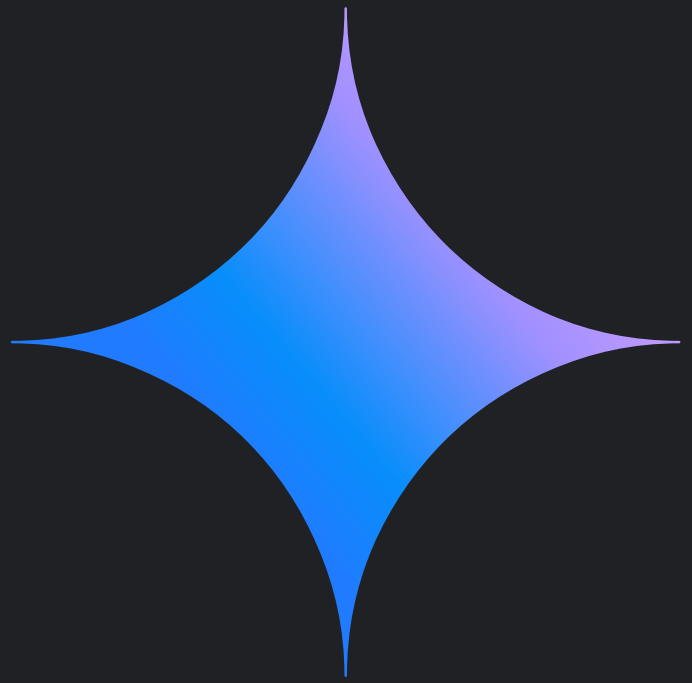


Google Cloud



User guide:

# Creating prompts with Gemini

in Security Operations  
and Threat Intelligence



**Gemini is a powerful AI tool that can be used to assist Google Security Operations and Google Threat Intelligence users. This guide will provide you with the information you need to get started with Gemini and create effective prompts.**

# Creating prompts with Gemini

When creating a prompt, you will need to provide Gemini with the following information:

01

**The type of prompt you want to create, if applicable (e.g. "Create a rule")**

02

**The context for the prompt**

03

**The desired output**

Users can create a variety of prompts, including questions, commands and summaries.

## Best practices for creating prompts

When creating prompts, it is important to keep the following best practices in mind:



**Use natural language:** Write as if you are speaking a command and express complete thoughts in full sentences.



**Provide context:** Include relevant details to help Gemini understand your request, such as timeframes, specific log sources, or user information. The more context you provide, the more relevant and helpful the results will be.



**Be specific and concise:** Clearly state the information you are looking for or the task you want Gemini to perform. Detail the purpose, trigger, action, and condition(s). For example, ask the assistant: "Is this (file name, etc.) known to be malicious?" and if it is known to be, you can ask to "Search for this (file) in my environment."



**Include clear objectives:** Start with a clear objective and specify triggers that will activate a response.



**Leverage all modalities:** Use in-line search functionality, chat assistant, and the playbook generator for your different needs.



**Reference integrations (for playbook creation only):** Request and specify integrations you've already installed and configured in your environment as they relate to next steps in the playbook.



**Iterate:** If the initial results are not satisfactory, refine your prompt, provide additional information, and ask follow-up questions to guide Gemini towards a better response.



**Include conditions for action (for playbook creation only):** You can enhance the prompt's effectiveness when creating a playbook by requesting additional steps such as enriching data.



**Verify accuracy:** Remember that Gemini is an AI tool, and its responses should always be validated against your own knowledge and other available sources.

# Using prompts in Security Operations

Gemini can be used in a variety of ways in Security Operations, including in-line search, chat assistance, and playbook generation. After receiving AI-generated case summaries, Gemini can help practitioners with:

01 **Threat detection and investigation**

02 **Security-related Q&A**

03 **Playbook generation**

04 **Threat intelligence summarization**

Google Security Operations (SecOps) is enriched with frontline intelligence from Mandiant, and crowdsourced intelligence from VirusTotal which can help security teams:



**Quickly access and analyze threat intelligence:** Ask natural language questions about threat actors, malware families, vulnerabilities, and IOCs.



**Accelerate threat hunting and detection:** Generate UDM search queries and detection rules based on threat intelligence data.



**Prioritize security risks:** Understand which threats are most relevant to their organization and focus on the most critical vulnerabilities.

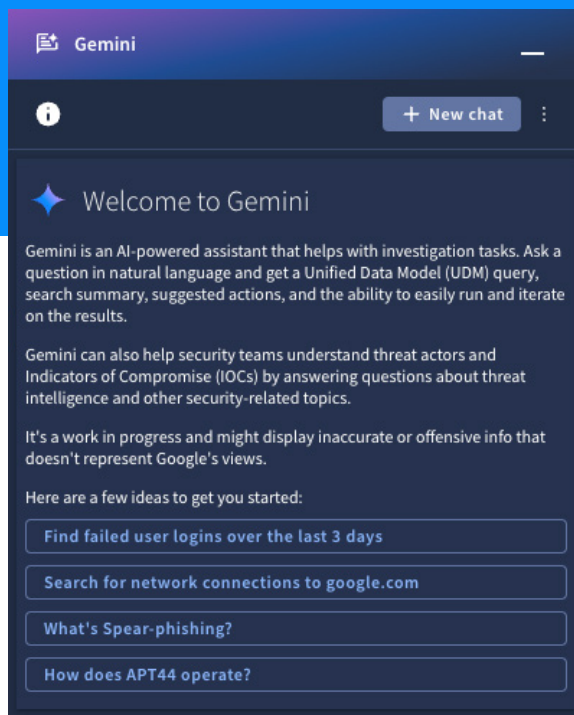


**Respond more effectively to security incidents:** Enrich security alerts with threat intelligence context and get recommendations for remediation actions.



**Improve security awareness:** Create engaging training materials based on real-world threat intelligence.

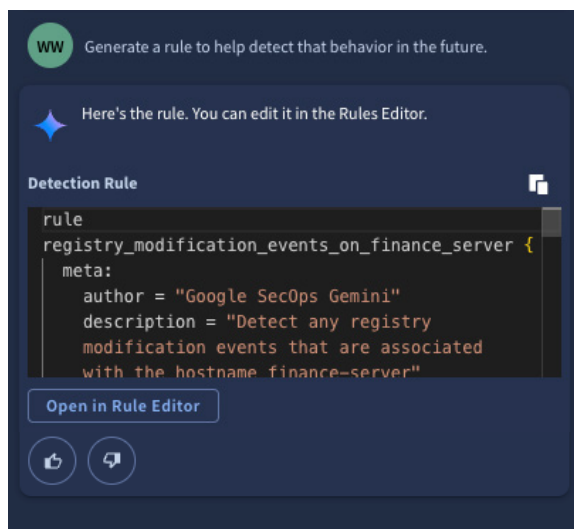
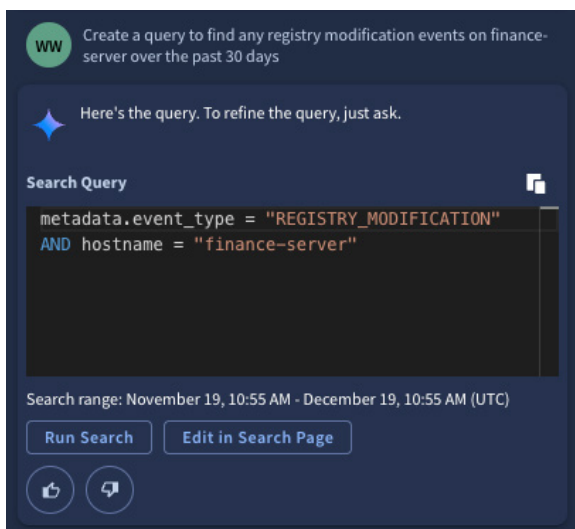
# Use cases for Security Operations



01

## Threat detection and investigation

Create queries, generate rules, monitor events, investigate alerts, search for data (generate UDM queries).



**Scenario:** A threat analyst is investigating a new alert and wants to know if there is any evidence in the environment of a particular command used to infiltrate infrastructure by adding itself to the registry.



**Sample prompt:** Create a query to find any registry modification events on [hostname] over the past [time period].



**Follow-up prompt:** Generate a rule to help detect that behavior in the future.

**WW** Show me network connection events for the userid starting with tim.smith case insensitive for the past 3 days

Here's the query. To refine the query, just ask.

**Search Query**

```
metadata.event_type = "NETWORK_CONNECTION" AND
user = /^tim\.smith/ nocase
```

Search range: January 23, 09:56 PM - January 26, 09:56 PM (UTC)

[Run Search](#) [Edit in Search Page](#)


**WW** Generate a YARA-L rule to detect for this activity in the future


Here's the rule. You can edit it in the Rules Editor.


**Detection Rule**

```
rule network_connection_tim_smith {
  meta:
    author = "Google SecOps Gemini"
    description = "Detect any network
connection events for the userid starting
with tim.smith case insensitive for the
past 3 days"
```

[Open in Rule Editor](#)

 **Scenario:** An analyst is told that an intern was doing suspicious "things" and wanted to get a better understanding of what was occurring.

 **Sample prompt:** Show me network connection events for the userid starting with tim.smith (case insensitive) for the past 3 days.

 **Follow-up prompt:** Generate a YARA-L rule to detect for this activity in the future.

**WW** Show me blocked user login events with an event code of 4625 where src.hostname is not null

Here's the query. To refine the query, just ask.

**Search Query**


```
metadata.event_type = "USER_LOGIN" AND
security_result.action = "BLOCK" AND metadata.
product_event_type = "4625" AND src.hostname
!= ""
```


Search range: January 25, 10:00 PM - January 26, 10:00 PM (UTC)


[Run Search](#) [Edit in Search Page](#)

**WW** How many users are present in the results set?

There are 15 unique users in the result set.

 **Scenario:** A security analyst receives an alert about suspicious activity on a user account.

 **Sample prompt:** Show me blocked user login events with an event code of 4625 where src.hostname is not null.

 **Follow-up prompt:** How many users are included in the result set?

## 02 Security-related Q&A

**WW** What is HANGMAN.V2?

HANGMAN.V2 is a malware variant of the HANGMAN backdoor. It's closely related to HANGMAN but distinguishes itself by using HTTP for network communication and employing a different data formatting scheme when interacting with its command and control (C&C) server. According to available threat intelligence, HANGMAN.V2 is linked to APT43, a North Korean advanced persistent threat (APT) group known for cyber espionage. It's been observed alongside other malware families like PUMPKINBAR and PENCILDOWN.

HANGMAN.V2 exhibits several capabilities, including hostname capture, Base64 and XOR encoding, AES encryption, file and process module listing, and file deletion. It's been detected by at least one security product (M\_Autopatt\_Backdoor\_HANGMAN\_V2\_1) and is known to target Windows systems. AhnLab also refers to it as NikiHTTP.

In the past 90 days, we found 2 Indicators of Compromise (IOCs) in your environment associated with [APT43, HANGMAN.V2] with the following Last Seen timestamps:

- File Hash: **a605570555620cea6d6be211520525fc95a30961661780da4cc4baf9864f394** (2024-12-18T15:31:16Z)
- File Hash: **21cffaa7f9bf224ce75e264bfb16dd0d** (2024-12-18T15:31:16Z)

[Here's a search to help investigate.](#)

**WW** How does HANGMAN.V2 persist?

HANGMAN.V2 achieves persistence by adding a registry entry to HKCU\Software\Microsoft\Windows\CurrentVersion\Run. It uses the command `reg add hkcu\software\microsoft\windows\currentversion\run /d "<SELF>" "iFfmHUtaWxNnxTHEiAAN" /t REG_SZ /v "System" /f` to accomplish this. This causes the malware to automatically execute upon system startup. The command-line argument "iFfmHUtaWxNnxTHEiAAN" then triggers a second execution path, which handles further actions such as communication with the command and control (C&C) server.

In the past 90 days, we found 2 Indicators of Compromise (IOCs) in your environment associated with [APT43, HANGMAN.V2] with the following Last Seen timestamps:

- File Hash: **a605570555620cea6d6be211520525fc95a30961661780da4cc4baf9864f394** (2024-12-18T15:31:16Z)
- File Hash: **21cffaa7f9bf224ce75e264bfb16dd0d** (2024-12-18T15:31:16Z)

[Here's a search to help investigate.](#)



**Scenario:** A security analyst is onboarding into a new job and notices that Gemini has summarized a case with recommended steps for investigation and response. They want to learn more about the malware identified in the case summary.



**Sample prompt:** What is [name of malware]?



**Follow-up prompt:** How does [name of malware] persist?

WW

Is this file hash  
8e570e32acb99abfd0daf62cff13a09eb694ebfa633a365d  
224aefc6449f97de known to be malicious?



Yes, the file hash  
8e570e32acb99abfd0daf62cff13a09eb694eb  
fa633a365d224aefc6449f97de is known to be  
malicious. According to available threat intelligence, this  
SHA256 hash is associated with the MD5 hash  
60375d64a9a496e220b6eb1b63e899b3, which is  
identified as URSNIF malware, a banking trojan.

VirusTotal analysis shows that out of 5 unique sources,  
51% flagged the file as malicious. The popular threat  
classifications include "gozi," "genericfca," and "ursnif,"  
with the suggested threat label being  
"trojan.gozi/genericfca." The analysis also reveals  
several concerning behaviors, such as checking user  
input, detecting debug environments, and making calls  
to WMI, all common techniques used by malware. The  
sandbox verdicts further support this assessment,  
showing 3 malicious detections and only 1 non-  
malicious detection.

Therefore, based on the available data, a high  
confidence, high severity threat rating is assigned to this  
file hash. It should be treated as malicious and  
quarantined immediately.



**Scenario:** A security analyst receives an alert about a potentially malicious file hash.



**Sample prompt:** Is this file hash [insert hash] known to be malicious?



**Follow-up prompt:** What other information is available about this file?



**Scenario:** An incident responder needs to identify the source of a malicious file.



**Sample prompt:** What is the file hash of the executable "[malware.exe]"?



**Follow-up prompts:**

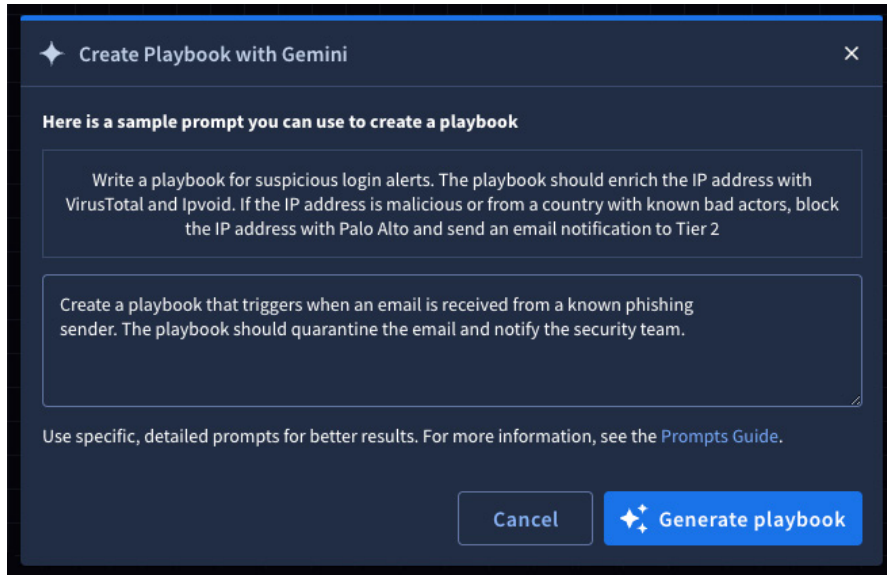
- Enrich with threat intelligence from VirusTotal for information about this file hash; is it known to be malicious?
- Has this hash been observed in my environment?
- What are the recommended containment and remediation actions for this malware?



03

# Playbook generation

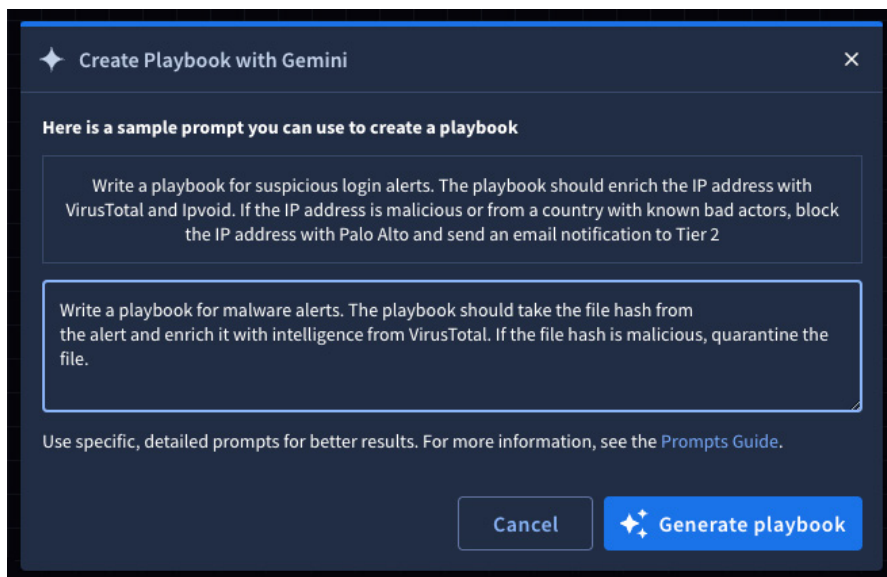
Take action and build playbooks.



**Scenario:** A security engineer wants to automate the process of responding to phishing emails.



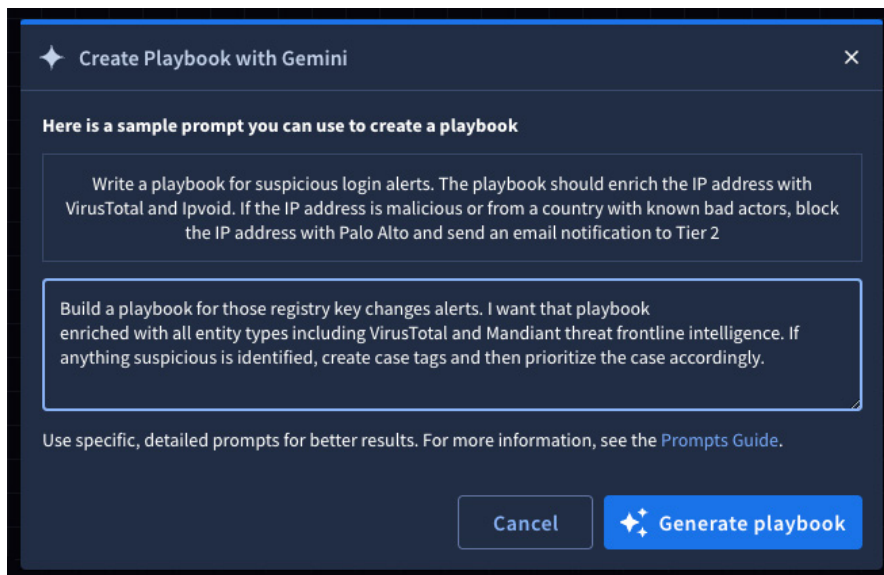
**Sample prompt:** Create a playbook that triggers when an email is received from a known phishing sender. The playbook should quarantine the email and notify the security team.



**Scenario:** A member of the SOC team wants to automatically quarantine malicious files.



**Sample prompt:** Write a playbook for malware alerts. The playbook should take the file hash from the alert and enrich it with intelligence from VirusTotal. If the file hash is malicious, quarantine the file.



**Scenario:** A threat analyst wants to create a new playbook that can help respond to future alerts related to registry key changes.



**Sample prompt:** Build a playbook for those registry key changes alerts. I want that playbook enriched with all entity types including VirusTotal and Mandiant threat frontline intelligence. If anything suspicious is identified, create case tags and then prioritize the case accordingly.



## Threat intelligence summarization

Gain insights about threats and threat actors.



**Scenario:** A security operations manager wants to understand the attack patterns of a specific threat actor.



**Sample prompt:** What are the known tactics, techniques, and procedures (TTPs) used by APT29?



**Follow-up prompt:** Are there any curated detections in Google SecOps that can help identify activity associated with these TTPs?



**Scenario:** A threat intelligence analyst learns about a new kind of malware (“emotet”) and shares a report from their research with the SOC team.



**Sample prompt:** What are the indicators of compromise (IOCs) associated with the emotet malware?



**Follow-up prompts:**

- Generate a UDM search query to look for these IOCs in my organization's logs.
- Create a detection rule that will alert me if any of these IOCs are observed in the future.



**Scenario:** A security researcher has identified hosts in their environment communicating with known command-and-control (C2) servers associated with a particular threat actor.



**Sample prompt:** Generate a query to show me all outbound network connections to IP addresses and domains associated with: [name of threat actor].



By using Gemini effectively, security teams can enhance their threat intelligence capabilities and improve their overall security posture. These are just a few examples of how Gemini can be used to improve security operations. As you become more familiar with the tool, you will find many other ways to use it to your advantage. Additional details can be found on the Google SecOps product documentation [page](#).

# Using prompts in Threat Intelligence

While Google Threat Intelligence can be used similarly to a traditional search engine with terms alone, users can also achieve intended results by creating specific prompts. Gemini prompts can be used in a variety of ways in Threat Intelligence, from searching for broad trends, to understanding specific threats and pieces of malware, including:

01 Threat intelligence analysis

02 Proactive threat hunting

03 Threat actor profiling

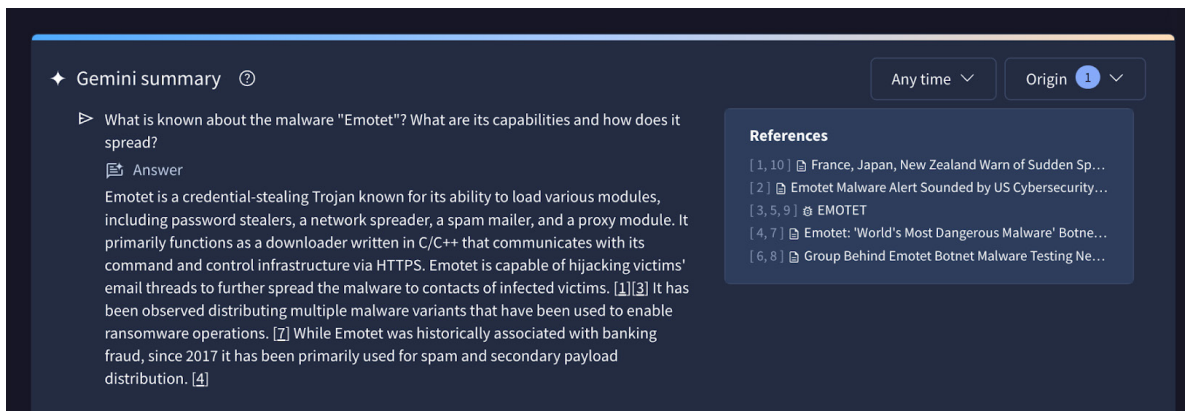
04 Vulnerability prioritization

05 Enriching security alerts

06 Leveraging MITRE ATT&CK

# Use cases for Threat Intelligence

## 01 Threat intelligence analysis



**Scenario:** A threat intelligence analyst wants to learn more about a newly discovered malware family.



**Sample prompt:** What is known about the malware "Emotet"? What are its capabilities and how does it spread?



**Related prompt:** What are the indicators of compromise (IOCs) associated with the emotet malware?

◆ Gemini summary ⓘ

Any time ▾ Origin 3 ▾

▶ Summarize the known TTPs of the ransomware group "LockBit 3.0." Include information about their initial access methods, lateral movement techniques, and preferred extortion tactics.

📄 Answer

LockBit 3.0, also known as LockBit Black, is a ransomware-as-a-service (RaaS) operation that utilizes various initial access methods, including Remote Desktop Protocol (RDP), phishing campaigns, and exploiting vulnerabilities like CVE-2023-27350. [1] Once inside a victim's network, LockBit 3.0 affiliates spread laterally using tools like SMB, PsExec, and Group Policy. [1] They then exfiltrate data using tools like Stealbit, Rclone, or WinSCP, uploading it to private servers or public websites like MEGA. LockBit 3.0 encrypts files using AES and RSA, erases logs, and tampers with backup mechanisms. [1] The group employs a double extortion tactic, threatening to publish stolen data if the ransom is not paid. [4]

**References**

- [ 1 ] 📄 THREAT ANALYSIS: Assemble LockBit 3.0
- [ 2, 3, 5, 6, 7, 9, 10 ] 📄 Understanding Ransomware Threat ...
- [ 4 ] 📄 Known LockBit 3.0 ransomware IOCs and TTPs foun...
- [ 8 ] 📄 LOCKBIT



**Scenario:** An analyst is investigating a new ransomware group and wants to quickly understand their tactics, techniques, and procedures (TTPs).



**Sample prompt:** Summarize the known TTPs of the ransomware group "LockBit 3.0." Include information about their initial access methods, lateral movement techniques, and preferred extortion tactics.



**Related prompts:**

- What are the common indicators of compromise (IOCs) associated with LockBit 3.0?
- Have there been any recent public reports or analysis of LockBit 3.0 attacks?

## 02 Proactive threat hunting

◆ Gemini summary ⓘ

Any time ▾ Origin 1 ▾

▶ What are the common indicators of compromise (IOCs) associated with the "Trickbot" malware?

📄 Answer

Trickbot is a backdoor malware that communicates via HTTP or HTTPS and utilizes a plug-in framework to expand its capabilities. [8] Common indicators of compromise (IOCs) associated with Trickbot include specific files, domains, and IP addresses. [1] For example, Trickbot has been linked to files such as 3778afb770788522dee0ca59bdf542cd121d5d3e7c0e6aa250f0d555b583ee5f and domains like web-analysis.live. [1] Additionally, Trickbot has been associated with IP addresses such as 51.75.58.175 and 73.2.223.45. Trickbot is known to target various industries, including financial services, healthcare, and government. [1][8]

**References**

- [ 1, 6, 8 ] 📄 TRICKBOT
- [ 2, 5 ] 📄 TrickBot Malware Profile
- [ 3 ] 📄 Threat Activity Report: Technical Details for Recent...
- [ 4, 7 ] 📄 LOKIBOT
- [ 9, 10 ] 📄 TRIK



**Scenario:** A threat intelligence analyst wants to proactively search for signs of a specific malware family known to target their industry.



**Sample prompt:** What are the common indicators of compromise (IOCs) associated with the "Trickbot" malware?



**Scenario:** A security researcher wants to identify any hosts in their environment communicating with known command-and-control (C2) servers associated with a particular threat actor.



**Sample prompt:** What are the known C2 IP addresses and domains used by the threat actor "[Name]"?

### 03 Threat actor profiling

◆ Gemini summary ⓘ

Any time ▾ Origin 1 ▾

➤ Generate a profile of the threat actor "APT29". Include their known aliases, suspected country of origin, motivations, typical targets, and preferred TTPs

📄 Answer

APT29, also known as Cozy Bear, Nobelium, and other aliases, is a Russian cyber espionage group. Their primary motivation is espionage, targeting Western governments, foreign affairs bodies, government contractors, universities, and possibly international news outlets. [1] They are known for their sophisticated capabilities, including custom tools, extensive command and control infrastructure, and strong operational security. [1] APT29 has been observed using phishing campaigns, exploiting vulnerabilities, and leveraging third-party access to steal data. [6] Their tactics, techniques, and procedures (TTPs) include OS credential dumping, data obfuscation, and remote system discovery. [10]

**References**

- [ 1, 3, 4, 6, 10 ] 🏠 APT29
- [ 2 ] @ APT29 Conducts Phishing Campaign Targeting Multi...
- [ 5 ] 📄 APT29 Threat Group Profile
- [ 7 ] 🏠 UNC2529
- [ 8, 9 ] 🏠 APT9

◆ Gemini summary ⓘ

Any time ▾ Origin 3 ▾

➤ Show me a timeline of APT29's most notable attacks

📄 Answer

APT29, also known as Nobelium, Cozy Bear, and Midnight Blizzard, has been active since at least 2008, targeting Western governments and related organizations. In 2020, they launched a major cyberattack against the U.S. government and private companies through the SolarWinds supply chain. In 2021, they exploited the ProxyShell vulnerabilities in Microsoft Exchange servers, and targeted global IT supply chains. [2] In 2022, they used Credential Roaming to gain access to a European diplomatic entity's network. [2][7] In 2023, they targeted NATO and EU member states' diplomatic and foreign ministries with spear phishing emails and malware. [4]

**References**

- [ 1, 2, 3, 4, 5, 7, 8 ] 📄 Evolution of Russian APT29 – New Att...
- [ 6, 9 ] 📄 Backchannel Diplomacy: APT29's Rapidly Evolvin...
- [ 10 ] 🏠 APT29



**Scenario:** A threat intelligence team is tracking the activities of a suspected APT group and wants to develop a comprehensive profile.



**Sample prompt:** Generate a profile of the threat actor "APT29". Include their known aliases, suspected country of origin, motivations, typical targets, and preferred TTPs.



**Related prompt:** Show me a timeline of APT29's most notable attacks campaign and timeline.

## 04 Vulnerability prioritization



**Scenario:** A vulnerability management team wants to prioritize remediation efforts based on the threat landscape.



**Sample prompt:** Which Palo Alto Networks vulnerabilities are being actively exploited by threat actors in the wild?



**Related prompt:** Summarize the known exploits for CVE-2024-3400 and CVE-2024-0012.



**Scenario:** A security team is overwhelmed with vulnerability scan results and wants to prioritize remediation efforts based on threat intelligence.



**Sample prompt:** Which of the following vulnerabilities have been mentioned in recent threat intelligence reports: [list identified vulnerabilities]?



**Related prompts:**

- Are there any known exploits available for the following vulnerabilities: [list identified vulnerabilities]?
- Which of the following vulnerabilities are most likely to be exploited by threat actors: [list identified vulnerabilities]? Prioritize them based on their severity, exploitability, and relevance to our industry.

## 05 Enriching security alerts



**Scenario:** A security analyst receives an alert about a suspicious login attempt from an unfamiliar IP address.



**Sample prompt:** What is known about the IP address [provide IP]?

## 06 Leveraging MITRE ATT&CK



**Scenario:** A security team wants to use the MITRE ATT&CK framework to understand how a specific threat actor might target their organization.



**Sample prompt:** Show me the MITRE ATT&CK techniques associated with the threat actor APT38.





**Gemini is a powerful tool that can be used to improve Security Operations and Threat Intelligence. By following the best practices outlined in this guide, you can create effective prompts that will help you get the most out of Gemini.**

**Note:** This guide provides suggestions for using Gemini in Google SecOps and Gemini in Threat Intelligence. It is not an exhaustive list of all possible use cases, and the specific capabilities of Gemini may vary depending on your product edition. You should consult the official documentation for the most up-to-date information.



Gemini  
in Security Operations



Gemini  
in Threat Intelligence