SC-200 - Notes by Alexander Söderhäll

List of Abbreviations

- Cyber Defence Operations Center (CDOC)
- Security Information and Event Management (SIEM)
- Extended Detection and Response (XDR)
- Active Directory (AD)
- Automated Investigation and Remediation (AIR)
- Anti-Virus (AV)
- Advanced Hunting (AH)
- Machine Learing (ML)
- Domain Controller (DC)
- Cloud access security broker (CASB)
- Web-Application Firewall (WAF)
- On-behalf of (OBO)
- Data Loss Prevention (DLP)
- Role-Based Access Control (RBAC)
- Server Message Block (SMB)
- Indication of Compromise (IoC)
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection (CWP)
- Azure Resource Graph (ARG)
- Common Event Format (CEF)

Defender XDR

XDR Introduction

- XDR is the "package" which contains all other Defender threat protection.
- Detects malicious activity across email, endpoints, application and identity.
- XDR has automation. Can remediate some threats automatically.
- Microsoft Graph is a REST API.
    - Security Graph API allows development of customized security.
    - API supports KQL.
- AD compromise is detected in Identity.
- Malicious emails are detected in Office 365.
- Malware is detected in Endpoint.

XDR

- XDR Portal brings together:
    - Office 365: All Office 365 resources like Outlook etc.
    - Endpoint: Automated investigation and response for devices.
    - XDR: Uses 365 portfolio to automatically analyze attacks across domains and build a picture on a single dashboard.

        - Cloud Apps: SaaS and PaaS solution, threat protection on cloud apps.
        - Identity: Security for AD.
        - Vulnerability Management: Asset visibility, risk-based assesment etc.
- With XDR Portal we can set up security policies.
    - We can configure how strict we should be against phishing for certain domains and the likes.
- XDR is aligned with the MITRE ATT&CK chain.
- The incident overview includes a multitude of tabs with information. Like Alerts, Devices, Users, Mailboxes, Apps, Investigations and Evicdence and Response as well as a Graph.
- Each Alert in XDR has a MITRE Category.
- Alert supression rules can be on either a device or an organization.
- AIR in Endpoint:
    - May quarantine emails, block a process or a domain.
    - Can detect other entities and the likes given an alert. If malware is found, it will investigate all other devices for that malware.
    - Has different settings of automation. Recommended is full automation, can then remediate threats.
- Action Center = Remediation actions for Endpoint and Office 365.
    - Includes remediation actions on automated investigations and AV for example.
    - One can undo completed actions.
    - One can send suspicious Emails/URLs/Files for analysis.
    - One can view user reported phishing.
- Advanced Hunting:
    - Can run queries on Endpoint, Office 365, Cloud apps and Identity.
    - We can make custom KQL detection with automated response.
    - AH has event/activity data, updated immediatley. Also has entity data, updated less often (ca. 15 min).
    - AH has multiple schemas.
- Secure Score exists, reflects organisations security posture.
- Threat analytics increase understanding of emerging threats, vulnerabilities, prevalent malware etc.
    - One can view updated threats and read more details, including recommended actions.

Entra ID

- Enables investigation, detection and remediation of identity-based risks, based on AD.
- Risk classification:
    - *user risk*: Abnormal user behaviour or leaked credentials.
    - *sign-in risk*: Unfamiliar sign-in/atypical travel/suspicious IP.
- Workflow:
    - *self-remediation*: User resets password, enforces MFA.
    - *admin remediation*: Admin decides on action when risk is detected. Admin sets policies that monitor for risk.
- Identity risk = configure policy, investigate with a report, then remediate.
- Risk policy:
    - How Identity Protection responds to particular type of risks.
    - *Sign-in risk policy*:
        - Every sign-in gets a risk score, we can set threshold of what action should be taken at what score.

    - *User-risk policy*:
        - Same as above but not uses the context of identity behaviour pattern.
    - We can also set-up MFA.

Office 365

- Protects against phishing, automated response, provides insights and can simulate phishing.
- On-premise/hybrid/cloud email protection.
- Remediation actions which require approval:
    - Soft delete emails or clusters.
    - Block URL.
    - Turn off external mail forwarding.
    - Turn off delegation.
- *Safe Attachments* protects against unknown email threats by routing all messages and attachments through ML and other techniques to detect malicious intent. If none is found the email is then released to the recipient.
    - We can create Safe Attachment policy, i.e. how malicious attachments should be handled if detected in an email.
- *Safe Links* gives access to policies related to URLs in emails, and protects users against malicious links!
- *Anti-phishing policies* checks emails if they may be phishing. Action is taken based on the policies set-up.
- Office 365 does not require any sensor or such on all devices.

Identity

- Leverages on-premises AD signals to identify, detect and investigate advanced threats, compromised identities and malicious insider actions.
- Creates behavioural profile of each user. Anomaly detection.
- Sensors monitor on DC.
- Can detect different stages of attack:
    - Reconnaissance (LDAP, Account enumeration etc)
    - Compromised Credential (Brute force attempt)
    - Lateral Movement (Pass-the-ticket)
    - Domain Dominance (NTLM Relay, DCSync)
- Intune is not supported in Identity.

Cloud Apps

- Protects cloud services.
- CASB is the middle-man between users and their cloud apps. Allows monitoring and security controls.
- Four elements of Cloud Apps framework:
    - Discover and control Shadow IT.
    - Protect sensitive information.
    - Anomaly detection.
    - Compliance assessment of cloud services.
- Cloud Apps Dashboard exists, gives good overview of IPs, top users, category of apps etc.
- If Endpoint exists, it can block unsanctioned applications automatically.
- Has *Conditional Access App Control*, works best with Entra ID.

    - Define policies related to data exfiltration, user behaviour, blocking of access etc.
- Protect Information:
    - Discover apps and data in the organisation.
    - Classify the data in different categories.
    - Create policies that respond to alerts.
    - Monitor and report.
- Cloud Apps has anomaly detection, can be configured.

Copilot

Generative AI

- Encoders and decoders do dimension explosion/reduction.
- Languange models try to predict sentences.
- One can use different versions of Copilot depending on the use-case.
    - Copilot is built in to Azure and can be used for help with KQL as well.

Responsible GenAI

- Responsible AI: Identify potential harms, measure presence of harms, mitigate with multiple layers and operate the solution responsibly.
- Basically, try to look for dangerous prompts and mitigate them.
- Having an incident response plan is good, also make sure to adhere to legal, privacy etc.
- Enable loggin of the solution as to detect problems.

Microsoft Copilot

- Copilot can:
    - Can streamline incident summary.
    - Analysis of incident impact.
    - Generate KQL.
    - Reverse engineer scripts.
    - Guide in response.
- Copilot does this through:
    - Orchestration through NLP
    - Has plugins (tools/skills) s.a. security software programs.
- Efficient prompts are required to make Copilot produce good and reliable results.
- Users require permission to use Copilot, set-up in Entra ID.
- Copilot has customizable access to tenant files and plugins.
    - Azure Firewall
    - Azure Web-Application Firewall
    - Entra
    - Intune
    - XDR
    - External Attack Surface Management
    - Threat Intelligence
    - Purview
    - Sentinel

    - Public web plugin
- Promptbooks exists, "pre-defined" prompts to Copilot. Can be configured.
- Third-party plugins require OAuth and not OBO authentication.
- Copilot is embedded currently in XDR and Purview, making prompts more efficient.

Purview

DLP Alerts

- DLP alerts originate from Purview or Cloud Apps.
- DLP Policies allow:
    - Monitoring on OneDrive, Sharepoint etc for sensitive data.
    - Prevention of accidental sharing.
    - Files shared outside organisation, block access to them.
    - Monitor desktop versions of Office 365.
- Sensitive information = can be defined by regex or function.
    - Purview can then detect credit card information etc.
- Encryption of files exist.
- DLP Policy contains:
    - Where (which services/apps) to protect files.
    - When and how to protect.
- eDiscovery allows for compliance scans.
- DLP in Cloud Apps:
    - Viewable in Alerts if DLP has been configured.
- DLP component 'Sensitivity label' classifies documents.
- The 'File Policy' in Cloud Apps is used for DLP.
- DLP component 'DLP Policy' protects contents in the cloud.

Purview manage Insider risk

- Insider risk workflow
    - Make policies: Templates and policy condition. Policy dashboard exists to view all policies. We can anonymize names of users which violate policies. We can make exceptions for file types.
    - Policies generate alerts:
    - Review alerts.
    - Investigate the interesting alerts.
    - Take action.
- Insider Risk Management requires permission set be a global administrator. Requires roles Insider Risk Management or Insider Risk Management Admin role group.
- Departing employee data theft template requires an HR Connector to be set-up.
- Privacy and Policy indicators apply to all insider risk policies.
- Each policy must have a template assigned in the policy.
- Alerts can be assigned to a Case. A Case can then be investigated more deeply, and closed once finished.
- In each case we can view a multitude of tabs. Including case overview, alerts, user activity, content explorer, case notes and contributors. We can also send notices to the user which relate to the case.

- To capture forensic evidence in Purview, users must consent to explicit capturing, their devices be onboarded and have the Purview client installed.
- Forensic evidence allows screen capturing (clips) of user devices, if they allow it.
- Insider risk management notices templates exist. Automatically send email to users when their risky actions match a policy.
- Policy Timeframes define past and future review periods after a policy matches.
- Alert indicators and users or groups are needed when creating a policy.
- eDiscovery premium is required in order to escalate a case for investigation.

Purview Audit

- Audit enables logging (minimum 180 days) and searching (through Seach-UnifiedAuditLog cmdlet) activities performed by users and admins across Microsoft Exchange, Sharepoint, OneDrive and Entra.
- Standard and Premium Audit exist. Premium allow logs to be stored for 1 year or up to 10, instead of 180 days of standard. Also, one can customize which services log what data, has increased API bandwidth and *Intelligent insights*, helps spot potential breaches. Premium allows greater loggin of emails with MailItemsAccessed, records all synced emails and which emails were interacted with.
- Auditing is enabled in Purview compliance portal under *Audit*.
- One can search the Audit logs with a multitude of parameters.
- One can run up to 10 search jobs at a time.
- Audit can be used to check how users interact with Copilot.
- Audit logs can be exported to `csv` format (maximum 50.000 entries).
    - Make a search job, export the results to `csv`.
    - Use Excel Power Query editor.
- We can also use PowerShell to search and export audit logs.
- Audit log retention policies (premium only) can be customized based on microsoft service, activity type and priority level (can override default policy).

Purview Content search

- Has KQL.
- eDiscovery can identify and deliver evidence in legal cases. Can search for content in Exchange, OneDrive, Sharepoint, Teams, 365 Groups and Yammer Teams.
- Three levels:
    - Content Search: Basic search and export.
    - eDiscovery standard: Make cases, access control for users to view cases.
    - eDiscovery premium: Advanced control (custodian) and workflow (tags, analytics etc).
- Content search delivers results of email messages (not calendar), different file extentions like `txt, html, doc, pdf, zip`. Maximum 1000 items can be previewed.
- Export reports contain a summary, results of the logs exported like messages and locations.
- *Search permission filters* exist.
    - Can manage what can be searched in eDiscovery.
    - One can also separate an organisation into compliance boundaries.
    - We can determine filters based on mailboxes/onedrive/contents/site, determines what users/groups can search for.
    - We tell what users/groups the filters apply to.
    - Permission filters are made through PowerShell commands.

- To run security filters one must connect PowerShell to Purview and Exchange Online.
- To run security filters one must be a member of the Organization Management role in the Purview Compliance portal.
- Content search can search and delete emails in the Exchange deployment.
- To create and run Content search one must be member of eDiscovery manager group or be assigned Compliance Search role.
- To delete messages, member of Organization Management group or Search and Purge role.

Purview Practical

View DLP Alerts in Purview

- MS Purview compliance portal > Solutions > **Data loss prevension** > Alerts.
- Choose filters.
- Select Alert
    - Events
    - Sensitive Info Types
    - Manage Alert
    - Management log (workflow history)

Set up HR Connector

- Global admin must consent to allow Office 365 Import service to access data in the organisation.
- User that creates HR connector needs to be assigned the **Mailbox Import Export** role in Exchange online.
- System must be in place that retrieves and exports data from organisations HR system and adds to `csv` file.
- Now HR connector is done by:
    - Create ap in Entra ID.
    - Generate `csv` file from HR system.
    - Create HR connector in Purview compliance portal.
    - Run script that uploads HR data in the `csv` file to Microsoft cloud.

Create new insider risk policy

- Use **Insider risk management** policy wizard in Purview compliance portal.
- In wizard, configure:
    - Policy template.
    - Users or groups to apply policy to.
    - Alert indicators.
    - Duration for monitoring.

Configure and Manage Forensic Evidence

- Confirm **insider risk management subscription** and add domain compliancedrive.microsoft.com to firewall allowlist.
- Onboard user devices to Purview compliance portal and install Purview Client on devices.

- Enable forensic evidence capturing, config parameters and offline capturing options in Purview compliance portal.
- Define forensic evidence policies. One of:
    - Specific activities.
    - All activities.
- Admin must visual capturing for specific users is defined and approved through dual auth. process.
- Members of **Insider Risk Management** or **Insider Risk Management Admins** submit approval requests for devices/users to member of **Insider Risk Management Approvers** for capturing to commence.
    - In Purview compliance portal, Insider risk management > Forensic evidence > User management.
    - Select Manage forensic evidence requests tab.
    - Select Create request.
    - On Users page, select Add users.
    - Locate user /w search and add, go next.
    - On Forensic evidence policy page, add policy for the users.
    - On Justification page, add justification in text.
    - On Email Notifications page, select email template. Will be sent out to the users when request is approved.

Approve or reject capturing requests

- Go to Insider risk management > Forensic evidence > Pending requests.
- Select a user to review.
- Review request, approve or reject.

Revoke capturing

- Go to Insider risk management > Forensic evidence > User management.
- Select Approved users tab.
- Select user and then remove.

View captured clips

- Can be viewed in **Forensics Evidence** tab.

Create a Notice Template

- In Purview compliance portal > Insider risk management > Notice templates tab (we can delete and update from here as well).
- Create notice template.
- Create a new notice template.
    - Name
    - Send from
    - CC and Bcc
    - Subject
    - Message Body.

Configure Audit in Purview

- Verify subscription.
    - Audit (standard) included in:
        - Microsoft 365: E3, E5, F1, F3
        - Office 365: E1, E3, E5, F3
    - Audit (premium) included in:
        - Microsoft 365: E5, E5 Compliance, F5 Compliance, F5 Security + Compliance
        - Office 365: E5
- Assign permissions.
    - **View-Only Audit Logs** or **Audit Logs** roles to admin or investigation members.
    - **Audit Manager** = export, search and manage audit settings.
    - **Audit Reader** = export and search audits.
- From now only for premium:
    - Set up Audit (premium) for users enable correct license under **Licenses and Apps** page.
    - Expand Apps section, ensure that **Microsoft 365 Advanced Auditing** is enabled.
    - Enable audit events.
    - Audit retention policies.

Endpoint

- Administrators can request updates to software.
- Has attack surface reduction:
    - Microsoft Edge is run as a container.
    - Applications must earn trust.
    - Network protection in Microsoft Edge.
    - Network firewall on host.
- Has automatatic remediation capabilities.
- We can view all devices, check all software, determine remediation steps based on vulnerabilities.
- Endpoint requires a separate license.

Deploy Endpoint

- To configure Endpoint portal, you must be global admin or sec admin.
    - Data retention is six months by default.
- Endpoint sensor requires Windows HTTP which it uses to send data and communicate with Endpoint service.
- Endpoint works on Windows, macOS, Linux, Android and iOS.
- To onboard a device, follow steps in the Defender portal.
- Use RBAC to create appropriate control of Endpoint for users.
- We can also group devices.
    - We can have different remediation settings of device groups.
- Advanced Features:
    - Automated investigations.
    - Remediate PUA.
    - Limit correlations to device groups.
    - Custom network indicators: block specific IP/domains basically.
    - Tamper protection.
    - Connect to Identity, Cloud Apps, Office 365, Purview, Intune.

    - Conditional Access Policy with Intune.
    - Find unmanaged devices (device discovery).
    - Download Quarantined files.

Attack Surface Reduction

- Attack surface reduction rules (requires Microsoft AV)
    - ASR either NaN/Block/Audit/Warn.
    - Many rules exist, including block executable content from email, office from creating child process, API calls to Office macro etc.
    - Can create exceptions of some folders.
    - Best practice, set all rules to audit first to evaluate impact.
- Hardware-based isolation
- Application control
- Exploit protection
- Network protection (requires Microsoft AV)
- Web protection
- Folder AC (requires Microsoft AV)

Device investigation

- Device inventory list contains meta-information on all devices.
- Each device has its own dashboard. We can view details on the device, conduct actions on it, like isolation or AV scan, see the timeline and software inventory.
- Behavioural blocking:
    - Uses AI and ML to identify and stop threats based on process trees and behaviour.
    - Uses Next-generation protection to detect threats by analyzing behaviour and stop threats that are running.
    - EDR makes incidents out of multiple alerts, linking things together.
- Client behavioural blocking sends Endpoint sensor signals to cloud, which uses ML to process, and if determined a threat will send back to block an artifact.
- Feedback-loop component can block similar attacks on other devices.
- Endpoint in block mode will automatically block certain artifacts.
    - Can be used with third-party AV.
- Device Discovery:
    - Basic mode: onboarded endpoints passively collect network events and extract device information.
    - Standard mode: onboarded endpoints actively find devices.

Actions on Device in Endpoint

- Live response exists = restricted remote shell on host.
    - Like normal CMD, can also download files and upload files to host.
- Investigation package.
    - Contains info on auto-start applications
    - Installed programs as `csv`
    - Network connections
    - Prefetch files = Tracks files recently used.

    - `csv` running process list.
    - `csv` scheduled tasks.
    - security event log.
    - `csv` services and states.
    - SMB sessions (network folders, misc net. comms)
- Isolate host from network.
- Restrict app execution.
- Run AV scans.

Evidence and entities investigations in Endpoint

- File page exists.
    - View details of file.
    - Download file.
    - Add indicator (Endpoint will now allow/block in tenant.)
    - Deep analysis (execute file in secure environment).
        - Report includes registry modifications made.
- User page exists.
    - Account details.
    - Logged on hosts.
    - Alerts related to user.
- Investigate IP Address
    - IP stats worldwide
    - DNS names
    - Alerts related to IP
    - IP in organisation
    - Prevalence
    - Observed devies with the IP.
- Investigate domain
    - Basically same as IP.

Manage automation in Endpoint

- Automations related to:
    - Automated investigations.
        - Set certain files to be sent for File Content Analysis.
        - Enable Memory Content Analysis if we want Endpoint to analyze processes.
        - Different levels for different device groups.
    - Enable EDR in block mode (block artifacts/behaviours).
    - Automatically resolve alerts.
    - Allow or block file (if Microsoft AV on host and cloud-based protection).
- Block risky devices from entering company resources with CA.
    - Requires Endpoint Manager with Intune and Azure AD, host must be W10 OS.
    - Configure AC in Azure AD, depending on risk level of hosts.

Configure alerts and detections in Endpoint

- Advanced features

    - Configure to allow RBAC users Live Response (shell).
    - Enable unsigned scripts in Live Response.
    - Enable Custom Network Indicators (allow/block certain IP/domains/URL).
- We can configure alert notifications (send new alerts to who).
- Supress alerts is possible.
- IoC can be setup to allow/alert/block hosts, IPs, files, domains, certificates.
    - We can also import a `csv` IoC list.

Vulnerability Management in Endpoint

- Real-time discovery sends sensor data on vulnerabilities and security configurations to the dashboard.
- We can view vulnerabilities and software.
- Uses data of vulnerabilities exploited in the wild.
- Real-time monitoring of remediations etc.
- Different licenses exist. Do more or less.
- Exploit availability graphs show which devices are most exploitable, viewable in Vulnerable Devices Report.
- Weaknesses in device dashboard show CVEs.
- Threat Analytics show recently published threat reports.

Endpoint Practical

Create and manage roles for RBAC

- As Sec admin or global admin access the Defender Portal.
- Goto Settings > Endpoints > Permissions > Roles
- Turn on roles.
- Add Item
- Enter role name, desc. and permissions
- Assign role to Security Group.

Configure Device Groups

- Defender Portal > Settings > Endpoints > Permissions > Device Group.
- Add device group.
- Configure group incl. automation settings.
- Assign the user group that can access the device group.

Cloud

- Cloud security two pillars:
    - Cloud Security Posture Management (CSPM)
        - Guidance on increasing security, provides visibility of cloud infrastructure.
    - Cloud Workload Protection (CWP)
        - Security Alerts.
        - This is the main idea of Cloud.
- Cloud can secure multiple Microsoft cloud solutions, Hybrid cloud environment and third part cloud.
- Can be integrated with Endpoint.

- Block Bruteforce attacks.
- To config Cloud:
    - Search Log Analytics, do some config.
    - Set up Defender for Cloud, do 'Getting started', do some config.
    - Onboard on-premise host with Azure Arc. Add a server. Download and run a script on the server.

Connect Azure assets to Cloud

- Cloud automatically analyzes azure resources to identify vulnerabilities.
- *Asset Inventory*, detect assets, we can query them with filters.
    - Uses Azure Resource Graph (ARG) which uses KQL to explore resources.
- Auto provisioning
    - Can be enabled in Log Analytics and of extensions.
    - Basically, it deploys resources and extension automatically, so no manual set-up required.
    - Policy Add-on for kubernetes is optional.
- We can also do manual set-up of agent provisioning.
    - Then we need to install Log Analytics Agent.

Connect non-Azure assets to Cloud

- We use Azure Arc to manage all resources.
    - It connects hybrid, on-prem and other non-Microsoft cloud assets to Azure Resource Management.
    - Hybrid machines, must install Azure Connected Machine Agent.
    - Log Analytics also good if we want to monitor the OS and workloads of the machine.
- We can connect AWS to Defender for Cloud.
    - Azure Arc deploys Log Analytics to AWS instances.
    - Do some configs, to authenticate AWS Security Center use IAM.
- We can connect GCP to Defender for Cloud.

Manage Cloud security posture

- Azure Policy
    - Rules about specific security conditions.
    - Mainly *Audit* policies what check for compliance.
    - *Enforce* policies also exist, enforce secure settings.
    - We can create custom rules.
- Azure Policy Initiative
    - Grouped Azure Policies.
    - Ensures compliance.
    - Default Initiative added to all = Azure Security Benchmark.
- Security recommendation
    - Result of periodic policy checks.
    - Provides recommendations on how to remediate.
    - To remediate a recommendation, press "Fix".
- Secure Score
    - A single score reflecting the security posture.
- We can explore recommendations that improve our security posture.

- Regulatory compliance dashboard exists.
    - Many compliance standards exist.
- Azure Monitor Workbooks
    - Provide easy report creating and data analysis.

Cloud workload protections

- Defender for Servers works on Windows and Linux machines.
    - Does File-integrity monitoring.
    - Hybrid and multicloud we use Azure Arc instead.
    - Defender for Servers can be connected with Endpoint.
- Defender for App Service.
    - Basically secure applications from attackers.
- Defender for Storage.
    - Looks for viruses in storage, suspicious accesses.
- Defender for SQL.
    - Scans, detects and helps remediate DB vulnerabilities.
    - Can detect brute-force, SQL injections, insidier threats.
    - Defender for open-source DB also exists.
- Defender for Key Vault.
    - Safeguards keys and certificates.
- Defender for Resource Manager.
    - Enables one to create, update and delete resources in Azure account.
- Defender for DNS.
    - Monitors DNS queries.
- Defender for Containers.
    - Protects Kubernetes.
    - Environmental Hardening, Vulnerability Assessment and Run-time threat protection.
    - Auto provisioning is enables for all containers by default.
- Defender additional protections.
    - Protection on network layer.
    - DDoS protection.
    - WAF.

Remediate alerts in Cloud

- Incidents and alerts work the same way as in Endpoint / XDR.
- Uses TI, Signature detection (ML) and anomaly detection.
- Logic App, workflow automation and automatic remediation of alerts.
- We can also supress alerts (supression rules).
- We can generate threat intelligence reports.

Cloud Practical

Configure auto provisioning

KQL for Sentinel

- Intro to KQL.
  - list: `datatable(account: string) [@"account1", @"account2"]`
  - `extend` creates a new column.
  - `order by colName1, colName2`
  - project:
    - `project` = what columns to include.
    - `project-away` = what to exclude.
    - `project-keep, project-rename, project-reorder`
  - summaries:
    - `count()`
    - Has many more, like avg(), max(), percentile(), variance().
  - `arg_max(TimeGenerated, *)` will return most current row.
    - `arg_min` same as above.
  - `make_list(), make_set()` return JSON objects.
  - `bin(TimeGenerated, 1d)` is really good, like zip.
  - timechart, barchart and scatterchart exists!
  - `union` supports wildcards, we can do `union Security*` to union all tables that start with Security.
  - `joins` exist in many different ways.
  - Extract data
    - `extract` and `parse` use regex to match things in unstructured strings.
    - Some table data contains Dynamic fields, we can access them by calling their key like `field.key`.
    - Some logs return JSON objects. We parse them with `extend object = parse_json(Column)`, and then we can call fields by calling the key like `object[0].key`
      - We can also make the entire thing into separete values with `mv-expand object = parse_json(Column)`, then we can do `object.key` instead.
      - We can also use `mv-apply object = parse_json(Column) on (wher object.key == "Something")` to make a condition instead.
  - We can read external data from other containers with `externaldata`.

Configure Sentinel

Introduction to Sentinel

- Sentinel is a Security Information and Event Management (SIEM).
- Sentinel is deployed in Azure.
- Logs arrive from *Data connectors*.
  - syslogs
  - Common Event Format (CEF)
  - Azure
  - AWS
- Stored using Log Analytics.
- Data visualisation with *Workbooks*.
- *Playbooks* = remediation/investigations etc, (SOAR) capabilities.

Create and manage Sentinel workspaces

- Create a Log Analytics workspace in Azure, to store the logs.
    - Specify region, states where logs are stored.
- 3 impl. options (single workspace, regional workspaces or multi-tenant).
- Manage Workspaces
    - Sentinel Workspace manager OR Azure Lighthouse.
- Sentinel uses RBAC.
- Data retention from 30 to 730 days.
- Configure logs:
    - Analytics Logs: Default.
    - Basic Logs: Only 8 day retention, basic, less expensive.
    - Archive Logs: Stored logs, less expensive.
- Sentinel Workspace Contributor can create workspaces.

Query logs in Sentinel

- Log Analytics workspace queried with KQL.
- Contains many different schemas/tables.
- Useful tables:
    - SigninLogs: AD signin events.
    - AuditLogs: Entra ID logs.
    - CommonSecurityLog: Syslog messages in CEF format.
- If XDR connector, tables:
    - Device*: Endpoint events related to devices.
    - Email*: 365 events, related to email.
    - Identity*: Related to Identity (AD).

Watchlists in Sentinel

- Data collection from external data sources.
- We can group items in watchlists, like high-valued servers.
- We can create and manage watchlists.

Threat Intelligence in Sentinel

- Common TI indicator (considered tactical) is called IoC.
    - Associate URLs, file hashes, IP and other.
- We can connect common TI platforms as data connectors to Log Analytics.
- Logs reside in table *ThreatIntelligenceIndiactor*

Connect logs to Sentinel

Data Connectors

- Data sources are connected in Sentinel Data Connectors.
- Data Connector providers:
    - XDR
        - Endpoint
        - Identity

        - Office 365
        - Cloud Apps
    - Azure
        - Entra ID
        - Azure Activity
        - Entra ID Protection
        - DDoS protection
        - Defender for IoT
        - WAF
        - etc....
    - Syslog or CEF protocol connectors are available.
        - Agent must be deployed in Azure VM.
- We can view connected hosts in Agents in Log Analytics.

Connect Microsoft Services to Sentinel

- We can connect different services like Office 365, Entra, Entra ID Protection.

Connect XDR to Sentinel

- Must install XDR Content Hub solution.
- Then we can activate XDR, Cloud and IoT as data connectors in Sentinel.
- XDR connects to the SecurityAlert table.

Connect Windows hosts to Sentinel

- Can be on-premise hosts or Azure VMs
- An agent must be installed on host:
    - Windows Security Events via AMA Connector
        - Requires Azure Arc on non-Azure VMs.
    - Security Events via Legacy Agent Connector.
        - `Microsoft-Windows-Sysmon/Operational` is the log name.
    - Sysmon events are stored in Event table.

Connect CEF logs to Sentinel

- Used to connect Linux VMs or the likes.
- CEF connector writes to CommonSecurityLog table.
- CEF connector deploys a Syslog forwarder.

Connect syslog to Sentinel

- Send syslog with Azure Monitor Agent Data Collection Rule (DCR).
- Syslog collector writes to Syslog table.
    - Message data is stored in string field named SyslogMessage.
    - We need to parse the fields manually with KQL parse `extract`.

Connect threat indicators to Sentinel

- We can use TAXII (v 2.0 or 2.1) or TI Platforms Connector, both write data to ThreatIntelligenceIndicator table.
    - Both use Graph Security API to send data to Sentinel.

Threat detection with Sentinel analytics

Analytics rules

- Search for threats by using rules that create alerts.
- Can use *Fusion engine* (ML) to detect multi-stage attacks.
    - Alert rules are created using the Fusion template.
- ML behaviour analytics exist.
- Scheduled analytic rules: One can customize them.
- Microsoft security can create incidents based on all alerts generated in Cloud.
- We can create custom schedule alerts with KQL and assign an automated response with Sentinel Playbook.
    - Define KQL in section 'Set rule logic'.

Automation in Sentinel

- Automation enabled through SOAR.
    - Automation rules = automatic response to multiple analytic rules.
        - Triggered when incident occurs. Can change status of incident, change severity, assign incdient or tag.
        - Can also run playbook!
    - Playbooks = More advanced, response and remediation actions.
        - Created with Logic Apps!

Playbooks in Sentinel

- Based on Logic Apps.
    - Connect to components like external services.
    - Uses triggers and actions
    - Trigger = some conditions which if satisfied start an event.
    - Action = operation that performs a task in the Logic Apps workflow.
        - Logic App allows for dynamic input to be used.
    - Pre-defined Playbooks exist from Sentinel GitHub.

Incident management in Sentinel

- Workflow: Data connectors (Log Analytics agents) -> Events (Log Analytics workspace) -> Analytics rules (KQL) -> Alerts -> Incidents (multiple alerts).
- Incident entities exist. Some sort of resource tied to an incident.
- An event is evidence.

Sentinel behaviour analytics

- Uses MITRE and other things to sift through logs to deduce possible alerts.
- Entities = IP/user accounts/hosts (data elements).

- Anomaly detection.
- Insights in the investigation graph show Entity Behavior information.
- Activities are shown in the Entity page timeline.

Data normalisation in Sentinel

- ASIM transforms Sentinel logs to user-friendly format.
- ASIM Parser:
    - Built with KQL.
    - Parses at query time.
    - Unifying parsers use source-specific parsers, unique to each schema.
    - We can replace values in KQL query with parameter names.
        - We can then assign the parameter names expected values.
    - We can create our own ASIM parser, and as such standardize logs collected by various devices.
- We can also parse data at ingestion time.
    - Data is then stored in the parsed format.

Query, visualize and monitor data in Sentinel

- Log Analytics stores logs. We can do KQL queries.
- Use saved query -> Query explorer page.
- Create analytics rule -> Microsoft Sentinel Alert.
- KQL is also called *Azure Data Explorer*.
- Workbook templates exist.
    - Workbook uses Markdown for text visualisation.
    - To display data in table -> Grid visualisation.
- Sentinel can be connected to GitHub and Azure DevOps repositories.
- Content Hub accepts Parsers.
- Maximum of 5 repos can be connected to Sentinel.

Sentinel Threat Hunting

Explain threat hunting

- Threat hunting = finding threats that have not been detected.
- Threat hunting starts with a well-structured Hypothesis.
- Threat hunting needs a throughly documented process, for repeatability.
- MITRE ATT&CK exists in Threat Management in Sentinel.

Threat Hunting in Sentinel

- Hunting page in Sentinel has built-in KQL queries and ordered by MITRE techniques.
- One can bookmark KQL query results under Hunting > Bookmarks tab.
- Livestream = query on live data.
- Search jobs
    - Results in Log Analytics, with *_SRCH suffix.
    - Searches analytics log and basic log asynchronously.
- We can restore archived and historical logs.

    - has *_RST suffix.

Threat Hunting with Notebooks

- Logs exist in Log Analytics.
- Sentinel uses API to access the data.
- External libraries `Kqlmagic` and `msticpy` (python) exist for external contact with the API.
    - https://msticpy.readthedocs.io/en/latest/

SC-200 Intended Learning Outcomes (from https://learn.microsoft.com/en-us/credentials/certifications/resources/study-guides/sc-200)

Manage a Security Operations Environment (20–25%)

Configure Settings in Microsoft Defender XDR

- Configure a connection from Defender XDR to a Sentinel workspace
    - https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE
    - **TLDR**
        - Prerequisites: XDR License, Global/Security Administrator role, r/w permission in Sentinel, install XDR in Sentinel Content Hub.
        - Can either connect XDR to Sentinel (Azure Portal), or both to a separate portal (Defender Portal).
        - Do setup in Sentinel for Azure Portal.
            - **Connect Incidents and Alerts**
            - **Connect entitites**
            - **Connect Events**
- Configure alert and vulnerability notification rules
    - https://learn.microsoft.com/en-us/defender-xdr/configure-email-notifications
    - **TLDR**
        - Only users with **Manage security settings** can configure email notifications.
        - As Global/Security Administrator, Goto **Settings > Endpoints > General > Email notification > Add item**
        - Specify rule name, org. name etc, incl. device name y/n?.
        - Enter recipients and save rule.
- Configure Microsoft Defender for Endpoint advanced features
    - https://learn.microsoft.com/en-us/defender-endpoint/advanced-features
    - **TLDR**
        - Edit in **Defender > Settings > Endpoint > Advanced features**
- Configure endpoint rules settings, including indicators and web content filtering
    - https://learn.microsoft.com/en-us/defender-endpoint/web-content-filtering
    - https://learn.microsoft.com/en-us/defender-endpoint/indicator-manage
    - **TLDR**

        - Goto **Settings > Endpoints > Rules**
        - Web content filtering.
            - As Global/Security Administrator, Goto **Settings > Endpoints > General > Advanced Features**
            - Block websites for device groups with policies.
            - Blocks with Defender SmartScreen (Edge) or network protection (the rest).
        - Indicators.
            - As Global/Security Administrator, Goto **Settings > Endpoints > Indicators**
        - Security policies.
            - As Global/Security Administrator, Goto **Endpoints > Configuration management > Endpoint security policies > Create new Policy**
- Manage automated investigation and response capabilities in Microsoft Defender XDR
    - https://learn.microsoft.com/en-us/defender-xdr/m365d-configure-auto-investigation-response
    - **TLDR**
        - As Global/Secrutiy Administrator, Goto **Settings > Endpoints > Device groups under Permissions** to review device group policies.
- Configure automatic attack disruption in Microsoft Defender XDR
    - https://learn.microsoft.com/en-us/defender-xdr/configure-attack-disruption
    - **TLDR**
        - As Global/Secrutiy Administrator, Goto **Settings > Endpoints > Device groups under Permission** to review device group policies.
        - Check Automation levels.

Manage Assets and Environments

- Configure and manage device groups, permissions, and automation levels in Microsoft Defender for Endpoint
    - https://learn.microsoft.com/en-us/defender-endpoint/machine-groups
    - https://learn.microsoft.com/en-us/defender-endpoint/configure-automated-investigations-remediation
    - **TLDR**
        - Goto **Settings > Permissions > Device Groups > Add device group**.
        - Specify name, automation list, include members section (what devices to add).
- Identify and remediate unmanaged devices in Microsoft Defender for Endpoint
    - https://learn.microsoft.com/en-us/defender-endpoint/device-discovery
    - **TLDR**
        - Only discovers devices connected to the corporate network.
        - Onboarded device use either Basic (passive) or Standard (active) device discovery.
        - Network devices are not managed by a sensor, we use onboarded device to scan network ranges instead.
        - Basically, detect devices and onboard them!
- Manage resources by using Azure Arc
    - https://learn.microsoft.com/en-us/azure/azure-arc/overview
    - **TLDR**
        - Basically, Azure Arc enables centralized control of non-Azure and on-prem. resources into the Azure Resource Manager.
            - Servers, Kubernetes, SQL and virtual machines.

- Connect environments to Microsoft Defender for Cloud (by using multi-cloud management)
    - https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-cloud-security-posture-management?source=recommendations
    - **TLDR**
        - Asset Inventory provides an overview of vulnerabilities in cloud assets.
            - Can also perform asset discovery through Asset management options.
        - Use Asset Inventory:
            - Goto **Inventory > Filter > relevant options > Search**.
        - Auto Provisioning: Auto-install feature.
            - Enable in Log Analytics agent.
                - Goto **Environment settings > relevant sub. > Auto provisioning page, On.**
- Discover and remediate unprotected resources by using Defender for Cloud
    - **TODO: Read up on this!**
- Identify and remediate devices at risk by using Microsoft Defender Vulnerability Management
    - https://learn.microsoft.com/en-us/training/modules/use-threat-vulnerability-management-microsoft-defender-for-endpoint/
    - **TLDR**
        - Microsoft Defender Vulnerability Management is for Endpoint.
        - Remediate software vulnerabilities:
            - Goto **Vulnerability Mangement > Recommendations > Click software > Request remedaition > Go through Wizard**.
        - In **Vulnerability Mangement > Inventories** We can see software etc. related to tenant. And request remediation through the Wizard.

Design and Configure a Microsoft Sentinel Workspace

- Plan a Microsoft Sentinel workspace
    - https://learn.microsoft.com/en-us/training/modules/create-manage-azure-sentinel-workspaces/
    - **TLDR**
        - Single tenant with single or regional workspaces OR multi-tenant?
        - Configure Log Analytics.
            - Then add Sentinel to the Log Analytics workspace.
- Configure Microsoft Sentinel roles
    - https://learn.microsoft.com/en-us/training/modules/create-manage-azure-sentinel-workspaces/5-understand-azure-sentinel-permissions-roles
    - **TLDR**
        - Uses RBAC.
        - Roles, Microsoft Sentinel.. Reader/Responder/Contributor/Automation Contributor.
        - To work with Playbooks:
            - Must have Logic App Contributor role.
        - Give Sentinel permission to run Playbooks:
            - Sentinel has special service account to run playbooks.
            - Requires explicit permissions to the resource group of the playbook.
        - Connect data sources to Sentinel:
        - Must have User Write permissions.
    - Guest users assign incidents:
        - Needs Sentinel Responder and Directory Reader role.

    - Create and delete Workbooks:
        - Sentinel Contributor role OR (lesser role AND Azure Monitor role of Workbook Contributor).
- Specify Azure RBAC roles for Microsoft Sentinel configuration
    - https://learn.microsoft.com/en-us/training/modules/create-manage-azure-sentinel-workspaces/5-understand-azure-sentinel-permissions-roles
    - **TLDR**
        - Entire roles for Azure exist:
            - Azure.. Owner/Contributor/Reader.
            - Log Analytics... Contributor/Reader.
- Design and configure Microsoft Sentinel data storage, including log types and log retention
    - https://learn.microsoft.com/en-us/training/modules/create-manage-azure-sentinel-workspaces/6-manage-azure-sentinel-settings
    - https://learn.microsoft.com/en-us/training/modules/create-manage-azure-sentinel-workspaces/7-configure-logs
    - **TLDR**
        - Log retention from 30-730 days.
        - Three primary log types:
            - Analytics logs: Can perform KQL on them. Alerts supported.
            - Basic logs: Specific data types, simple KQL, alerts not supported.
            - Archive logs: Store up to 7 years, cannot query.
        - Can configure logs: Goto **Sentinel Settings > Log Analytics portal > Tables > Manage table > do stuff > save**.
- Manage multiple workspaces by using workspace manager and Azure Lighthouse
    - https://learn.microsoft.com/en-us/training/modules/create-manage-azure-sentinel-workspaces/4-manage-workspaces-across-tenants-using-azure-lighthouse
    - **TLDR**
        - Sentinel Workspace manager = manage multiple workspaces within one or more Azure tenants.
        - Azure Lighthouse = Basically OAuth, can manage mutliple tenants with one account.

Ingest Data Sources in Microsoft Sentinel

- Identify data sources to be ingested for Microsoft Sentinel
    - https://learn.microsoft.com/en-us/training/modules/connect-data-to-azure-sentinel-with-data-connectors/2-ingest-log-data-with-data-connectors
    - **TLDR**
        - Connect to Sentinel Data Connectors.
            - Included in Content Hub Solutions in Sentinel.
        - Data sources:
            - XDR (Identity/Endpoint/Office 365/Cloud Apps)
            - Azure Services (Entra ID/Activity/Entra ID Protection/DDoS etc.)
            - Custom connectors through Log Analytics Data Collector API.
            - Send any logs through Sentinel Logstash plugin.
            - Common Event Format (CEF) (Industry-standard).
            - Syslog connector (Linux).
        - Syslog and CEF requires host to be deployed in dedicated Azure VM.

- Implement and use Content hub solutions
  - https://learn.microsoft.com/en-us/azure/sentinel/sentinel-solutions-deploy?tabs=azure-portal
  - **TLDR**
    - All included in the **Sentinel > Content management > Content hub**
    - Has many pre-defines contents that can be installed using auto-provisioning.
- Configure and use Microsoft connectors for Azure resources, including Azure Policy and diagnostic settings
  - https://learn.microsoft.com/en-us/training/modules/connect-microsoft-services-to-azure-sentinel/
  - **TLDR**
    - Done through Data Connectors.
    - Activate Azure Activity (which uses Azure Policy):
      - Goto **Sentinel > Content Management > Content Hub > Type Azure Activity > Select Azure Activity > Select Install > Select Azure Activity Data connector > Open connector page > In Instructions/Configuration > Connect your subscriptions.. Launch Azure Policy Assignment Wizard > In Basics select your Azure Sub. > In Parameters chose workspace > in Remediation > Create a remediation task > Finish**.
- Configure bidirectional synchronization between Microsoft Sentinel and Microsoft Defender XDR
  - https://learn.microsoft.com/en-us/defender-xdr/microsoft-365-defender-integration-with-azure-sentinel
  - **TLDR**
    - Add XDR Connector in Content Hub. This will make a bi-directional synchronization between Defender and XDR.
- Plan and configure Syslog and Common Event Format (CEF) event collections
  - https://learn.microsoft.com/en-us/training/modules/connect-common-event-format-logs-to-azure-sentinel/
  - **TDLR**
    - Need Log Analytics agent on either host or Azure VM connected to host.
    - Goto **Sentinel > Configuration > Data Connectors > Select CEF > Copy "sudo wget ..." command > run on Linux VM**.
  - https://learn.microsoft.com/en-us/training/modules/connect-syslog-data-sources-to-azure-sentinel/
  - **TLDR**
    - Need Log Analytics agent on either host or Azure VM connected to host.
    - Different steps to setup Syslog if its a Azure Linux VM or not.
    - Configure Data Collection Rule (DCR):
      - Goto **Data collection rule > Data Sources > Add data source > Config + Data sources + Linux syslog > Minimum log level > Save**.
- Plan and configure collection of Windows Security events by using data collection rules, including Windows Event Forwarding (WEF)
  - https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-rule-overview
  - https://learn.microsoft.com/en-us/training/modules/connect-syslog-data-sources-to-azure-sentinel/
  - **TLDR**
    - Uses the Azure Monitor pipeline.

        - DCR is used in Azure Monitor to filter the ingested data.
            - What data to collect, how to transform it (KQL) and where to send it.
- Configure threat intelligence connectors, including platform, TAXII, upload indicators API, and MISP
    - https://learn.microsoft.com/en-us/training/modules/connect-threat-indicators-to-azure-sentinel/
    - **TLDR**
        - TAXII threat connector (2.0/2.1)
            - Goto **Data connectors > Threat intelligence - TAXII > Open connector > Specify requirements > Add**.
        - Threat Intelligence Connector
            - Done through MS Graph Security API.
            - We connect Sentinel to other TI platform.
                - Register an app in Entra ID to get credentials.
        - TI data can be accessed in ThreatIntelligenceIndicator.
- Create custom log tables in the workspace to store ingested data
    - https://learn.microsoft.com/en-us/azure/sentinel/data-transformation
    - **TLDR**
        - Log Analytics stores all data.
        - With DCR we can create customized tables.

Configure Protections and Detections (15–20%)

Configure Protections in Microsoft Defender Security Technologies

- Configure policies for Microsoft Defender for Cloud Apps
    - https://learn.microsoft.com/en-us/training/modules/microsoft-cloud-app-security/
    - **TLDR**
        - We can configure AC through the Conditional Access App Control.
        - Entra ID AC integrated if used already.
- Configure policies for Microsoft Defender for Office 365
    - https://learn.microsoft.com/en-us/training/modules/m365-threat-remediate/
    - **TLDR**
        - Configure policies in the Defender portal.
        - Safe Attachments exist, protects against malware.
        - Safe Links exists.
        - Anti-phishing policies exist as well.
- Configure security policies for Microsoft Defender for Endpoints, including attack surface reduction (ASR) rules
    - https://learn.microsoft.com/en-us/training/modules/implement-windows-10-security-enhancements-with-microsoft-defender-for-endpoint/3-enable-attack-surface-reduction-rules?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.sc-200-mitigate-threats-using-microsoft-defender-for-endpoint
    - https://learn.microsoft.com/en-us/training/modules/deploy-microsoft-defender-for-endpoints-environment/6-create-manage-roles-for-role-based-access-control
    - https://learn.microsoft.com/en-us/training/modules/deploy-microsoft-defender-for-endpoints-environment/7-configure-device-groups
    - https://learn.microsoft.com/en-us/training/modules/configure-manage-automation-microsoft-defender-for-endpoint/4-configure-automated-investigation-remediation-capabilities?ns-

enrollment-type=learningpath&ns-enrollment-id=learn.wwl.sc-200-mitigate-threats-using-microsoft-defender-for-endpoint

- **TLDR**
  - ASR
    - Available for Windows OS machines.
    - Config in Endpoint, Goto **Settings > Endpoint Security > ASR > config/create ASR**.
    - Works well with group policies as well.
  - RBAC
    - As Sec/Global Admin Goto **Defender Portal > Settings > Endpoints > Permissions > Roles > Turn on roles > add items > add permissions to role > assign role to Entra Sec. group**.
  - Device Groups
    - As Sec/Global Admin Goto **Defender Portal > Settings > Endpoints > Permissions > Device Groups > Add device group > Config automation settings and rules to match devices to group > config users that can access device group (must be user assigned to RBAC group)**.
  - Automated investigation and remediation exists.
    - To turn on Goto **Settings > Endpoints > Advanced features > Turn on auto. investigation and remediation**.

- Configure cloud workload protections in Microsoft Defender for Cloud
  - https://learn.microsoft.com/en-us/azure/defender-for-cloud/workload-protections-dashboard
  - https://learn.microsoft.com/en-us/training/paths/sc-200-mitigate-threats-using-azure-defender/
  - **TLDR**
    - Workload protections dashboard exists in Defender for Cloud.
    - Basically, it logs data from cloud/hybrid/on-prem resources and makes it secure through the service.
    - Has tons of different subscriptions for servers/DNS/SQL etc.

Configure Detection in Microsoft Defender XDR

- Configure and manage custom detections
  - https://learn.microsoft.com/en-us/defender-xdr/custom-detection-rules
  - **TLDR**
    - Custom detections can be made with KQL.
      - Query must return Timestamp and ReportId, and one other ID for device or similar etc.
      - Select **Create detection rule** and configure it.
        - Configure frequency on how often it should run.
        - Choose which entity is the impacted one, i.e. if rule hits, what is the impacted entity?
        - Specify actions (device = run AV, isolate etc.) (files = block / quarantine) (users = isolate etc.)
        - Set rule scope. (All devices / device groups).
    - We can mage existing ones in **Hunting > Custom detection rules**.
- Configure alert tuning
  - https://learn.microsoft.com/en-us/defender-xdr/investigate-alerts?tabs=settings

    - **TLDR**
        - Goto **Settings > Defender XDR > Alert Tuning > Add new rule > specify which service (Enpoint/Office 365 etc) > add conditions that should supress the alert > Select either Hide/Resolve alert**.
- Configure deception rules in Microsoft Defender XDR
    - https://learn.microsoft.com/en-us/defender-xdr/configure-deception
    - **TLDR**
        - Deception basically adds decoy accounts and hosts in the tenant.
        - Turn on deception Goto **Settings > Endpoints > Advanced Features under General > Toggle on Deception capabilities**.
        - To create/modify deception rules:
            - Goto **Settings > Endpoints > Add deception rule > Config name, lure types > Add devices lure should belong to**.

Configure Detections in Microsoft Sentinel

- Classify and analyze data by using entities
    - https://learn.microsoft.com/en-us/azure/sentinel/entities
    - **TLDR**
        - Entities are special pieces of data recognized by Sentinel.
            - Includes IP, Hosts, Accounts, URLs etc.
        - Strong identifiers exist = can always uniquely identify an entity.
        - Weak identifiers exist = can sometimes uniquely identify an entity.
- Configure scheduled query rules, including KQL
    - https://learn.microsoft.com/en-us/azure/sentinel/create-analytics-rules?tabs=azure-portal#get-started-creating-a-scheduled-query-rule
    - **TLDR**
        - First we define the rule logic = KQL.
        - Goto **Azure Portal > Configuration > Analytics > Create > Scheduled query rule**.
            - Config name etc.
            - Add KQL rule logic.
            - Determine scope and schedule of query.
- Configure near-real-time (NRT) query rules, including KQL
    - https://learn.microsoft.com/en-us/azure/sentinel/create-nrt-rules?tabs=azure-portal
    - **TLDR**
        - Goto **Azure Portal > Configuration > Analytics > +Create > NRT query rule**.
            - Same configuration as scheduled query rules.
- Manage analytics rules from Content hub
    - https://learn.microsoft.com/en-us/training/modules/manage-content-microsoft-sentinel/2-use-solutions-from-content-hub?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.sc-200-create-detections-perform-investigations-azure-sentinel
    - https://learn.microsoft.com/en-us/azure/sentinel/sentinel-solutions-deploy?tabs=azure-portal
    - **TLDR**
        - Content hub can be used to install functionality/content automatically to products in Sentinel.
- Configure anomaly detection analytics rules
    - https://learn.microsoft.com/en-us/azure/sentinel/work-with-anomaly-rules

    - https://learn.microsoft.com/en-us/training/modules/use-entity-behavior-analytics-azure-sentinel/4a-use-anomaly-detection-analytical-rule-templates?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.sc-200-create-detections-perform-investigations-azure-sentinel
    - **TLDR**
        - Goto **Sentinel > Analytics > Rule templates > Filter for Anomaly templates**.
            - Configure rule.
            - Description, data sources, parameters, theshold, rule frequency.
- Configure the Fusion rule
    - https://learn.microsoft.com/en-us/azure/sentinel/configure-fusion-rules
    - **TLDR**
        - Goto **Sentinel > Analytics > Active rules**.
        - Under Advanced Multistage Attack Detection we can check the status of Fusion rules.
        - We can also configure source signals of the fusion rule.
- Query Microsoft Sentinel data by using ASIM parsers
    - https://learn.microsoft.com/en-us/training/modules/data-normalization-microsoft-sentinel/5-create-asim-parser?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.sc-200-create-detections-perform-investigations-azure-sentinel
    - **TLDR**
        - Advanced Security Information Model (ASIM) uses source-specific parsers instead of tables in their queries.
            - Enables greater detail of data from specific sources.
        - Create ASIM:
            - Collect Sample logs.
            - Identify schemas.
            - Map source fields to indentified schemas.
            - Develop ASIM parser(s) for each schema.
            - Deploy in parser in Sentinel workspace.
- Manage and use threat indicators
    - https://learn.microsoft.com/en-us/training/modules/connect-threat-indicators-to-azure-sentinel/
    - **TLDR**
        - TAXII 2.0 and 2.1 data sources can be connected.
            - Goto **Data connectors > Threat Intelligence - TAXII > Open connector**.
                - Configure and Add.
        - Connect Sentinel to third-party TI-platform.
            - Register an app in Entra ID to get app ID, sectret and tenant ID.
            - Config API permissions for the registered app.
            - Admin consent to app: **Microsoft Entra ID > App registrations > app name > View API Permissions > Grant admin consent for tenant name**.
            - Configure TI product to integrate with Graph Security TI API (feed app ID from sentinel).
            - Goto **Microsoft Sentinel > Data connectors > select the Threat Intelligence Platforms (Preview) connector > Open connector page > Connect**
        - TI indicators can be queried with KQL, found in table ThreatIntelligenceIndicator.

Manage Incident Response (35–40%)

Respond to Alerts and Incidents in Microsoft Defender XDR

- Investigate and remediate threats to Microsoft Teams, SharePoint Online, and OneDrive
- Investigate and remediate threats in email by using Microsoft Defender for Office 365
    - https://learn.microsoft.com/en-us/training/modules/m365-threat-remediate/automate-investigate-remediate
    - **TLDR**
        - Automated Investigation and Response (AIR) exists, playbooks that can be launched directly if an alert is triggered or manually from the Explorer view.
            - Remediations include delete email messages or clusters, block URL, turn off external email forwarding or turn off delegation.
            - AIR can be configured as Global/Sec Admin.
- Investigate and remediate ransomware and business email compromise incidents identified by automatic attack disruption
    - https://learn.microsoft.com/en-us/defender-xdr/automatic-attack-disruption
    - **TLDR**
        - Automated response action can contain devices and users as to remediate above incidents.
- Investigate and remediate compromised entities identified by Microsoft Purview data loss prevention (DLP) policies
    - https://learn.microsoft.com/en-us/training/modules/respond-to-data-loss-prevention-alerts-microsoft-365/3-investigate-data-loss-prevention-alerts-microsoft-365-compliance
    - **TLDR**
        - View Alerts Goto **Purview > Solutions > DLP > Alerts**
            - One can also filter alerts.
            - Select alert.
                - Events tab show events related to alert.
                - Sensitive Info Types: Details on information detected in the content.
            - Manage Alert.
                - Active/Investigating/Dismissed/Resolved
- Investigate and remediate threats identified by Microsoft Purview insider risk policies
    - https://learn.microsoft.com/en-us/training/modules/m365-compliance-insider-manage-insider-risk/
    - **TLDR**
        - One can view alerts in the portal.
        - One can filter alerts based on status, severity, time detected and policy.
        - Case overview: Shows details of each case.
            - Can have multiple alerts.
            - User activity view
            - Content explorer.
            - One can escalate for investigation and resolve it.
- Investigate and remediate alerts and incidents identified by Microsoft Defender for Cloud
    - https://learn.microsoft.com/en-us/training/modules/remediate-azure-defender-security-alerts/3-remediate-alerts
    - **TLDR**
        - View alerts: **Cloud overview > Defender for Cloud tab > Security Alerts**.
        - Take action tab

            - Mitigate the threat: Manual remediation steps for alert.
            - Prevent future attacks: Security recommendations.
            - Trigger automated response: Trigger logic app.
            - Supress similar alerts.
- Investigate and remediate security risks identified by Microsoft Defender for Cloud Apps
    - https://learn.microsoft.com/en-us/training/modules/microsoft-cloud-app-security/
    - **TLDR**
        - Remediations:
            - Prevent data exfiltration.
            - Protect downloaded cloud files with Azure Information Protection (AC).
            - Prevent upload for unlabeled files.
            - Monitor users for compliance.
            - Block access/custom activities.
        - Azure Information Protection:
            - First discover data in Cloud Apps.
            - Classify data discovered (Personal/Public/General/Confidential/Highly Confidential)
            - Enable Azure Information Protection under **Cloud Apps > Settings > Azure Information Protection > Automatically scan new files for Azure Information Protection classification labels**
            - File policies under **Cloud Apps > Control > Policies > Create Policy > File Policy**
- Investigate and remediate compromised identities in Microsoft Entra ID
    - https://learn.microsoft.com/en-us/training/modules/protect-identities-with-aad-idp/
    - **TLDR**
        - Two risks exist
            - User Risk: Unusual behaviour/leaked credentials.
            - Sign-in risk: Unfamiliar sign-in/atypical travel.
        - Remediation workflow
            - Define a Risk Policy: Can have automated response.
            - Or let administrators decidec when risk policy detects.
        - Remediation methods
            - Self-remediation (let user do it)
            - Reset passwords manually.
            - Rismiss user risk
            - Block users through risk policy.
- Investigate and remediate security alerts from Microsoft Defender for Identity
    - https://learn.microsoft.com/en-us/training/modules/m365-threat-safeguard/review-compromised-accounts
    - **TLDR**
        - Each alert has an activity log.
        - Can be integrated with Cloud Apps and Endpoint.
- Manage actions and submissions in the Microsoft Defender portal
    - https://learn.microsoft.com/en-us/training/modules/mitigate-incidents-microsoft-365-defender/7-use-action-center
    - **TLDR**
        - We can view pending and completed remediation actions for devices, email and identities.
        - Submission portal exists.

        - Can submit email messages, URLs and attachment to MS for scanning.

Respond to Alerts and Incidents Identified by Microsoft Defender for Endpoint

- Investigate timeline of compromised devices
    - https://learn.microsoft.com/en-us/defender-endpoint/device-timeline-event-flag
    - **TLDR**
        - Open an alert, go to the device and inspect the timeline.
        - Alternatively, go directly to the device page and timeline tab.
- Perform actions on the device, including live response and collecting investigation packages
    - https://learn.microsoft.com/en-us/defender-endpoint/respond-machine-alerts
    - https://learn.microsoft.com/en-us/defender-endpoint/live-response
    - **TLDR**
        - Go to device page, select **Collect investigation package** (.zip file).
        - Live response: Device inventory, open device, initiate live response session.
- Perform evidence and entity investigation
    - https://learn.microsoft.com/en-us/training/modules/perform-evidence-entities-investigations-microsoft-defender-for-endpoint/
    - **TLDR**
        - Files: Go to file page, see prevalance, incidents, observed in organization etc. Deep file analysis executes file in secure environment.
        - Accounts: Has a page, can see user details, alerts, observed in organization.
        - IPs: IP in organization, prevalance, devices observed with IP.
        - Domains: URL in organization, recent devices with URL.
- Enrich investigations by using other Microsoft tools
    - **TLDR**
        - KQL?
- Investigate threats by using unified audit log
    - https://learn.microsoft.com/en-us/training/modules/investigate-threats-using-audit-in-microsoft-365-defender-microsoft-purview-standard/5-search-audit-log
    - **TLDR**
        - UAL contains logs from a ton of MS 365 services.
        - We search it through audit log search: Specify date interval, activities, users, files/folders/sites/all to search.
        - We can view results (up to 50k rows): Date, IP, user, activity, item, details.
        - Export results to a .csv file.
- Investigate threats by using Content Search
- Perform threat hunting by using Microsoft Graph activity logs

Manage Incidents in Microsoft Sentinel

- Triage incidents in Microsoft Sentinel
    - https://learn.microsoft.com/en-us/azure/sentinel/investigate-incidents
    - **TLDR**
        - Conduct investigations from the **Sentinel > Threat management > Incidents** page.
        - **Sentinel Responder** role is required to investigate incidents.
        - Clicking on Actions of an incident can:

        - Investigate
        - Run playbook
        - Create automation rule
    - We can view Logs (KQL), Tasks and Activity logs (things done already).
    - Each incident has:
        - Incident timeline.
        - Similar incidents.
        - Entities.
    - Investigation graph exists to graphically inspect incident.
- Investigate incidents in Microsoft Sentinel
    - Same as above.
- Respond to incidents in Microsoft Sentinel
    - Same as above.

Configure Security Orchestration, Automation, and Response (SOAR) in Microsoft Sentinel

- Create and configure automation rules
    - https://learn.microsoft.com/en-us/training/modules/automation-microsoft-sentinel/3-create-automation-rules
    - **TLDR**
        - Create under **Sentinel > Configuration > Automation > Create > Automation rule**
        - Configure
            - When the rule should be triggered (what incidents).
            - Conditions to be met and what actions should be taken.
            - Actions to take (change status/severity, assign user to incident, add tag to incident).
- Create and configure Microsoft Sentinel playbooks
    - https://learn.microsoft.com/en-us/azure/sentinel/automation/create-playbooks?tabs=azure-portal%2Cconsumption
    - **TLDR**
        - Goto **Sentinel > Configuration > Automation > Create > Playbook with X**.
            - X = incident trigger.
            - X = alert trigger.
            - X = entity trigger.
        - Add actions to playbook.
            - Add actions/logical conditions/loops/switch case conditions.
- Configure analytic rules to trigger automation
    - https://learn.microsoft.com/en-us/azure/sentinel/create-manage-use-automation-rules?tabs=azure-portal%2Conboarded
    - **TLDR**
        - Automation rules are triggered when incidents are created/updated or alerts are created.
- Trigger playbooks manually from alerts and incidents
    - Go to an incident/alert and simply "Run Playbook".
- Run playbooks on on-premises resources
    - Can't find any information on it...
        - Link it through a VM, make a connector to Log Analytics workspace. Then its another entity. (?)

Perform Threat Hunting (15–20%)

Hunt for Threats by Using KQL

- Identify threats by using Kusto Query Language (KQL)
  - EZ.
- Interpret threat analytics in the Microsoft Defender portal
  - Goto **Defender > Threat Intelligence > Threat analytics**.
  - EZ.
- Create custom hunting queries by using KQL
  - Goto **Sentinel > Threat management > Hunting > Queries > New query**.
  - Make KQL.

Hunt for Threats by Using Microsoft Sentinel

- Analyze attack vector coverage by using the MITRE ATT&CK in Microsoft Sentinel
  - https://learn.microsoft.com/en-us/azure/sentinel/mitre-coverage
  - **TLDR**
    - Attack coverage found under **Sentinel > Threat management > MITRE ATT&CK**.
    - See incident attack vector: view under **Tactics and techniques**.
- Customize content gallery hunting queries
  - https://learn.microsoft.com/en-us/azure/sentinel/hunting?tabs=azure-portal
  - **TLDR**
    - Goto **Sentinel > Threat management > Hunting > Queries**
      - Contains all hunting queries install with security solutions from Content Hub.
      - We can also create queries from here.
- Use hunting bookmarks for data investigations
  - https://learn.microsoft.com/en-us/azure/sentinel/bookmarks
  - **TLDR**
    - Found in **Sentinel > Threat management > Hunting > Bookmarks**
    - Saves results from Log Analytics KQL queries. Can also add notes and tags to them.
    - To save goto **Sentinel > Threat management > Hunting > Hunting**
      - Run a query, view results. Then Add bookmark.
- Monitor hunting queries by using livestream
  - https://learn.microsoft.com/en-us/azure/sentinel/livestream
  - **TLDR**
    - Found in **Sentinel > Threat management > Hunting > Livestream**
    - To make a livestream goto **Sentinel > Threat management > Hunting > Queries**
      - Right click on query and select Add to livestream.
      - Then goto Livestream tab and select New Livestream.
        - Modify query selected from previous step OR create your own query.
- Retrieve and manage archived log data
  - https://learn.microsoft.com/en-us/azure/sentinel/restore
  - **TLDR**
    - Goto **Sentinel > General > Search > Restore > Saved Searches > Restore**
      - Configure time range and table, then select restore.
    - Can view the data in the Restoration tab.

        - Can query it like any other Log Analytics logs.
- Create and manage search jobs
    - https://learn.microsoft.com/en-us/azure/sentinel/search-jobs?tabs=azure-portal
    - **TLDR**
        - We can do search jobs on all logs (Archived, Analytics and Basic) up to seven years old.
        - Do by **Sentinel > General > Search > Search in Search bar and click Start > Enter KQL > toggle Search job mode on**
            - Filter time range
            - Select Search Job, save as a table name and then Run a search job.
        - Results are found under **Saved Searches**.
            - We can add filters in the results.

Analyze and Interpret Data by Using Workbooks

- Activate and customize Microsoft Sentinel workbook templates
    - https://learn.microsoft.com/en-us/azure/sentinel/monitor-your-data?tabs=azure-portal
    - **TLDR**
        - Create workbook from template
            - Goto **Sentinel > Threat management > Workbooks > Templates**
                - Click on a template, hit save and click View saved workbook.
                - We can edit the workbooks.
- Create custom workbooks that include KQL
- https://learn.microsoft.com/en-us/azure/sentinel/monitor-your-data?tabs=azure-portal
    - **TLDR**
    - Create new workbook
        - Goto **Sentinel > Threat management > Workbooks > Templates > Add Workbook**
            - Edit the workbook, build query (set Data Source to logs and Resource Type to Log Analytics).
- Configure visualizations
    - https://learn.microsoft.com/en-us/azure/azure-monitor/visualize/tutorial-logs-dashboards
    - https://learn.microsoft.com/en-us/azure/sentinel/get-visibility
    - **TLDR**
        - Overview page exists under General.

Other useful links

- Other notes
    - https://github.com/OneEqualsOne/Azure-Learning-Materials/blob/main/SC-200/SC-200 Notes.md
- SIEM Cert for Sentinel
    - https://learn.microsoft.com/en-us/credentials/applied-skills/configure-siem-security-operations-using-microsoft-sentinel/
- Roles in Sentinel

    - https://learn.microsoft.com/en-us/azure/sentinel/roles

Practise for Exam

URL

- https://www.examtopics.com/exams/microsoft/sc-200
- https://www.itexams.com/exam/SC-200?

Q&A

- Exclude certain servers from agentless scanning.
    - Create an exclusion tag when using Azure Defender for Servers.
    - Requires Defender for Servers Plan 2.
- Generate alerts in Cloud Apps for external sharing of confidential files.
    - Enable file monitoring in Cloud Apps.
    - Add automatic scan of new files for Azure Information Protection classification labels and content inspection warnings.
- Live Shell connection to Onboarded devices in Defender 365.
    - Create RBAC
    - Enable Live Response.
- Investigate Teams chats related to a user.
    - Location: Exchange mailboxes
    - Keywords: Kind
- Collect investigation packages
    - Can be collected from onboarded Windows/Linux/Mac hosts.
- View recommendations to resolve alerts in Azure Security Center:
    - Select 'Mitigate the threat' under Security Alerts.
- Manage Azure Defender Key Vault
    - One can modify Key Vault firewall to reduce risk of adversary entering from bad IP.
- Enable email notifications in Defender for Cloud
    - **Environment settings -> click subscription -> Email notifications**
- Alert suppression in Endpoint can be made on: (1) this device or (2) the entire organization (not device groups).
- Remediate unsanctioned apps in Cloud Apps
    - Select app, tag as unsanctioned, generate block script and run the script on the source appliance.