Experts Live Norway

Using Log Analytics to catch the bad guys

Marius Sandbu
Cloud Tech Lead @ EVRY
@msandbu

Experts Live Norway

Azure Sentinel

Using ~~Log Analytics~~ to catch the bad guys

Marius Sandbu
Cloud Tech Lead @ EVRY
@msandbu

Agenda

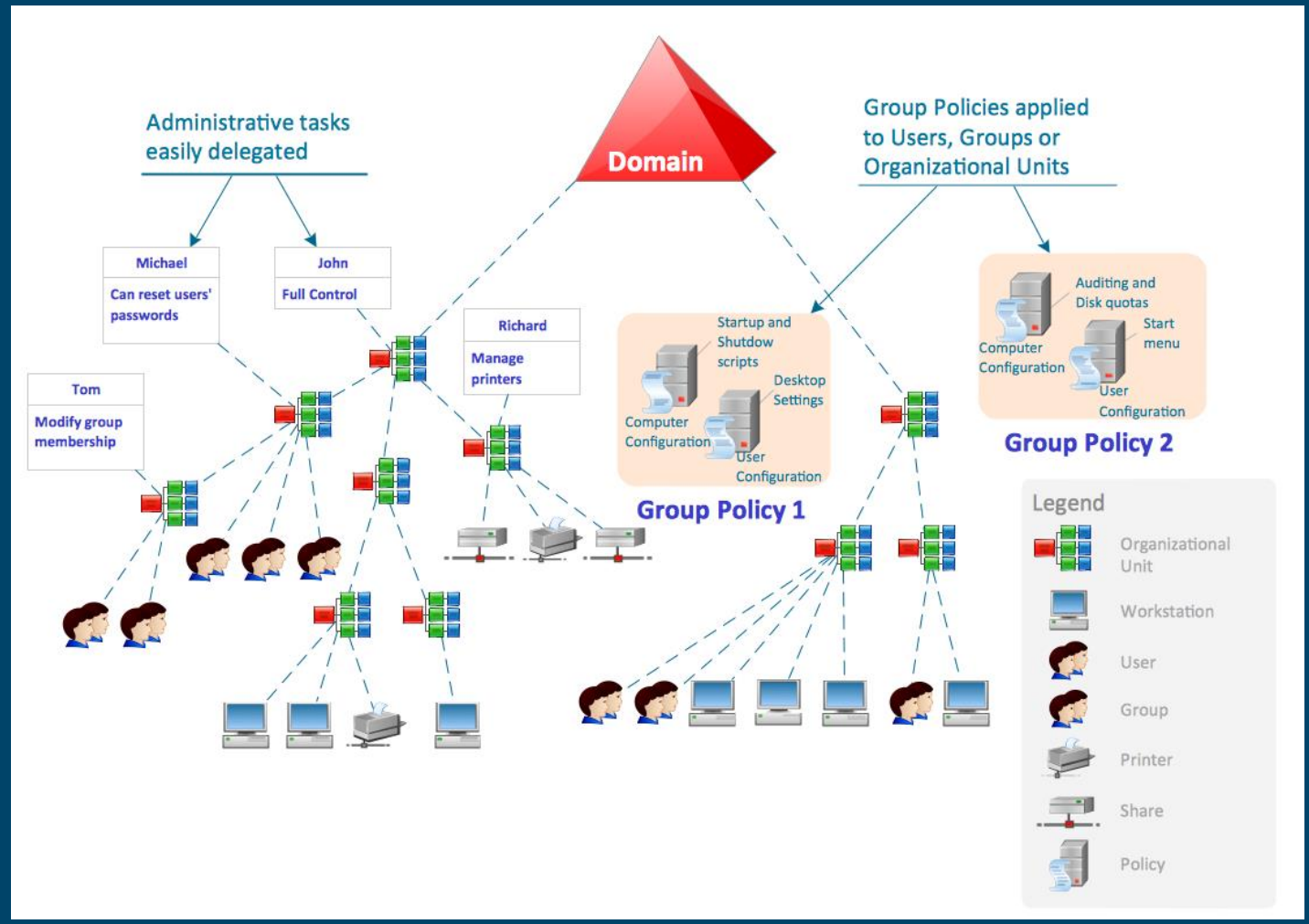
- The Evolution
- Attacks and the landscape in 2019
- A Overview on Azure Security Ecosystem
- What is Sentinel
- Connecting the dots

Agenda

- **It’s hunting season!**

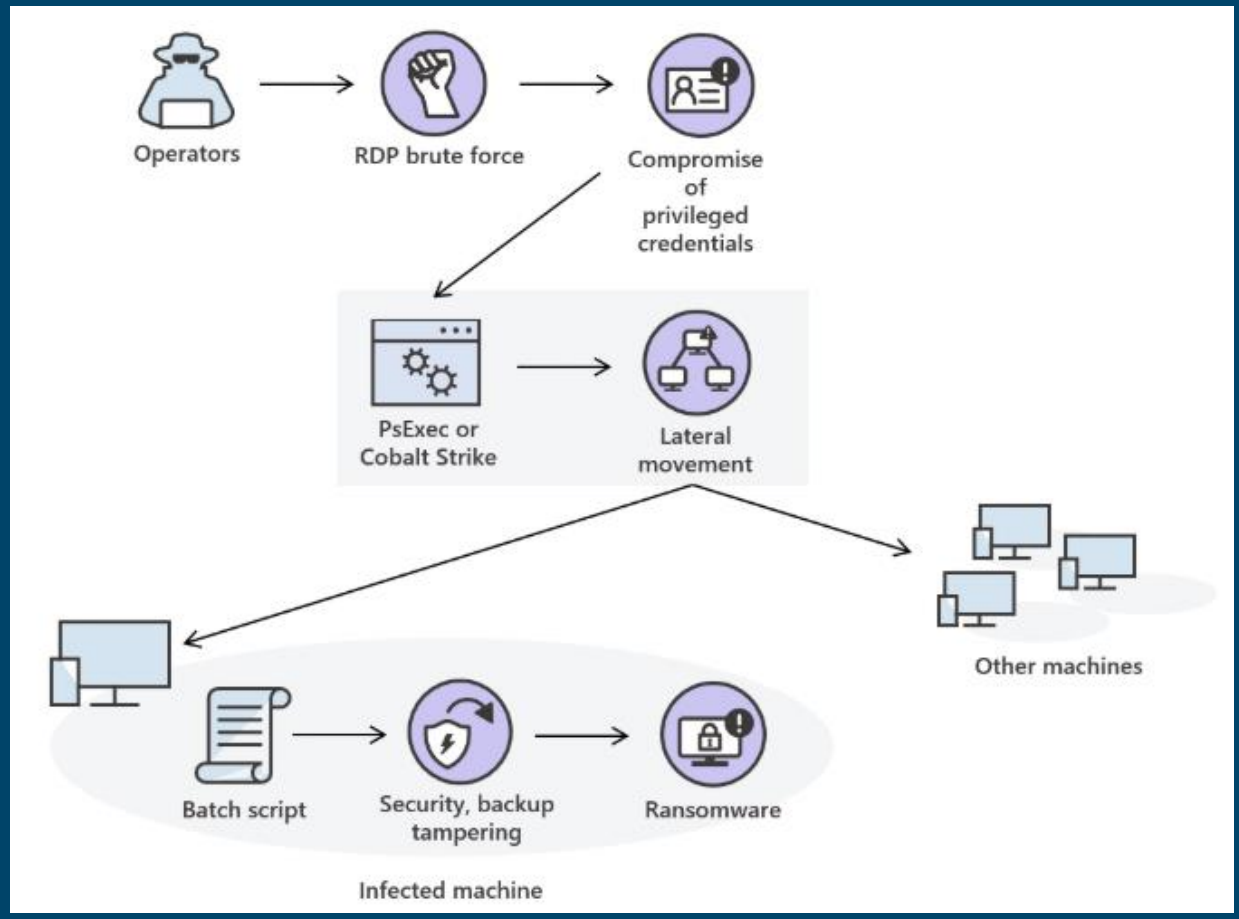
Once Upon a time..

- Active Directory
- Group Policy ~~was~~ is king!
- AD joined clients
- On-premises Collaboration
- System Management tools



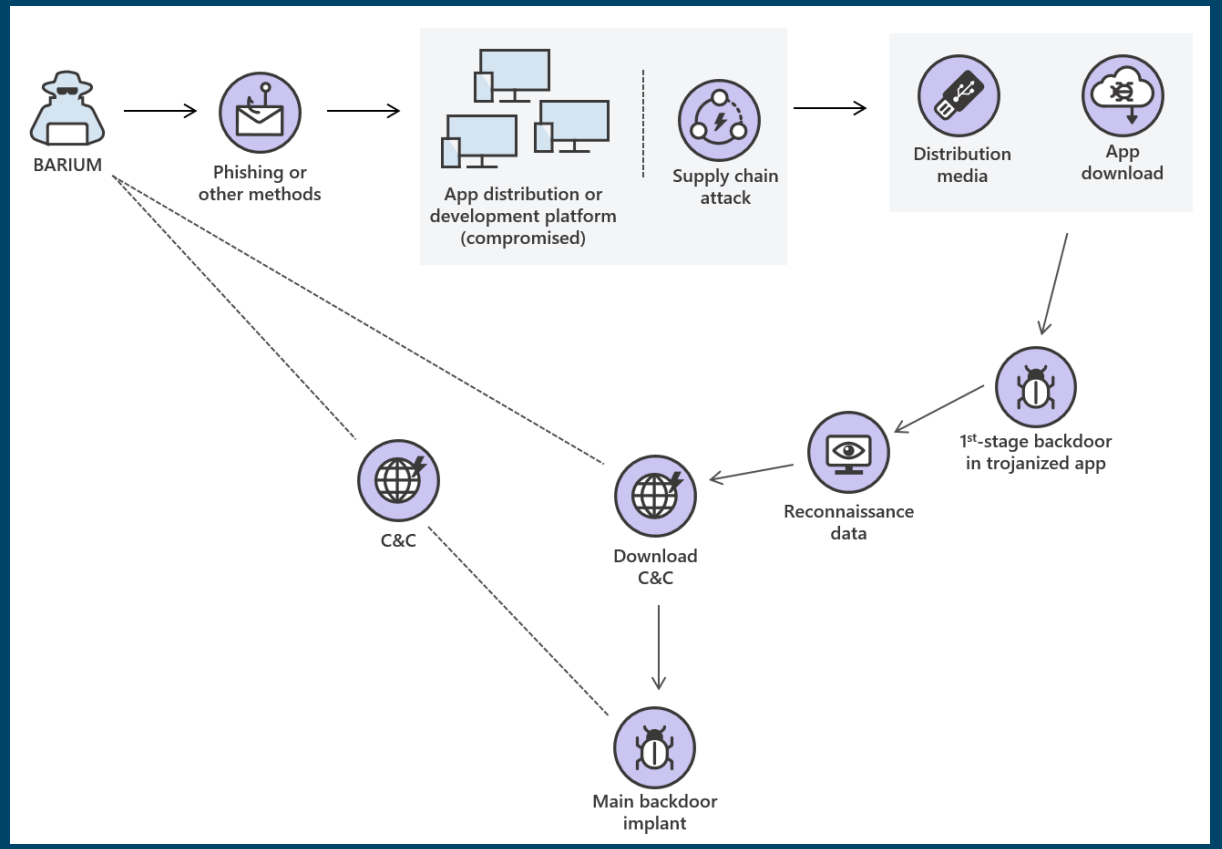
Lockergoga

- Entrypoint trough Email or drive-by download
- Distributed using Group Policy
- Each Payload is Unique
- Digitally signed by trusted third party



BARIUM

- Infected Trusted Sources and using drive-by download
- CCleaner and ASUS Update
- Compromised endpoints with ransomware



The latest addition – RDP BlueKeep

- Pre-auth RDP Bug
  - Pre 2012/Windows 8
  - Mitigated trough patching and NLA
- No exploit in the wild yet ☺
  - Only DoS attacks

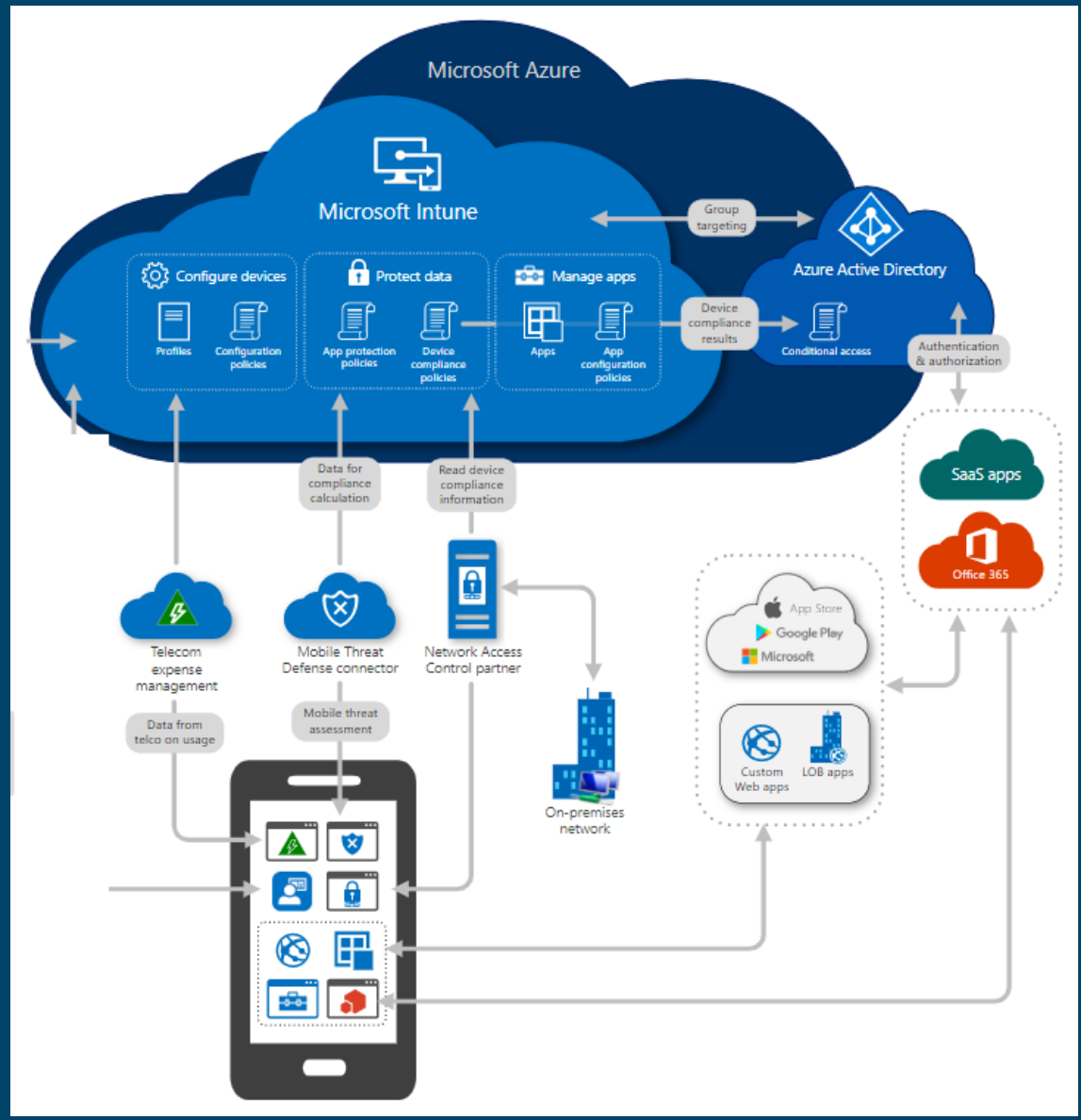
- Script for Scanning here →
- http://bit.ly/30OuCsQ

The Cloud is Magic!

"The cloud is more secure since INSERT VENDOR NAME spends millions every year on cloud security"

Landscape 2019

- Azure Active Directory
- Mobile Device Management
- Endpoint Protection
- SaaS and Package Distribution
- Web-based collaboration
- Multiple OS and devices
- + The cool existing legacy stuff



Alerts included in this incident

	DESCRIPTION	COUNT
	Threat Intelligence Information - Team Cymru	

```
  1  [##########################100.0%]   Tasks: 55, 253 thr; 4 running
```

```
#!/bin/sh

##############################################################################\
### A script for killing cryptocurrecncy miners in a Linux enviornment
### Provided with zero liability (!)
###
### Some of the malware used as sources for this tool:
### https://pastebin.com/pxc1sXYZ
### https://pastebin.com/jRerGP1u
### SHA256: 2e3e8f980fde5757248e1c72ab8857eb2aea9ef4a37517261a1b013e3dc9e3c4
##############################################################################\
```

Attack by the numbers

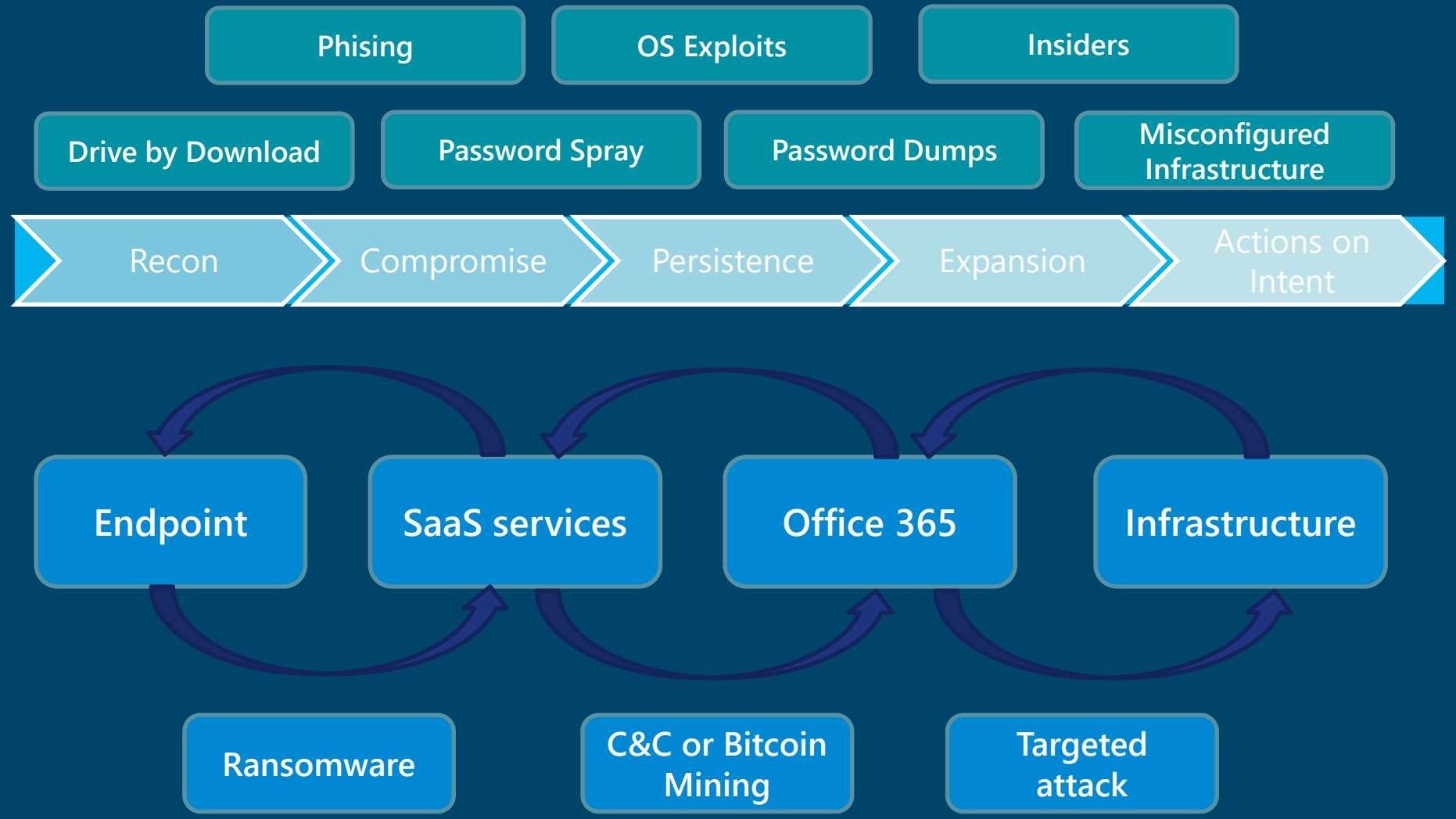
300% Increase in Identity Attacks over the past year

350 Thousand
Compromised Accounts detected in April 2018

46 Billion
Attacker driven sign-ins May 2018

23 Million
High Risk Enterprise Sign-in attempts March 2018

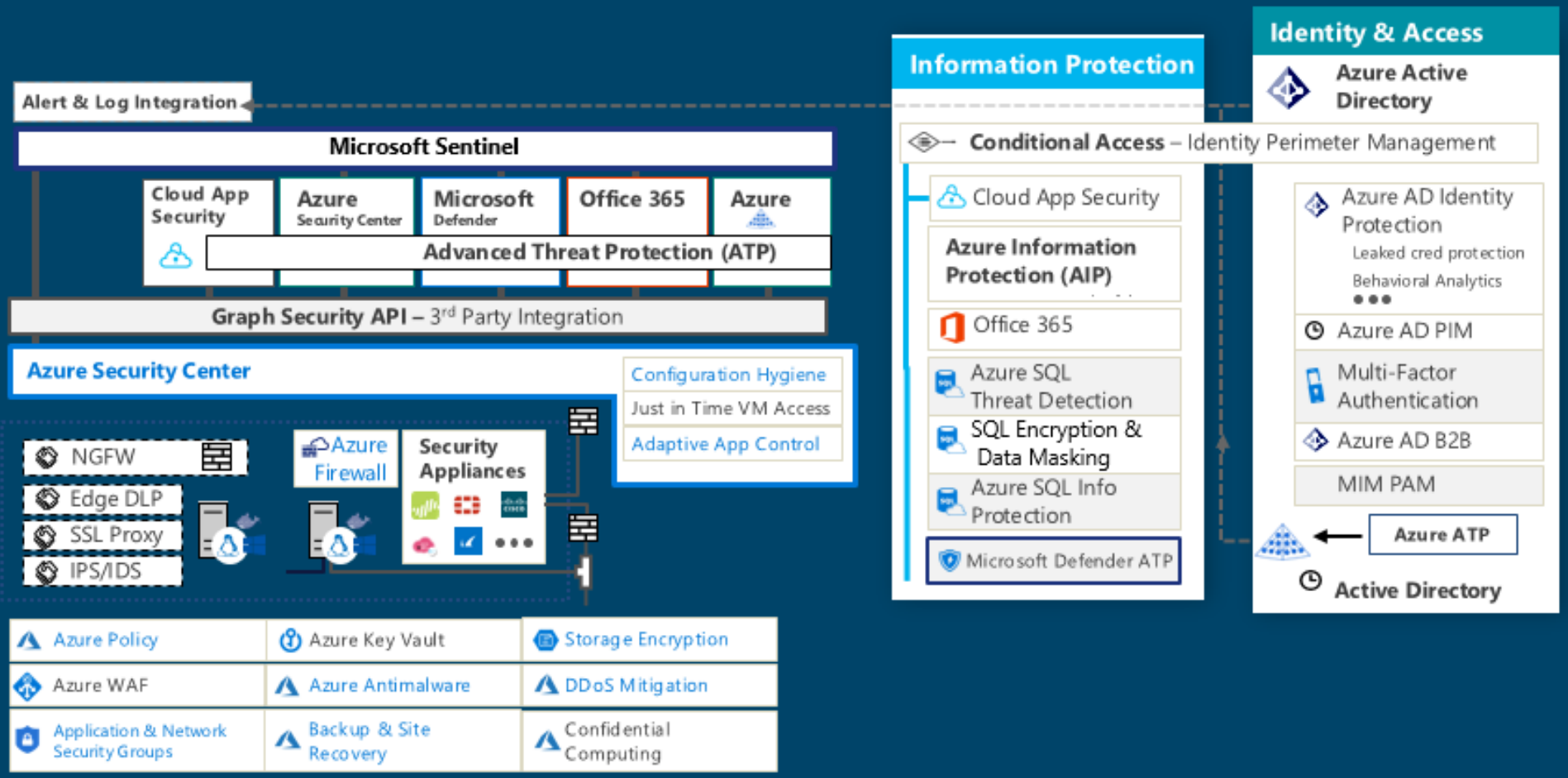
1,29 Billion
Authentications Blocked in August 2018



AAD	• Dump users and groups with Azure AD	• Password Spray: MailSniper • Password Spray: CredKing			
O365	• Get Global Address List: MailSniper • Find Open Mailboxes: MailSniper • User account enumeration with ActiveSync • Harvest email addresses • Verify target is on O365, [DNS], [urls], [list], [getuserrealm] • Enumerate usernames, 2FA status via ActiveSync [o365userenum] • Role, group, admin enumeration with Get-MsolRoleMember [RainDance]	• Bruteforce of Autodiscover: SensePost Ruler • Phishing for credentials • Phishing using OAuth app • 2FA MITM Phishing: evilginx2 [github]	• Add Mail forwarding rule • Add Global Admin Account • Delegate Tenant Admin	• MailSniper: Search Mailbox for credentials • Search for Content with eDiscovery • Account Takeover: Add-MailboxPermission • Pivot to On-Prem host: SensePost Ruler • Exchange Tasks for C2: MWR • Send Internal Email	• MailSniper: Search Mailbox for content • Search for Content with eDiscovery • Exfil email using EWS APIs with PowerShell • Download documents and email • Financial/wire fraud
End Point	• Search host for Azure credentials: SharpCloud	• Ransomware	• Persistence through Outlook Home Page: SensePost Ruler • Persistence through custom Outlook Form • Create Hidden Mailbox Rule [tool]		
On-Prem Exchange	• Portal Recon • Enumerate domain accounts using Skype4B, [LyncSmash] • Enumerate domain accounts: OWA & Exchange • Enumerate domain accounts: OWA: FindPeople • OWA version discovery	• Password Spray using Invoke-PasswordSprayOWA, EWS, Atomizer • Bruteforce of Autodiscover: SensePost Ruler • PasswordSpray Lync/S4B [LyncSniper]	• Exchange MTA	• Search Mailboxes with eDiscovery searches (EXO, Teams, SPO, OD4B, Skype4B) • Delegation	

Prepared by @JohnLaTwC, May 2019, v1.06
Microsoft

The Azure Security Ecosystem



Logging of Activity in Cloud

Audit Item	Category	Enabled by Default	Retention
User Activity	Office 365 Security	No	90 Days
Admin Activity	Office 365 Security	No	90 Days
Mailbox Audit	Exchange Online	Yes	90 Days
Sign-In Activity	Azure AD	Yes	30 Days (AAD P1)
Users at Risk	Azure AD	Yes	7 Days (30 Days, P1/P2)
Risky Sign-ins	Azure AD	Yes	7 Days (30 Days, P1/P2)
Azure MFA Usage	Azure AD	Yes	30 Days
Directory Audit	Azure AD	Yes	7 Days (30 Days, P1/P2)
Intune Activity Log	Intune	Yes	1 Year (Graph API)

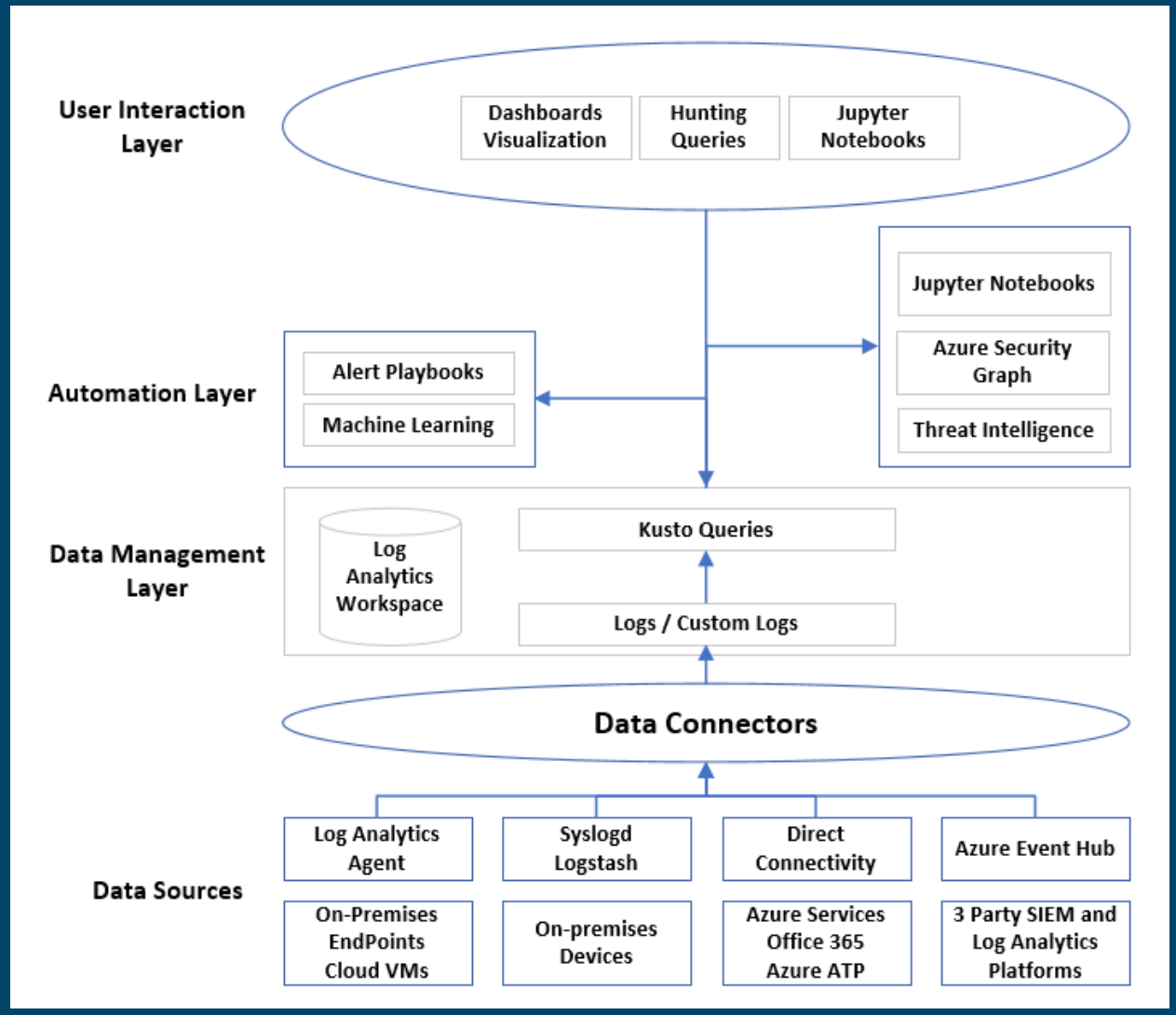
Logging of Activity in Cloud

Audit Item	Category	Enabled by Default	Retention
Azure Resource Manager	Azure	Yes	30 Days
Network Security Group Flow Logs	Azure	No	Depending on Configuration
Azure Diagnostics Logs*	Azure	No	Depending on Configuration
Azure Application Insight	Azure	No	Depending on Configuration
VM Logs	OS	Yes	Size defined in Group Policy
Custom Logs	OS	N/A	
Azure Security Center	Azure	No	
SaaS Usage	N/A	No	Requires Cloud App Discovery

* *Diagnostics logs available for most Azure Services*

Azure Sentinel

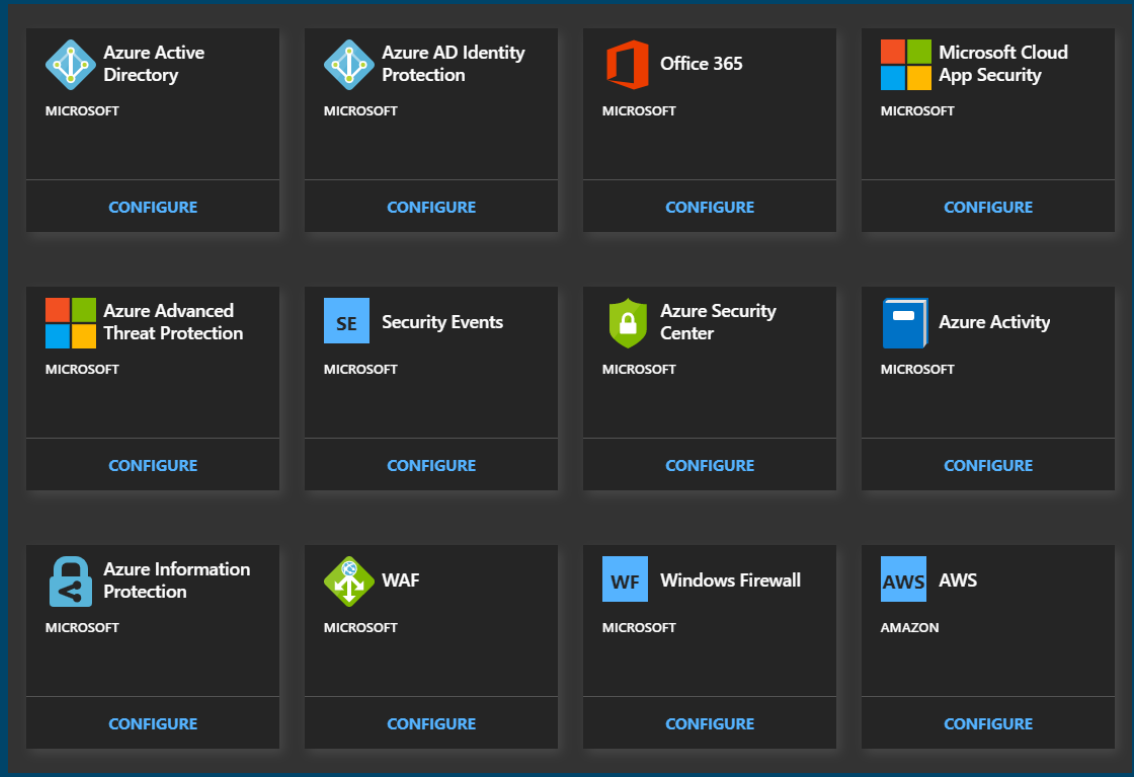
- SIEM and SOAR Solution based on Log Analytics
- Provides unified view and dashboards to the data sources
- Utilizes Machine Learning to collerate data from multiple sources
- Can integrate Threat Intelligence data from different sources own data or public



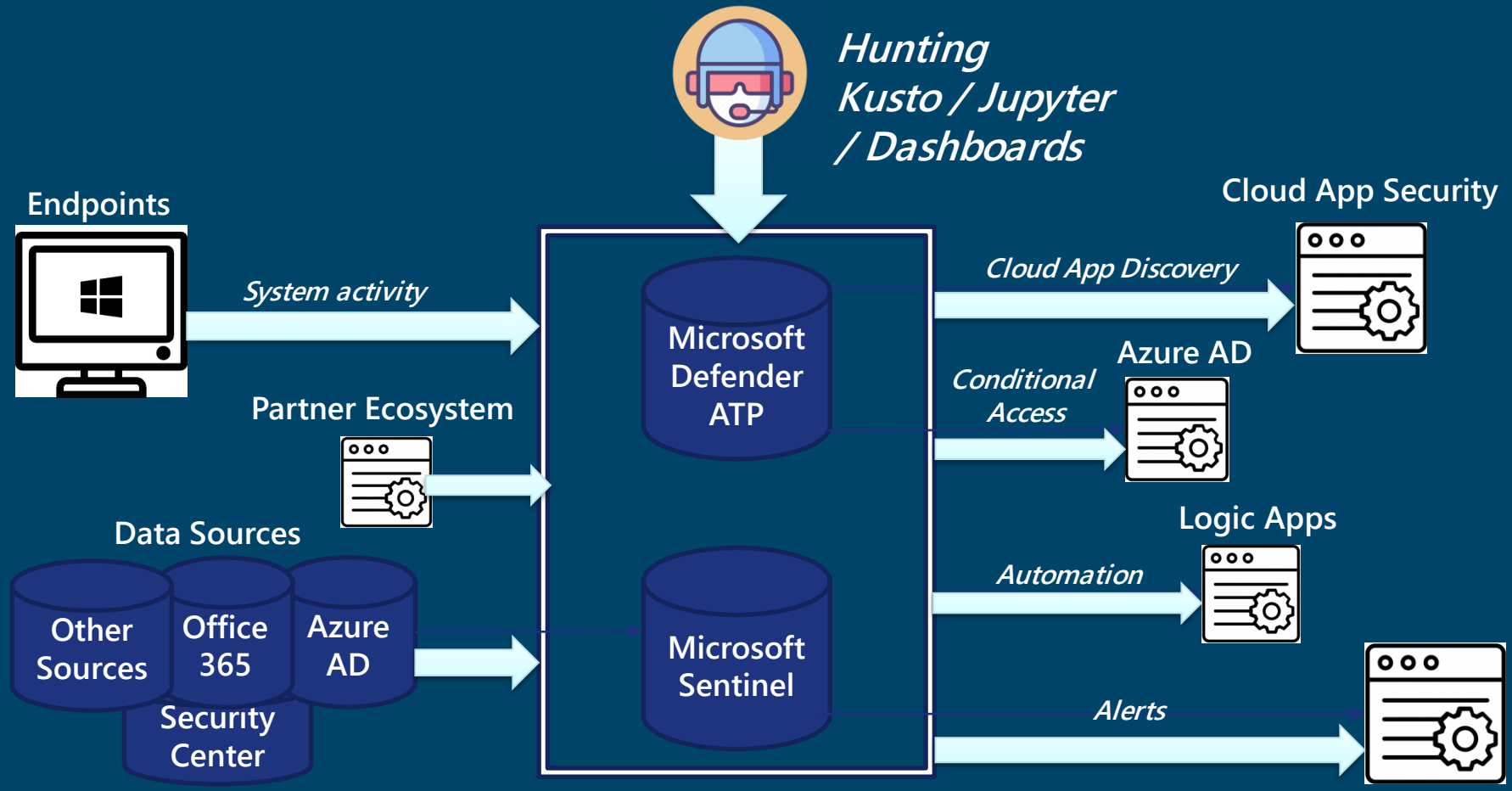
Azure Sentinel - Capabilities

- Data stored in data lake using Log Analytics
- Supports multiple data sources
- Predefined Connectors with dashboards
- Integrateable with Jupyter for in-depth analysis
- Playbooks using Azure Logic Apps
- Alerts available using Security Graph API

(Only supports GET and not PATCH or Subscribe)



Azure Sentinel - Capabilities



So how to get started?

Azure Sentinel

Activate the service → Create a Log analytics Workspace → Connect Data Sources** → Connect Threat Intelligence → Enable Fusion** → Create Playbooks

NAME
AzureAutomation(hybridWorkspace15525)
DnsAnalytics(hybridWorkspace15525)
InfrastructureInsights(hybridWorkspace15525)
SecurityInsights(hybridWorkspace15525)
ServiceMap(hybridWorkspace15525)
WireData2(hybridWorkspace15525)

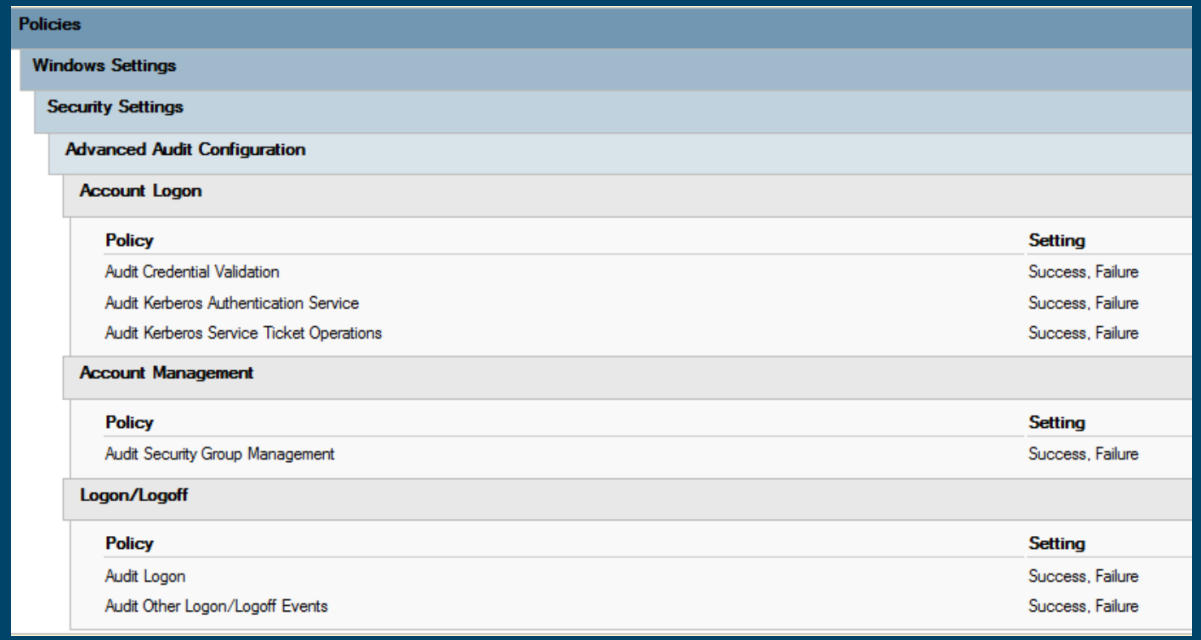
** Supported Data Sources are based upon Log Analytics*

***az resource update --ids /subscriptions/{Subscription Guid}/resourceGroups/{Log analytics resource Group Name}/providers/Microsoft.OperationalInsights/workspaces/{Log analytics workspace Name}/providers/Microsoft.SecurityInsights/settings/Fusion --api-version 2019-01-01-preview --set properties.IsEnabled=true --subscription "{Subscription Guid}"*

Enabling data sources

Insecure Protocols Dashboard

1: Enable Audit in Group Policy



Policies

Windows Settings

Security Settings

Advanced Audit Configuration

Account Logon

Policy	Setting
Audit Credential Validation	Success, Failure
Audit Kerberos Authentication Service	Success, Failure
Audit Kerberos Service Ticket Operations	Success, Failure

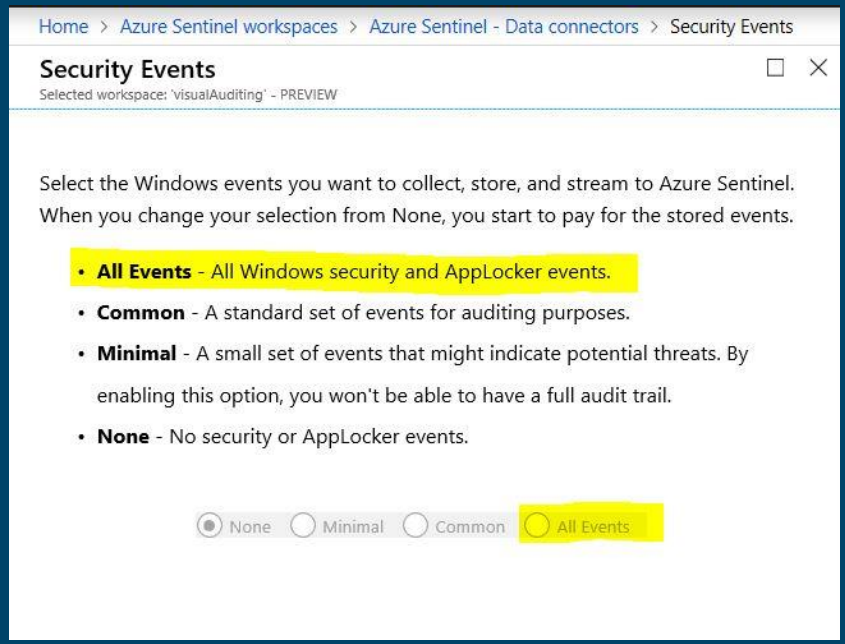
Account Management

Policy	Setting
Audit Security Group Management	Success, Failure

Logon/Logoff

Policy	Setting
Audit Logon	Success, Failure
Audit Other Logon/Logoff Events	Success, Failure

2: Enable Collection of Security Events

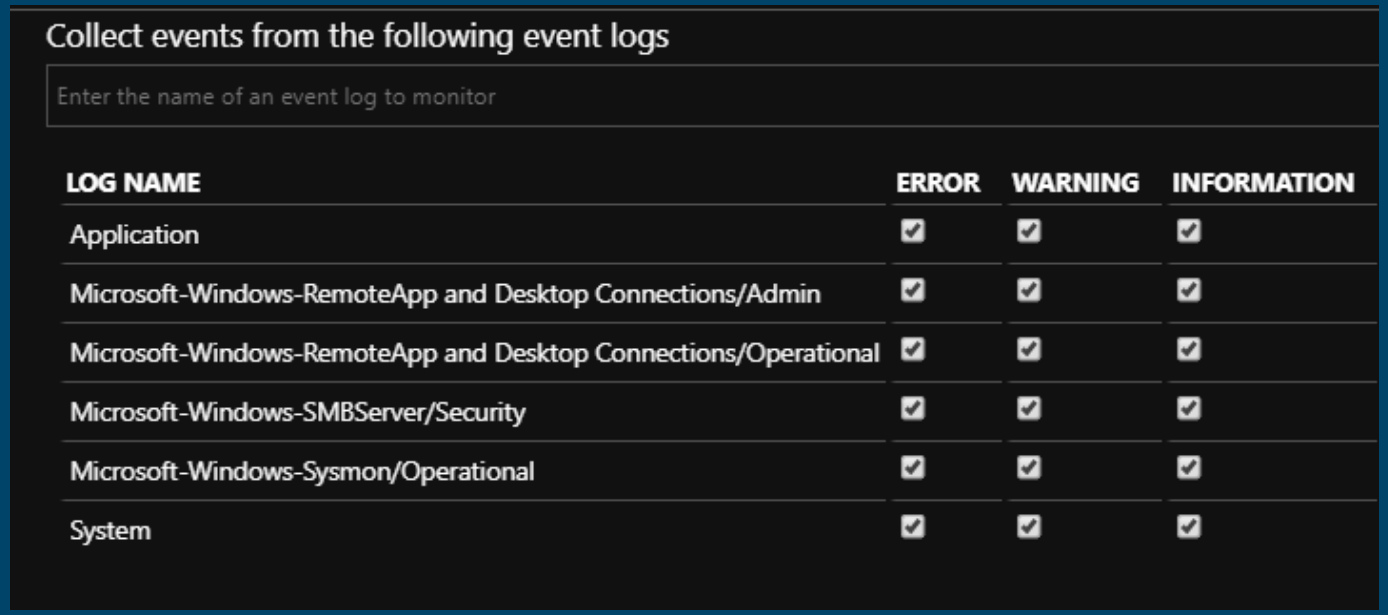


https://blogs.technet.microsoft.com/jonsh/azure-sentinel-insecure-protocols-dashboard-setup/

Enabling data sources

Custom Logs and log sources

Workspace - Advanced Settings - Data - Event Logs



Utilize Sysmon from Sysinternals to collect process information on Infrastructure

Somethings to consider first

- Microsoft Defender ATP data is not available in Sentinel
- No simple way to sanitize data only available trough REST API
  - Microsoft.OperationalInsights/workspaces/{workspaceName}/purge?api-version=2015-03-20
- Security Center is deprecating feature in July (Moving towards Sentinel)
- Retention is based upon the Log Analytics Workspace (Multiple Sentinel instances)
  - Azure Monitor also uses Log Analytics – Prefer to have seperate instances (Scoped Configurations)
- Cost? (Security Center, Log Analytics, Monitor, Machine Learning, Retention)

Intro to Kusto Query Language

- Read only request to process data and results from a dataset
- Queries are built defining the source and statements with applied filters
- Prefer to use time-filters to sort data

SQL to Kusto cheat sheet

The table below shows sample queries in SQL and thier KQL equivalients.

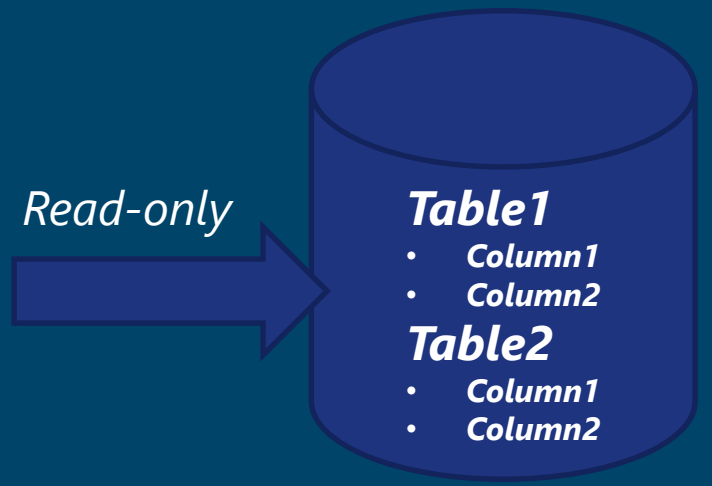
Category	SQL Query	Kusto Query
Select data from table	`SELECT * FROM dependencies`	`dependencies`

Query Example:

Table1

| where Timestamp > ago(1d)
| where Column1 == «value1»
| count

Read-only



Example hunting Sentinel and ATP

- **Attack techniques defined by MITRE ATT&CK**

  Knowledge base -- https://attack.mitre.org/

- **Universal but adapted using Kusto queries by Microsoft**

  https://github.com/Microsoft/WindowsDefenderATP-Hunting-Queries

  https://github.com/Azure/Azure-Sentinel

Example hunting Sentinel

- Looking after failed authentication attempts to virtual infrastructur

```
SecurityEvent
| where EventID == 4625
| where AccountType == "User"
| summarize CountToday = count() by EventID, Account, LogonTypeName, SubStatus, AccountType,
Computer, WorkstationName, IpAddress
```

Requires Security Center enabled

- Looking after failed authentication attempts to Azure portal

```
SigninLogs
| where TimeGenerated >= timeRange
| extend OS = DeviceDetail.operatingSystem, Browser = DeviceDetail.browser
| extend StatusCode = tostring(Status.errorCode), StatusDetails = tostring(Status.additionalDetails)
| extend State = tostring(LocationDetails.state), City = tostring(LocationDetails.city)
| where AppDisplayName contains "Azure Portal"
| where ResultType !in ("0", "50125", "50140")
```

Requires integration with Azure AD

Example hunting Sentinel

- **Mass Download Office 365 SharePoint**

```
let historicalActivity=
OfficeActivity
| where  RecordType == "SharePointFileOperation"
| where Operation in ("FileDownloaded", "FileUploaded")
| where TimeGenerated between(ago(30d)..ago(7d))
| summarize historicalCount=count() by ClientIP;
let recentActivity = OfficeActivity
| where  RecordType == "SharePointFileOperation"
| where Operation in ("FileDownloaded", "FileUploaded")
| where TimeGenerated > ago(1d)
| summarize recentCount=count() by ClientIP;
recentActivity | join kind= leftanti (
   historicalActivity
) on ClientIP;
```

Requires integration with Office 365

Example hunting Sentinel

- **Password Spray attacks**

```
let valid_logons = (OfficeActivity
    | where TimeGenerated > ago(30d)
    | where Operation == 'UserLoggedIn'
    | summarize by ClientIP);
let only_invalid_logons = (OfficeActivity
    | where TimeGenerated > ago(30d)
    | where Operation == 'UserLoginFailed'
    | summarize by ClientIP)
    | join kind=anti (valid_logons) on ClientIP;
OfficeActivity
    | where TimeGenerated > ago(30d)
    | join kind=inner (only_invalid_logons) on ClientIP
    | extend UserAgent=tostring(parse_json(ExtendedProperties)[0].Value)
    | where (UserAgent matches regex 'Microsoft Office/\\d+\\.\\d+ \\(Windows NT \\d+\\.\\d+; Microsoft
Outlook \\d+\\.\\d+\\.\\d+; Pro\\)'
            or UserAgent == 'CBAInPROD'
            or UserAgent matches regex '^[\\w\\.\\d\\-\\_]{4,15}\\/[\\.\\w\\d\\-\\_]{4,30}$')
    | summarize by ClientIP, UserAgent
```

Requires integration with Office 365

Let's go hunting!

Azure Sentinel moving forward

- **Unified Approach** to logging and threat hunting across plattforms
- (Identity, SaaS, Endpoint, PaaS and Infrastructure)
- **More Intelligence built-in** using Machine Learning and threat intelligence
- **Having Automated response** that can work across cloud providers, SaaS applications and across other security products.
- Ohhh and hopefully not cost too much.... ☺

Questions?

Thank You!

Platinum

Microsoft

Gold

audiocodes

Silver

au2mator

pexip

Jabra

logitech