

Copilot for Security – User Personas, 1P Plugin Capabilities & Sample Prompts Documentation

The roles & responsibilities of the 6 user personas identified along with the assistance that Copilot for Security can provide in their daily tasks are briefly encapsulated below –

Personas	Role	Responsibility	Products	Assistance
Security Champions (Threat Intel Analyst, CISO)	Members of DevOps teams and executives with a particular interest in security. They act as intermediaries between the DevOps and Security teams.	Provide knowledge bases to drive the creation of threat models, enabling them to assist their teams in improving security posture.	Defender, USX, MDTI, Intune, Entra, Purview	"Copilot for Security" can provide real-time threat intelligence and automated threat modeling tools, enabling Security Champions to quickly identify and mitigate potential security risks within their DevOps processes.
Security Operations Center (SOC Teams)	Responsible for monitoring, detecting, and responding to security incidents.	Implement automated management, standardized patching, antivirus, policy enforcement, and application protection across all devices. This reduces the need for manual intervention and improves incident response times.	Defender, USX, MDTI, Intune, Entra, Purview	The product can enhance SOC teams' capabilities by offering advanced threat detection, automated incident response, and continuous monitoring. This helps in reducing the time to detect and respond to

				security incidents.
Cloud Security Architects (Network Security Admin, Cloud Security Admin)	Design and implement security architecture for cloud environments.	Adopt a Zero Trust architecture approach, ensuring every access attempt is verified. This increases security and allows users to work from anywhere with any device type.	MDC, MDEASM, Azure WAF, Azure Firewall	"Copilot for Security" can assist in designing and implementing secure cloud architectures by providing best practices, compliance checks, and automated security assessments. This ensures that cloud environments are secure and compliant with industry standards.
Privileged Access Managers (Identity Admin)	Manage and secure privileged access to critical systems and data.	Implement a privileged access strategy that balances security and productivity, ensuring that security controls do not impede user workflows.	Entra	The product can help manage and secure privileged access by offering tools for monitoring and controlling access to critical systems. It can also provide automated alerts and reports on any suspicious activities related to privileged accounts.
Governance, Risk, and Compliance (GRC) Teams	Ensure that the organization adheres to regulatory	Develop and document security posture, identify risks,	MDTI, Defender, Purview	"Copilot for Security" can streamline compliance

<i>(Data Security Admin, Data Compliance Admin, Data Governance Admin)</i>	requirements and manages risks effectively.	and implement compliance measures. Use tools like Microsoft Secure Score to track progress and compliance status.		management by providing automated compliance checks, risk assessments, and reporting tools. This helps GRC teams ensure that the organization adheres to regulatory requirements and manages risks effectively.
<i>IT Operations Teams (IT Admins)</i>	Manage the day-to-day operations of IT infrastructure.	Optimize network for cloud connectivity, implement device compliance policies, and ensure that security measures do not hinder productivity.	Intune, Entra, Autopatch, W365	The product can assist IT operations teams by offering tools for network optimization, device compliance, and security policy enforcement. This ensures that security measures are integrated seamlessly into the IT infrastructure without hindering productivity.

Demo scenario of standalone experience for each user persona –

Personas	Scenario	Prompts	Responses
Security Champion	A Security Champion is tasked with promoting secure coding practices within their development team.	"Copilot for Security, can you provide a checklist of secure coding practices for our team?"	"Sure! Here is a checklist: 1. Validate input data. 2. Use parameterized queries. 3. Implement proper error handling. 4. Use HTTPS. 5. Regularly update dependencies."
		"Can you give me an example of how to validate input data in Python?"	Certainly! Here is an example: <pre>import re; def validate_input(user_input): if re.match('[a-zA-Z0-9_]*\$', user_input): return True else: return False</pre>
		"Thanks! Can you also provide a brief explanation of why input validation is important?"	"Input validation is crucial to prevent malicious data from being processed by your application, which can lead to security vulnerabilities like SQL injection and cross-site scripting (XSS)."
Security Operations Center (SOC) Teams	A SOC team member is investigating a potential phishing attack.	"Copilot for Security, how can I identify phishing emails in our logs?"	"Look for indicators such as suspicious sender addresses, unexpected attachments, and links to unfamiliar domains."
		"Can you show me an example of a suspicious email log entry?"	"Sure! Example: From: suspicious@phish.com; Subject: Urgent! Update your account; Attachment: invoice.zip; Link: http://malicious-site.com"
		"What steps should I take if I confirm a phishing attack?"	"1. Isolate affected systems. 2. Notify impacted users. 3. Block malicious domains and IPs."

			<p>4. Conduct a thorough investigation.</p> <p>5. Report the incident to relevant authorities."</p>
Cloud Security Architects	A Cloud Security Architect is designing a secure architecture for a new cloud application.	Copilot for Security, what are the best practices for securing a cloud application?"	<p>"Best practices include:</p> <ol style="list-style-type: none"> 1. Use IAM roles and policies. 2. Encrypt data at rest and in transit. 3. Implement network segmentation. 4. Regularly audit and monitor resources. 5. Use multi-factor authentication (MFA)."
		"Can you provide an example of an IAM policy for read-only access to an S3 bucket?"	<p>"Certainly! Example:</p> <pre>{ 'Version': '2012-10-17', 'Statement': [{ 'Effect': 'Allow', 'Action': 's3:GetObject', 'Resource': 'arn:aws:s3:::example-bucket/*' }] }</pre>
		"Thanks! How can I ensure data encryption in transit for my application?"	<p>"Use TLS/SSL certificates to encrypt data transmitted between clients and servers. Ensure all endpoints are configured to use HTTPS."</p>
Privileged Access Managers	A Privileged Access Manager is reviewing access controls for critical systems.	"Copilot for Security, what are the key principles of privileged access management?"	<p>"Key principles include:</p> <ol style="list-style-type: none"> 1. Least privilege. 2. Just-in-time access. 3. Regular access reviews. 4. Strong authentication. 5. Session monitoring and recording."
		"Can you help me create a policy for least privilege access?"	<p>"Sure! Policy: 'Access to critical systems should be granted only to users who need it to perform their job functions. Access should be limited to the minimum necessary permissions.'"</p>
		"What tools can I use to monitor privileged sessions?"	<p>"You can use tools like CyberArk, BeyondTrust, and Thycotic to monitor and record privileged sessions."</p>

Governance, Risk, and Compliance (GRC) Teams	A GRC team member is preparing for an upcoming compliance audit.	"Copilot for Security, what are the common compliance frameworks we need to consider?"	"Common frameworks include: 1. GDPR. 2. HIPAA. 3. PCI-DSS. 4. ISO 27001. 5. NIST."
		"Can you provide a checklist for GDPR compliance?"	"Sure! GDPR checklist: 1. Obtain user consent. 2. Ensure data portability. 3. Implement data protection by design. 4. Conduct regular data protection impact assessments. 5. Report data breaches within 72 hours."
		"What documentation should I prepare for the audit?"	"Prepare documentation such as: 1. Data protection policies. 2. Records of processing activities. 3. Incident response plans. 4. Employee training records. 5. Audit logs and reports."
IT Operations Teams	An IT Operations team member is tasked with patching vulnerabilities in the company's software.	"Copilot for Security, how can I identify vulnerabilities in our software?"	"Use vulnerability scanning tools like Nessus, Qualys, or OpenVAS to identify vulnerabilities."
		"Can you show me an example of a vulnerability scan report?"	"Sure! Example: Vulnerability: CVE-2021-34527; Severity: Critical; Affected Systems: Windows Server 2019; Description: PrintNightmare vulnerability; Recommended Action: Apply patch KB5004945"
		"What are the best practices for patch management?"	"Best practices include: 1. Regularly schedule patching. 2. Test patches in a staging environment."

			<p>3. Prioritize critical patches.</p> <p>4. Maintain an inventory of systems.</p> <p>5. Document and review patching processes."</p>
--	--	--	---

Persona-specific list of few sample prompts to experiment with –

Personas	Sample Prompts
Security Champions	Generate a security checklist for new software deployments
	Create a guide for secure coding practices in Python
	List common vulnerabilities in web applications and how to mitigate them
	Draft a security awareness email for developers
	Provide examples of secure API design
	Generate a report on the latest OWASP Top 10 vulnerabilities
	Create a training module on secure code reviews
	List best practices for handling sensitive data in applications
	Generate a template for a security incident report
	Create a guide for secure configuration of development environments
Security Operations Center (SOC) Teams	Generate a daily threat intelligence report
	Create a playbook for responding to phishing attacks
	List common indicators of compromise (IOCs) for ransomware
	Generate a script to automate log analysis for suspicious activity
	Create a guide for setting up SIEM alerts
	List best practices for incident response
	Generate a report on recent security incidents and their resolutions
	Create a checklist for post-incident analysis
	Generate a guide for monitoring network traffic for anomalies
	List common attack vectors and how to detect them
Cloud Security Architects	Generate a security architecture diagram for a multi-cloud environment
	Create a guide for securing AWS S3 buckets
	List best practices for identity and access management in Azure

	Generate a checklist for securing Kubernetes clusters
	Create a guide for implementing zero trust architecture in the cloud
	List common cloud security misconfigurations and how to avoid them
	Generate a report on cloud security compliance requirements
	Create a guide for encrypting data at rest and in transit in GCP
	List best practices for securing serverless applications
	Generate a template for a cloud security policy
Privileged Access Managers	Generate a guide for implementing least privilege access
	Create a checklist for auditing privileged accounts
	List best practices for managing privileged access in Active Directory
	Generate a report on recent privileged access breaches and lessons learned
	Create a guide for setting up multi-factor authentication for privileged accounts
	List common risks associated with privileged access and how to mitigate them
	Generate a template for a privileged access management policy
	Create a guide for monitoring and logging privileged access activities
	List best practices for securing remote access for privileged users
	Generate a report on the effectiveness of current privileged access controls
Governance, Risk, and Compliance (GRC) Teams	Generate a compliance checklist for GDPR
	Create a guide for conducting a risk assessment
	List best practices for maintaining PCI DSS compliance
	Generate a report on the organization's current risk posture
	Create a template for a security policy document

	List common compliance requirements for healthcare organizations
	Generate a guide for implementing a risk management framework
	Create a checklist for preparing for a security audit
	List best practices for managing third-party risk
	Generate a report on recent changes in cybersecurity regulations
IT Operations Teams	Generate a guide for patch management best practices
	Create a checklist for securing network devices
	List best practices for endpoint security
	Generate a report on the current status of system updates
	Create a guide for implementing network segmentation.
	List common vulnerabilities in legacy systems and how to address them.
	Generate a template for a system hardening policy.
	Create a guide for setting up secure remote access.
	List best practices for backup and disaster recovery.
	Generate a report on the effectiveness of current security controls.

1P plugin capabilities & feature-specific sample prompts –

A) Defender XDR

Capabilities

Investigate and respond to threats in a guided experience

Summarize an incident, assess its impact, provide actionable recommendations for faster investigation and remediation, and, lastly, generate a post-response activity report.

Upskill security talent

Unlock new skills that allow analysts at all levels to complete complex tasks like threat hunting, reverse engineering of malware, and more.

Assess risks with AI-driven threat intelligence

Inquire in natural language about emerging threats and your organization's exposure and gain contextualized insights for rapid response to new and evolving threats.

Sample Prompts

Threat Actor Profiles and Activities

- Summarize recent threat intelligence.
- What threat actors have been active lately?
- Can you tell me about more specific threat intelligence related to the <Financial services industry>?
- It was observed that <Manatee Tempest> was active in this event. Provide a summary of the actor and their intersection with ransomware.

KQL Queries and Log Analysis

- Can you help me with creating a KQL to search for relevant public IOCs from <Evilproxy> Phishing Attacks in Microsoft Defender? I

would like to be able to search from a list of domains, IP addresses, and file hashes and add searching from alert evidence as well.

- Can you explain line by line what this KQL above is doing?
- Can you create the same KQL but adapt it for Sentinel?
- Write a KQL query to identify Log4J in my M365Defender and list resources that are impacted with the Log4J vulnerability.

Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs)

- Summarize threat intelligence articles for <T1585.001>
- Show me 5 indicators per actor for the actors above
- Show relevant TTPs.
- Show a relevant list of indicators.

B) Unified SOC Platform

Capabilities

Intelligent context for alerts and incidents

Quickly assess emerging threats and your organization's exposure. Respond with enriched, AI-driven insights.

Rapid investigation and response

Security Copilot provides end-to-end support of analysts. From summaries of incidents and response, to assessment of incident impact, to actionable recommendations for faster investigation and remediation.

Unlock advanced SOC skills

Unlock new skills that allow analysts at all levels to complete complex tasks translating natural language to KQL or analyzing malicious scripts.

Sample Prompts

Incident Summaries

- Provide me a summary of Defender incident <Incident ID>?

- Tell me more about Sentinel incident <Incident ID>

Incident Details and Entities

- Extract the entities associated with the incident.
- If a user is listed in the incident details, show which devices they have used recently and indicate whether they are compliant with policies.

Critical Incidents and Trends

- List the 10 most critical defender incidents.
- Show defender incidents detected over the last 14 days and summarize the trends.

Reporting and Summaries

- Write a report summarizing the investigation. Lead with a non-technical executive summary. Next provide the breakdown of the Defender incident report, the takeaways from the Sentinel Hunt, the Intune device state, and finally the threat intel summary.
- Can you provide me with a concise summary of the key actions and entities involved in this security incident?

Current Critical Incidents

- What are the critical Sentinel incidents right now?
- What are the critical Defender incidents right now?

Alerts and Vulnerabilities

- List the alerts on Sentinel incident <Incident ID>
- Check Defender for vulnerabilities related to <CVE-XXXX>

Sentinel Workspaces and Incidents

- List all Sentinel workspaces.
- List the last 5 incidents from Sentinel workspace <Workspace ID>

Threat Actors and TTPs

- Tell me more about <Silk Typhoon>, and include the IOCs and any TTPs associated with <Silk Typhoon>?
- Show me MITRE TTPs from M365D incidents in the last month.
- What is the MITRE TTP number for account manipulation?

C) Purview

Capabilities

Scaled visibility

Gain comprehensive, integrated visibility across solutions and insight into relevant compliance regulatory requirements.

Summarization for speed

Quickly summarize alerts containing a breadth of signals and lengthy content to review in the lens of data security and compliance policies

Unlock expert skills

Receive step-by-step guidance, conduct searches in natural language, and conduct advanced investigations without keyword query language

Sample Prompts

- Show me the top 5 DLP alerts that I should prioritize today?
- Can you summarize purview alert <AlertID>?
- Can you summarize the risk associated with user: <UPN> involved in this alert?
- What information does Purview have about the risk associated with this user?
- Which Purview Data Loss Prevention alerts should I prioritize today?
- Can you summarize the first purview alert?
- Tell me more about the user <UPN>
- What was the data or action that triggered this alert?

- What are the data risks related to this alert?
- For the files related to the alert, show me all activities done in the last 7 days?
- Can you get me the status of labeling on these files
- Which Purview Data Loss Prevention alerts should I prioritize today?
- Retrieve all DLP alerts for this user in the last 7-days?
- Can you summarize the first purview alert?
- List all impacted entities for this alert.
- What was the data or action that triggered this alert?
- Show me the Meta Data related to these files
- Who is the user involved in this alert
- What is the risk level of this user?
- What is the status of labels on these files?
- What is the Purview risk associated with this user?
- Show me all the activities for this user in the last 7 days.
- What type of unusual activities did the user engage in the last 7 days?
- What type of exfiltration activities did the user engage in the last 5 days?
- What type of sequential activities did the user engage in the last 10 days?
- What are the data risks related to this alert?
- For the files related to the alert, show me all activities done in last 7 days
- Can you get me the status of labeling on these files?
- What Suspicious Actions Have Been Performed On This Files?
- Tell me more about Sensitivity label X

D) Entra

Capabilities

Rapid identity risk investigation

Explore sign-ins and risky users, understand the 'why' and get contextualized insights on what to do to protect the accounts, all in natural language.

Faster troubleshooting

With context at your fingertips, find gaps in access policies, generate identity workflows, and get to the root of the problem faster.

New levels of efficiency

Guided recommendations allow admins at all levels to complete complex tasks such as incident investigations. Sign-in log analysis eliminates the need for manual inspection.

Sample Prompts

User Details

- Who am i
- What login attempts exist for the user on December 31st? (Created KQL)
- What login attempts exist for the user in the last 14 days? (Created KQL)
- What login attempts exist for the user <UPN>? in the last 14 days? (Targeting a specific user)
- Is the user considered risky? If so, why?
- List all risky user by risklevel
- Tell me more about user <UPN>? in format-list.
- How many times login failed for this user in the last 30 days and tell me the reasons.
- Generate a report based on Entra plug-in: Is the user <UPN>? considered risky? If yes, list the reasons.
- Show me the most recent failed sign-in for my account in the last month.
- Show me the sign-in logs of users who signed in from ,<location>?
- Show me the authentication methods enabled for user
- What are the terms of use agreements for this user
- Show me the successfully deleted users in the last 7 days.
- List the groups <Username>? is part of
- Tell me about security group <<name>? including who created it and how many members are in it.
- What is the status of the user account for <UPN>? Is it locked out?
- Show me the successfully deleted users in the last 7 days.

Audit Logs

- Show me the audit logs for <UPN>?
- Show me audit logs for the last 24 hours
- Show me the audit logs for provisioningManagement category
- Show me the audit logs for <service name>?
- Show me audit logs for successful activities
- Show me audit logs for failed activities
- Show me the changes in <resource>? from audit logs.
- Show me the successfully deleted users in the last 7 days.
- Show me newly created conditional access policies from audit logs.
- Show me recently changed conditional access policies from audit logs.

Sign in Logs

- Show me sign-in logs for the last 24 hours
- Show me the sign-in logs for <UPN>?
- Show me the sign-in logs of users who signed in from <Location>?
- Show me the sign-in logs from <Application>?
- Show me the sign-in logs from operating system 'MAC OS
- Show me the sign-in logs from Edge
- Show me the sign-in logs from compliant devices
- Show me the sign-in logs from managed devices
- Show me the sign in logs for which conditional policies have been applied
- Show me ca policies evaluated for sign in with request id <Request ID>?
- Show me the sign-in logs from client app
- Can you tell me if conditional access policy is working from sign-in logs
- Show me the sign-in logs from unmanaged devices in the past 14 days and list the entities involved

Terms of Use Agreements

- List user terms of use agreements
- What are the terms of use agreements for this user
- List all the terms of use agreements in my tenant for this user

- Get all terms of use agreements acceptance for user
- Show me all agreement acceptances this user
- Show me all terms of use agreements of user
- List all TOU agreements of user
- Get my terms of use agreements
- Show my terms of use agreements

E) Intune

Capabilities

Faster response

Swiftly respond to threats, incidents and vulnerabilities with full device context and AI assisted insights and actions.

More informed outcomes

Proactively apply targeted policies and remediate endpoint issues with what-if analysis, actionable guidance and deep understanding of device, user and app status

Simplified posture management

Quickly translate business intent into recommended and compliant configurations and policies using natural language

Sample Prompts

Device Information

- Which devices are used by user <UPN>?
- Tell me about this device.
- Identify Weak hosts.
- Could you give me the total number of devices in Intune?

Configuration and Policies

- Show me configuration policies for this device.

- What groups is this device a member of?
- Tell me about managed apps on this device.
- Tell me about the app policy that isn't compliant. Why would this device be failing this policy?
- Tell me about the app policy that isn't compliant. Why would this device not have the policy applied and why is it in a state of non-compliance?

User and Device Specific Queries

- Tell me about devices for <Username>?
- Show me the devices for <Username>?
- How are managed apps on this device different from (insertDevice name)?
- Give me the status of the <Devicename>?. Is it managed, is it compliant with management policies?

Application and Group Management

- What groups is <Appname> assigned to?
- Show me the users <Notepad ++> assigned to

Hardware and Compliance

- Show me the difference in the hardware for the above device
- Show me the difference in managed applications for the above devices.