What is M365

License bundle

• Office 365
• Windows 10
• Enterprise Mobility + Security
E5 (Security)

- Microsoft Defender ATP
- Azure ATP
- Office 365 ATP P2
- Microsoft Cloud App Security
- Azure AD Premium P2
- AIP P2
Auditing, Logs and APIs

Where are they
Logs

Verify Mailbox auditing per mailbox
Get-Mailbox -ResultSize Unlimited -Filter{RecipientTypeDetails -eq "UserMailbox"} | select name, auditenabled

Verify Tenant settings
Get-OrganizationConfig | select AuditDisabled

Enable unified logging
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true

Office 365 (EOP/ATP) best practices script
Accessing Logs

**PowerShell**
- Search-AdminAuditLog
- Search-MailboxAuditLog
- Search-UnifiedAuditLog
- ... and more

**Portals**
- portal.azure.com
- protection.office.com
- security.microsoft.com
- ... and more
Placement of Detection Logic

Service vs SIEM Queries

- Data Retention
- Correlation with other sources
- Data Volumes
- Log Management
Security Graph

**Apps**
- Web apps
- Device & native apps
- Bots
- Background processes
- Analytics dashboard & tools
- Automation workflows

**Microsoft Graph**
- Common Libraries, Authentication, and Authorization
  - Alerts
  - Secure Score
  - Indicators
  - Actions
  - Other Graph Services (Azure AD, O365, SharePoint, Intune ...)

**Microsoft Graph Security API**
Federates Queries, Aggregates Results, Applies Common Schema

**Security Providers**
- Microsoft Defender ATP
- Azure Information Protection
- Azure ATP
- Azure AD Identity Protection
- Cloud App Security
- Azure Security Center
- Office 365 ATP
- Azure Sentinel
Graph Explorer

Automation

Security Orchestration and Automation for the win
Microsoft M365 Built-in Automation

Microsoft Defender ATP
- Automated Investigations (Hexadite)
  - Alerts -> “Incidents”

MCAS
- Automated Governance

Office 365 ATP
- Automated Investigation and Response (AIR)
  - Exposed through UI or Management API
  - Alerts -> “Incidents”

Microsoft Threat Protection
- Alerts Correlated across M365 to “Incidents”
Demo

Built-in Automation & Governance
Cloud Automation Technologies

- Azure Automation
- Power Automate
- Logic Apps
- Azure Functions
- Power Apps
Logic Apps / Power Automate

- Automatic execution
- Easy to use and re-deploy
- Ready to use Connectors

Who does not want to put incidents on twitter? 😊
Azure Automation

- Automation
- Cloud + On-prem
- PowerShell & Python
- Source Code Control
Extend remediations to on-prem

- Alert Trigger
  - Logic App
  - Azure Automation Runbook
  - Hybrid worker
    - On-prem systems
Demo

Power Automate / Logic Apps + Azure Automation
Demo

Enrichment of Alert
Demo

Automated Remediation
lördag 11 januari

Inga äldre notiser
What about proactive hunting?

Hunting capabilities in M365 E3/E5
Threat Hunting capabilities

Defender ATP
- Devices and Servers

SIEM

```
// Hunting for malicious HID Keyboard devices
// PHP Event and Powershell or CMD within 10 seconds after driver load
let MalPnPDevices = 
[MiscEvents
| where ActionType == "PnpDeviceConnected"
| extend parsed=parse_json(AdditionalFields)
| sort by EventTime desc nulls last
| where parsed.DeviceDescription == "HID Keyboard Device"
| project PlugInTime=EventTime, computerName, parsed.className, parsed.deviceId, parsed.devicename, parsed.driverId, parsed.devicetype]
```

```
ProcessCreationEvents
| where ProcessCommandLine contains "powershell" Or
| ProcessCommandLine startswith "cmd"
| where isnotempty(ProcessCommandLine)
| project ProcessCommandLine, ComputerName, EventTime, ReportId, MachineId
| join Kind-Inner MalPnPDevices on ComputerName
| where (EventTime-PlugInTime) between (0min..10s)
| extend day = iff(floor(EventTime, 1d)==floor(now(), 1d), "today", "yesterday or earlier")
```
Microsoft Threat Protection

Unified Threat Hunting

Hunt across
• Email
• Devices
• Vulnerabilities
• Identity
Thank you

Blog post with links related to this talk:
http://blog.sec-labs.com/2020/01/sans-threat-hunting-summit-link-list

Twitter:
@mattiasborg82
@stefanschorling

Blog:
https://blog.sec-labs.com

#HappyHunting