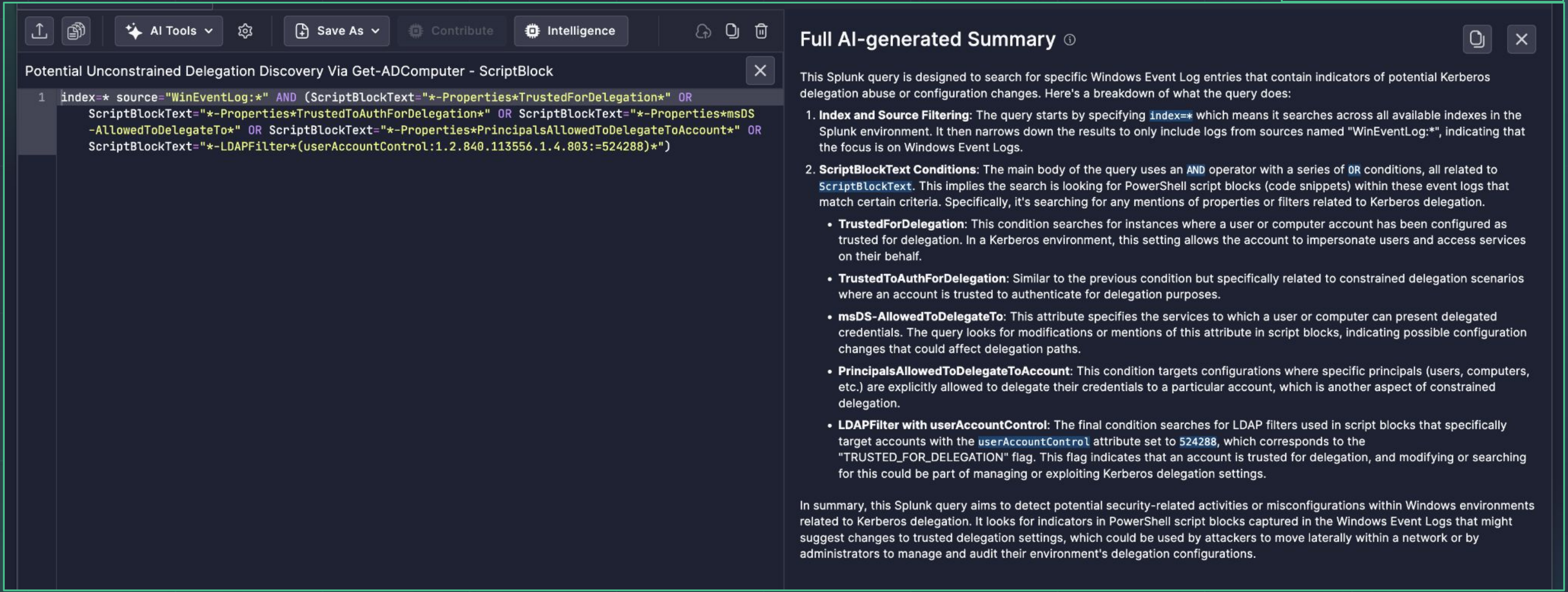
Rule/Query Full Summary with AI

Uncoder AI

Rule/Query Full Summary with AI

In production



Potential Unconstrained Delegation Discovery Via Get-ADComputer - ScriptBlock

```
index=* source="WinEventLog:*" AND (ScriptBlockText="*-Properties*TrustedForDelegation*" OR
    ScriptBlockText="*-Properties*TrustedToAuthForDelegation*" OR ScriptBlockText="*-Properties*msDS
    -AllowedToDelegateTo*" OR ScriptBlockText="*-Properties*PrincipalsAllowedToDelegateToAccount*" OR
    ScriptBlockText="*-LDAPFilter*(userAccountControl:1.2.840.113556.1.4.803:=524288)*")
```

Full AI-generated Summary

This Splunk query is designed to search for specific Windows Event Log entries that contain indicators of potential Kerberos delegation abuse or configuration changes. Here's a breakdown of what the query does:

1. **Index and Source Filtering**: The query starts by specifying `index=*` which means it searches across all available indexes in the Splunk environment. It then narrows down the results to only include logs from sources named "WinEventLog:*", indicating that the focus is on Windows Event Logs.
2. **ScriptBlockText Conditions**: The main body of the query uses an `AND` operator with a series of `OR` conditions, all related to `ScriptBlockText`. This implies the search is looking for PowerShell script blocks (code snippets) within these event logs that match certain criteria. Specifically, it's searching for any mentions of properties or filters related to Kerberos delegation.
    - **TrustedForDelegation**: This condition searches for instances where a user or computer account has been configured as trusted for delegation. In a Kerberos environment, this setting allows the account to impersonate users and access services on their behalf.
    - **TrustedToAuthForDelegation**: Similar to the previous condition but specifically related to constrained delegation scenarios where an account is trusted to authenticate for delegation purposes.
    - **msDS-AllowedToDelegateTo**: This attribute specifies the services to which a user or computer can present delegated credentials. The query looks for modifications or mentions of this attribute in script blocks, indicating possible configuration changes that could affect delegation paths.
    - **PrincipalsAllowedToDelegateToAccount**: This condition targets configurations where specific principals (users, computers, etc.) are explicitly allowed to delegate their credentials to a particular account, which is another aspect of constrained delegation.
    - **LDAPFilter with userAccountControl**: The final condition searches for LDAP filters used in script blocks that specifically target accounts with the `userAccountControl` attribute set to `524288`, which corresponds to the "TRUSTED_FOR_DELEGATION" flag. This flag indicates that an account is trusted for delegation, and modifying or searching for this could be part of managing or exploiting Kerberos delegation settings.

In summary, this Splunk query aims to detect potential security-related activities or misconfigurations within Windows environments related to Kerberos delegation. It looks for indicators in PowerShell script blocks captured in the Windows Event Logs that might suggest changes to trusted delegation settings, which could be used by attackers to move laterally within a network or by administrators to manage and audit their environment's delegation configurations.

Rule/Query Full Summary with AI

Modern SOC teams need to process large volumes of detection logic. Much of it is complex, verbose, and time-consuming to understand. Uncoder AI analyzes rule/query and provides you with a detailed yet clear explanation of the detection logic and all the fine points involved. For this purpose, Uncoder AI uses Llama 3.3 customized for detection engineering and threat intelligence processing, hosted at SOC Prime SOC 2 Type II private cloud for maximum security, privacy, and IP protection.

- Clear and structured summary of the detection logic in human language
- Multiple languages supported
- Data doesn't leave SOC Prime's infrastructure

Rule/Query Full Summary with AI

48 languages supported in production

ANOMALI	APACHE kafka	ArcSight	CORTEX XSIAM BY PALO ALTO NETWORKS	CORTEX XDR BY PALO ALTO NETWORKS	AWS Athena	OpenSearch	DEVO
CROWDSTRIKE	FORTINET	C# REGEX	graylog	DATADOG	DNIF	ElastAlert	Elastic Stack
HUNTERS	LOGPOINT	LogRhythm	Falco	CrowdStrike Falcon LogScale	FIREEYE	Google Security Operations	hawksearch
Radar	LACEWORK	LIMA CHARLIE	LOGIQ	Microsoft Defender for Endpoint	Microsoft Sentinel	nviso	PowerShell
Qualys	GREP	ROOTA	RSA NETWITNESS	securonix	SentinelOne	snowflake	splunk>
SQL	SQLite	STIX	StreamAlert	sumo logic	Sysmon	uberAgent	Carbon Black.