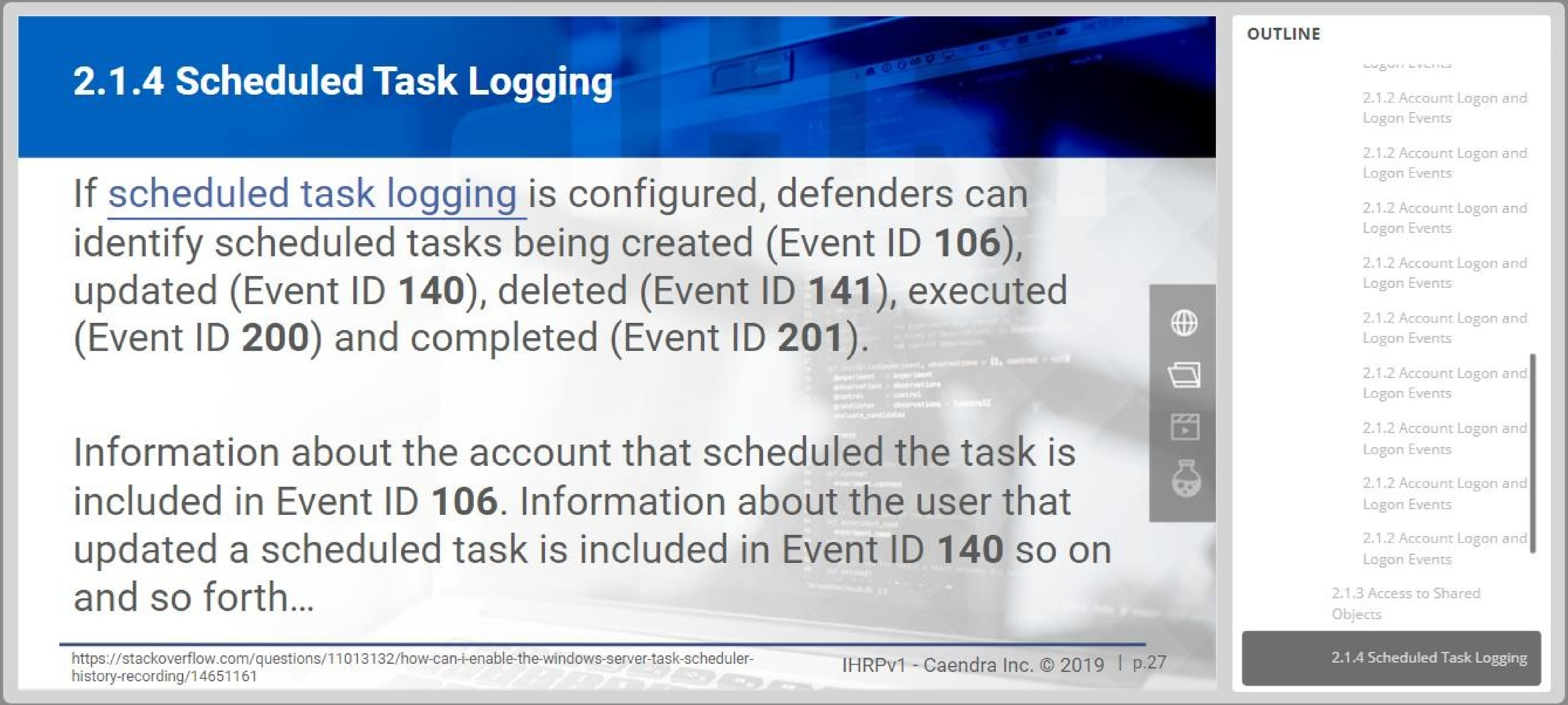


2.1.3 Access to Shared Objects

By configuring additional logging defenders can identify network share objects being accessed (Event ID **5140**), added (Event ID **5142**), modified (Event ID **5143**) and deleted (Event ID **5144**).

It should be noted that Event ID **5140** will contain source address and accessing account information. Unfortunately, information about specific files being accessed is not provided.

OUTLINE



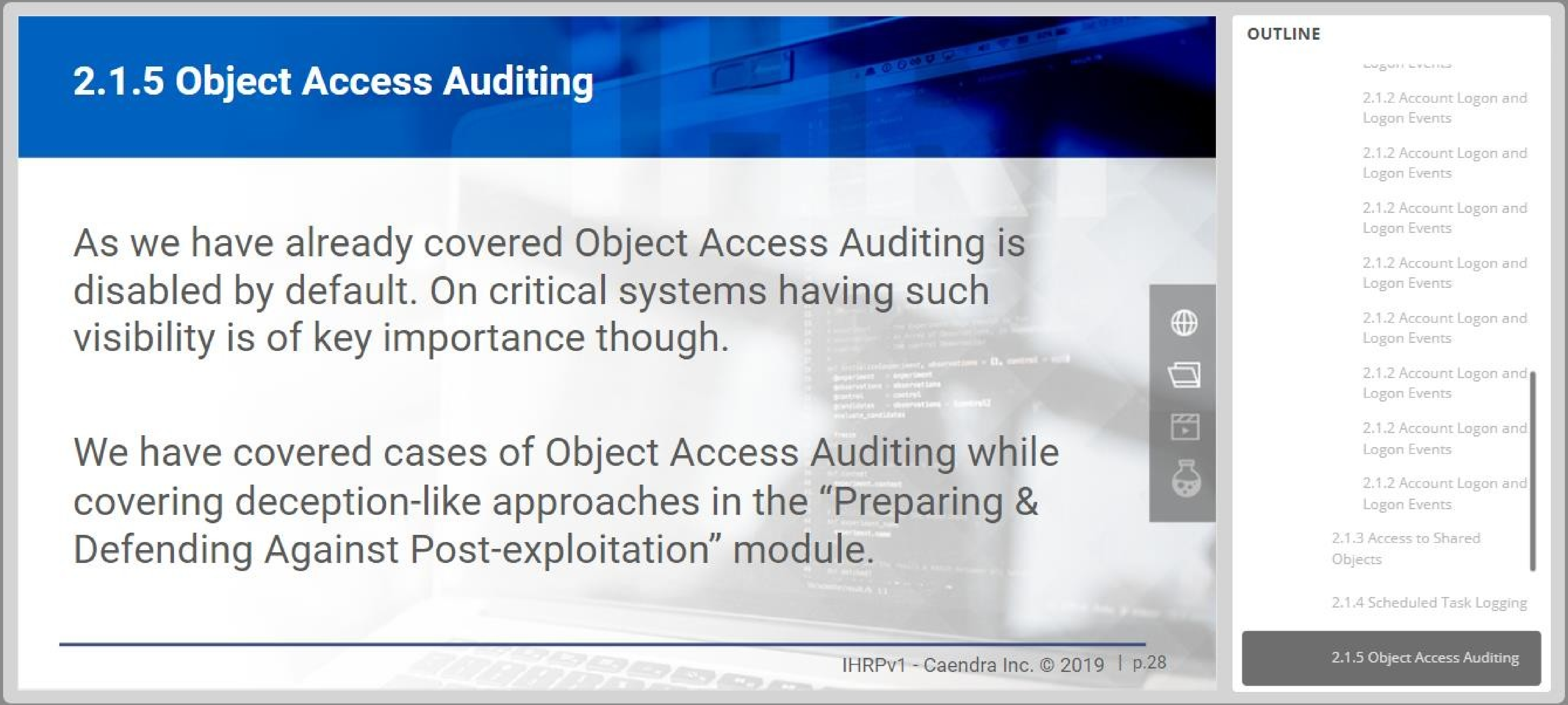
OUTLINE
Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.3 Access to Shared Objects
2.1.4 Scheduled Task Logging

2.1.4 Scheduled Task Logging

If scheduled task logging is configured, defenders can identify scheduled tasks being created (Event ID **106**), updated (Event ID **140**), deleted (Event ID **141**), executed (Event ID **200**) and completed (Event ID **201**).

Information about the account that scheduled the task is included in Event ID **106**. Information about the user that updated a scheduled task is included in Event ID **140** so on and so forth…

https://stackoverflow.com/questions/11013132/how-can-i-enable-the-windows-server-task-scheduler-history-recording/14651161

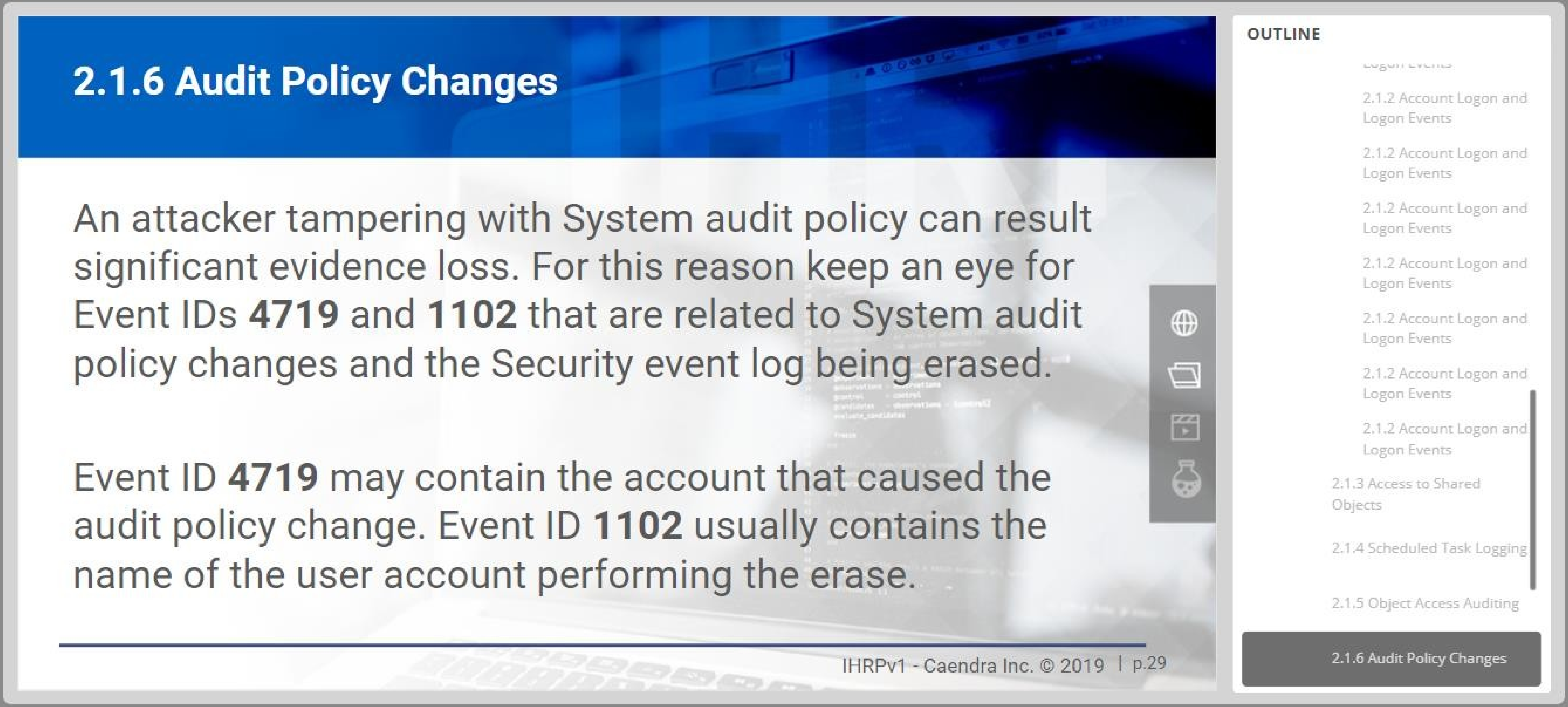


2.1.5 Object Access Auditing

As we have already covered Object Access Auditing is disabled by default. On critical systems having such visibility is of key importance though.

We have covered cases of Object Access Auditing while covering deception-like approaches in the “Preparing & Defending Against Post-exploitation” module.

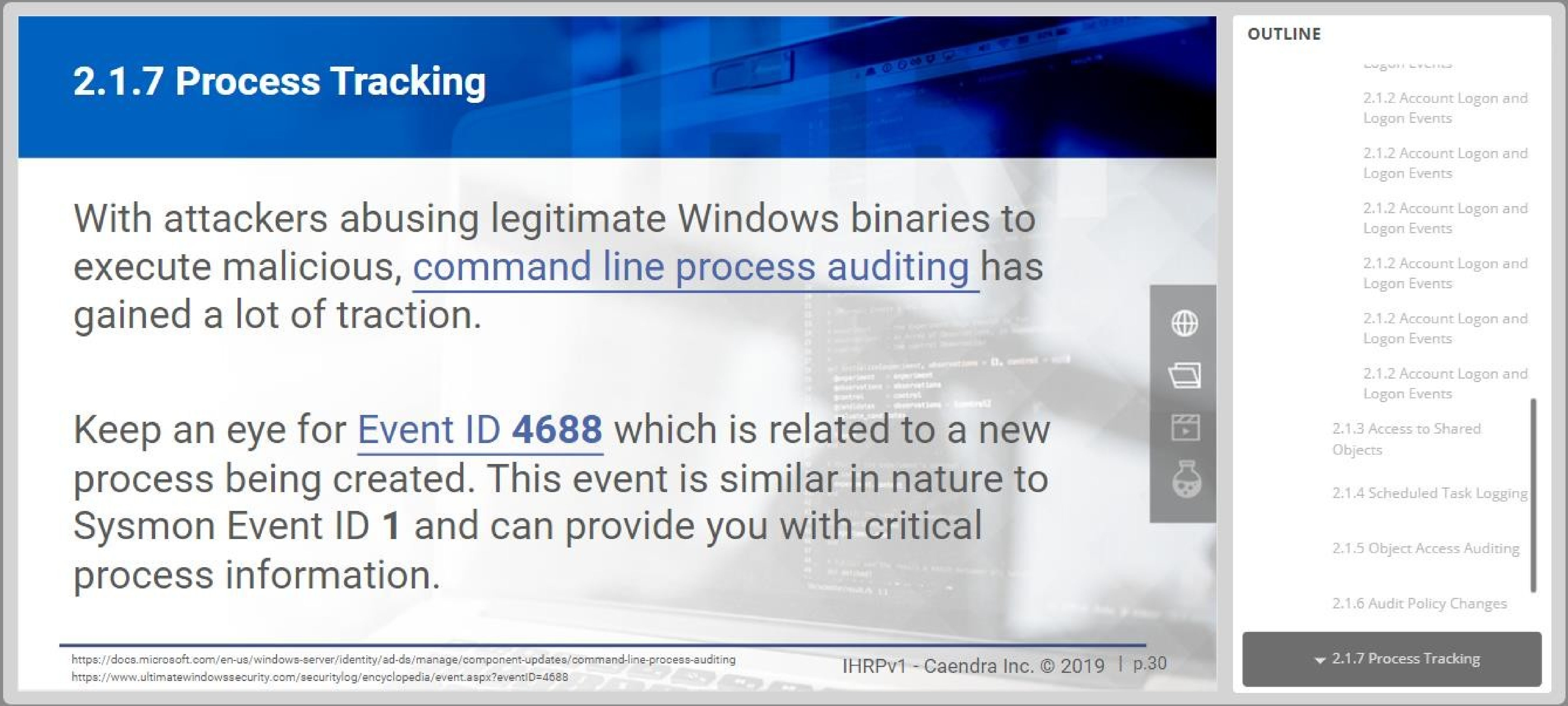
OUTLINE



2.1.6 Audit Policy Changes

An attacker tampering with System audit policy can result significant evidence loss. For this reason keep an eye for Event IDs **4719** and **1102** that are related to System audit policy changes and the Security event log being erased.

Event ID **4719** may contain the account that caused the audit policy change. Event ID **1102** usually contains the name of the user account performing the erase.

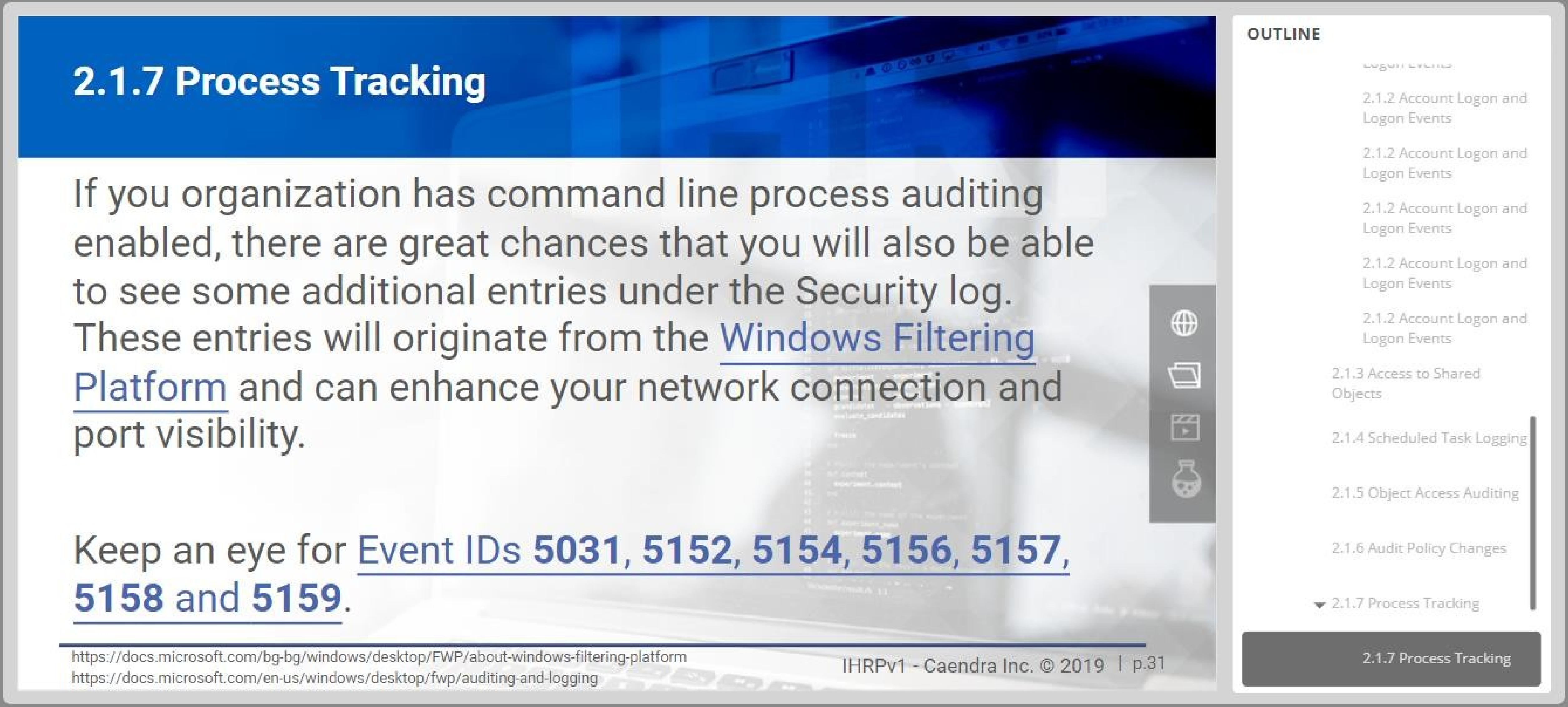


2.1.7 Process Tracking

With attackers abusing legitimate Windows binaries to execute malicious, command line process auditing has gained a lot of traction.

Keep an eye for Event ID **4688** which is related to a new process being created. This event is similar in nature to Sysmon Event ID **1** and can provide you with critical process information.

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4688



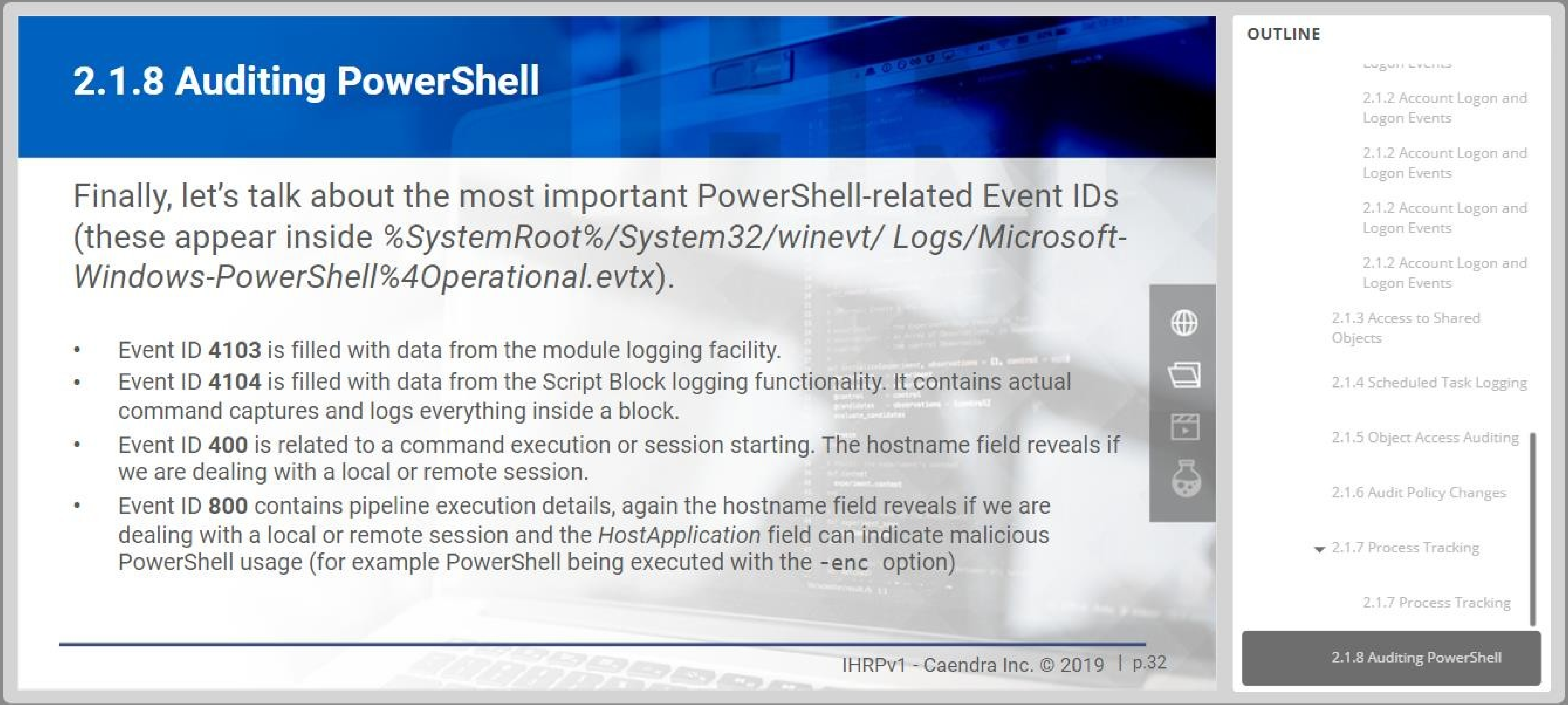
2.1.7 Process Tracking

If you organization has command line process auditing enabled, there are great chances that you will also be able to see some additional entries under the Security log. These entries will originate from the Windows Filtering Platform and can enhance your network connection and port visibility.

Keep an eye for Event IDs **5031**, **5152**, **5154**, **5156**, **5157**, **5158** and **5159**.

https://docs.microsoft.com/bg-bg/windows/desktop/FWP/about-windows-filtering-platform
https://docs.microsoft.com/en-us/windows/desktop/fwp/auditing-and-logging

OUTLINE

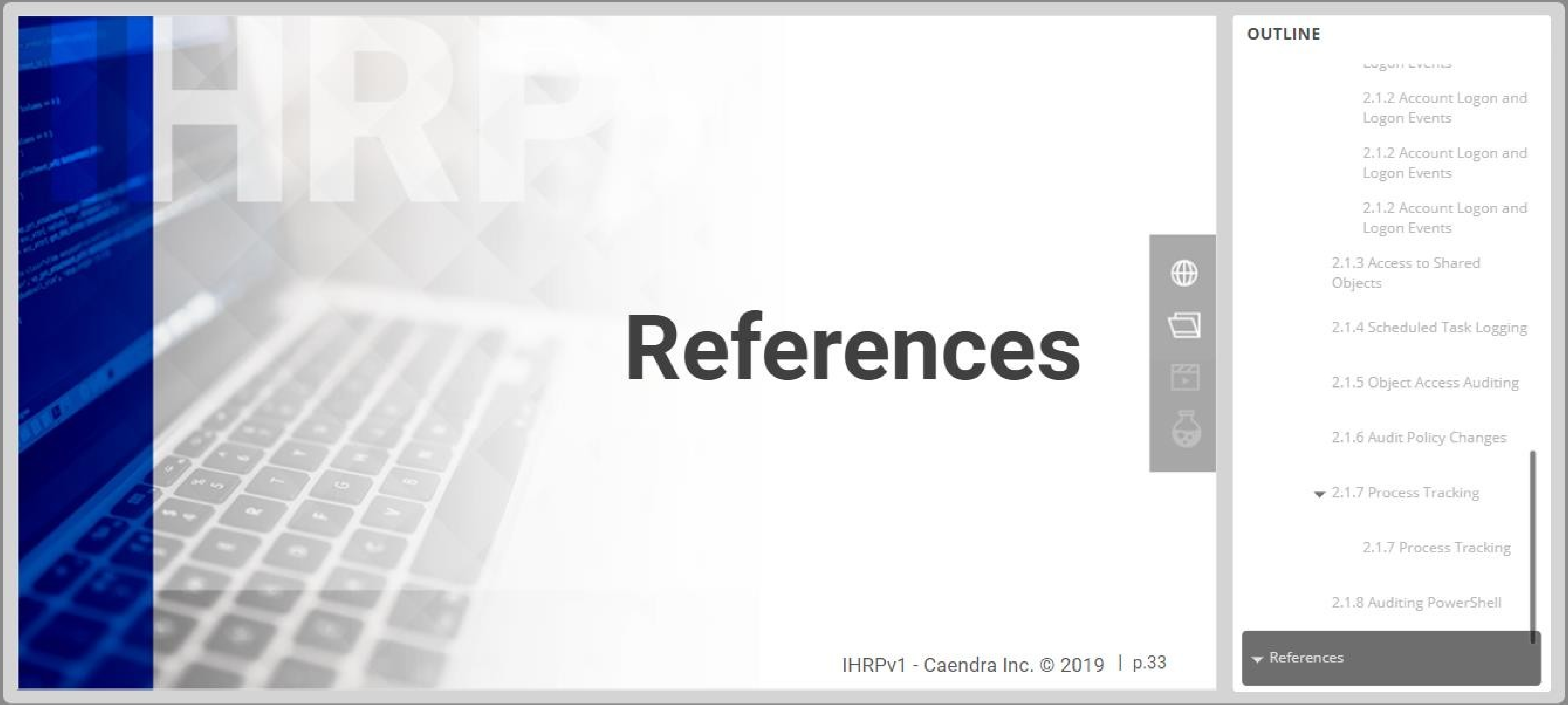


2.1.8 Auditing PowerShell

Finally, let’s talk about the most important PowerShell-related Event IDs (these appear inside *%SystemRoot%/System32/winevt/ Logs/Microsoft-Windows-PowerShell%4Operational.evtx*).

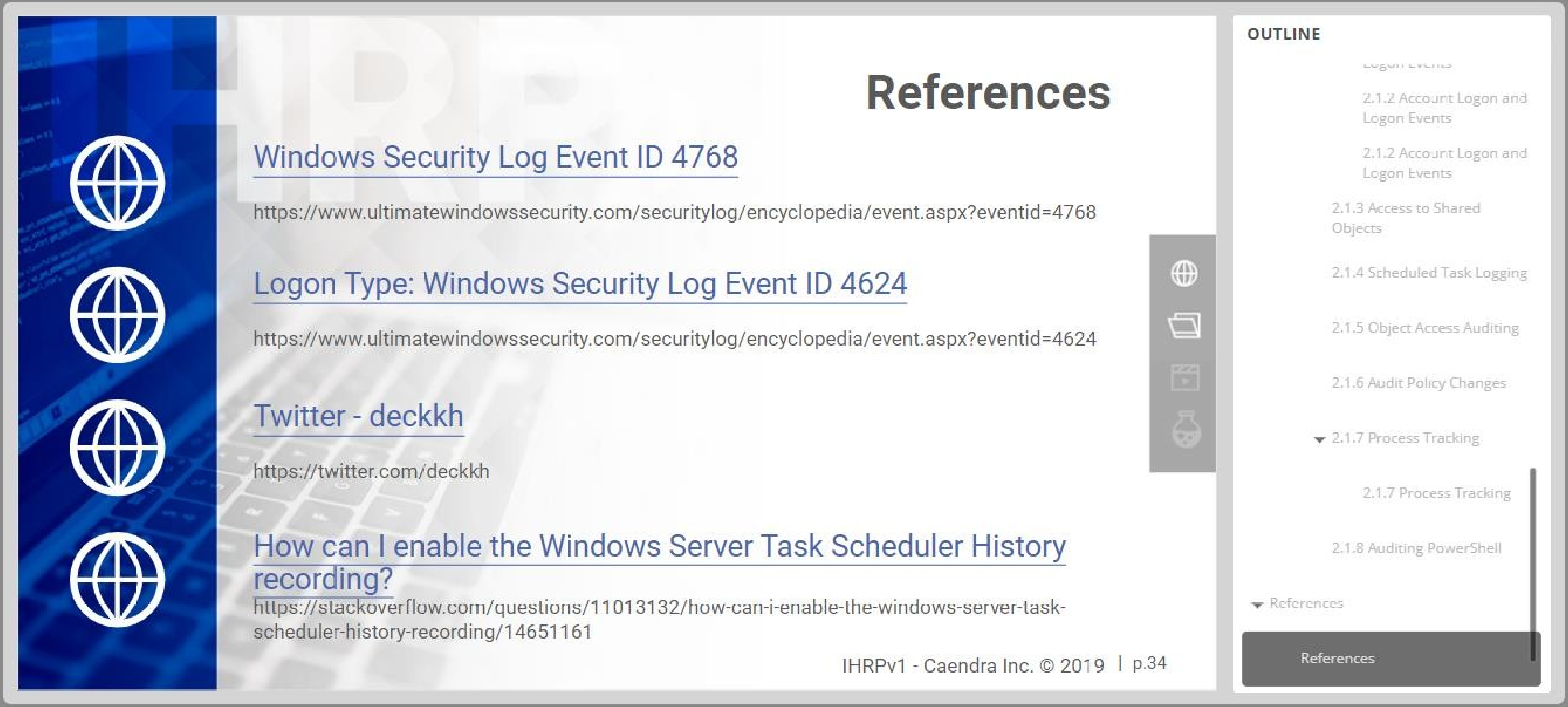
- Event ID **4103** is filled with data from the module logging facility.
- Event ID **4104** is filled with data from the Script Block logging functionality. It contains actual command captures and logs everything inside a block.
- Event ID **400** is related to a command execution or session starting. The hostname field reveals if we are dealing with a local or remote session.
- Event ID **800** contains pipeline execution details, again the hostname field reveals if we are dealing with a local or remote session and the *HostApplication* field can indicate malicious PowerShell usage (for example PowerShell being executed with the `-enc` option)

OUTLINE



References

OUTLINE



OUTLINE
Logon Events
2.1.2 Account Logon and Logon Events
2.1.2 Account Logon and Logon Events
2.1.3 Access to Shared Objects
2.1.4 Scheduled Task Logging
2.1.5 Object Access Auditing
2.1.6 Audit Policy Changes
2.1.7 Process Tracking
2.1.7 Process Tracking
2.1.8 Auditing PowerShell
References
References

References

Windows Security Log Event ID 4768

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4768

Logon Type: Windows Security Log Event ID 4624

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4624

Twitter - deckkh

https://twitter.com/deckkh

How can I enable the Windows Server Task Scheduler History recording?

https://stackoverflow.com/questions/11013132/how-can-i-enable-the-windows-server-task-scheduler-history-recording/14651161

References

command line process auditing

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing

Windows Security Log Event ID 4688

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4688

Windows Filtering Platform

https://docs.microsoft.com/bg-bg/windows/desktop/FWP/about-windows-filtering-platform

Event IDs **5031**, **5152**, **5154**, **5156**, **5157**, **5158** and **5159**

https://docs.microsoft.com/en-us/windows/desktop/fwp/auditing-and-logging

OUTLINE

Logon Events

2.1.2 Account Logon and Logon Events

2.1.3 Access to Shared Objects

2.1.4 Scheduled Task Logging

2.1.5 Object Access Auditing

2.1.6 Audit Policy Changes

2.1.7 Process Tracking

2.1.7 Process Tracking

2.1.8 Auditing PowerShell

References

References

References