# Securing Automation with API Gateways

SOAR (Security Orchestration, Automation, and Response) technology enables orchestration and automation of many different security components, services, and applications. SOAR products automate the activity of these tools through their Application Programming Interfaces (APIs) and associated API keys. However, each security application uses its own API key and may implement the keys in different ways, which complicates SOAR workflows when using multiple products and could possibly expose more functionality than desired within an enterprise network.

Utilizing automation and orchestration improves the speed and scale of security operations, but it can also be leveraged by an attacker. Compromise of API keys used by automated workflows can lead to unauthorized access to security products and services. To mitigate this risk, organizations implementing automation environments such as SOAR platforms should have a way to monitor and restrict API accesses. It is also important to have a way to recover from the potential compromise of an API key in an automated manner.

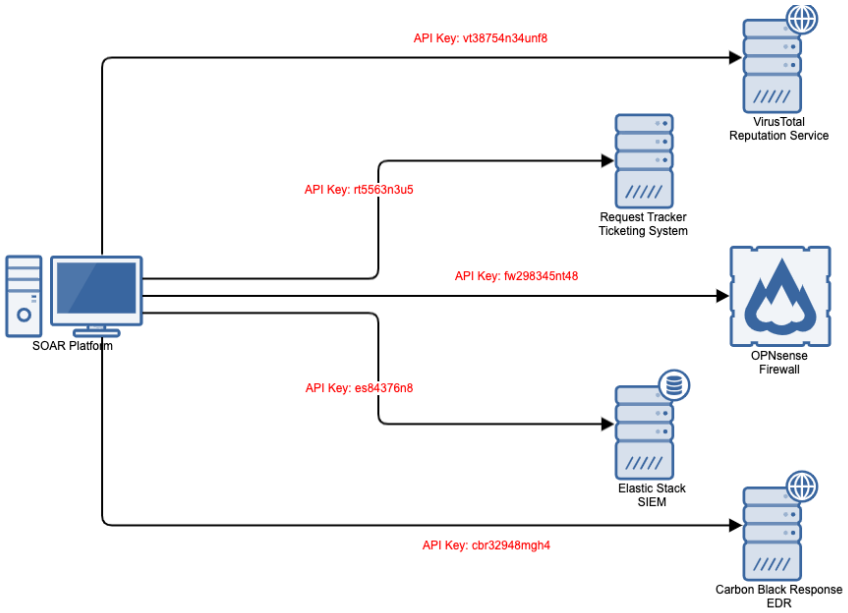
An API gateway is a set of products/services that provides a single point of access to internal and external APIs. API gateways are often used for scalability when managing a large number of keys for the many products deployed within an organization. API gateways enable centralized logging and auditing of API usage. An API gateway can also improve the management and security of API keys associated with security products orchestrated by an automation environment.

The Integrated Adaptive Cyber Defense (IACD) initiative demonstrated the use of an API gateway to manage the API keys used by a SOAR product in a set of experiments, showing how an API gateway can help better secure automation environments. In addition to all of the benefits of API gateways mentioned previously, the combination of an API gateway and SOAR product ensures that only authorized commands are issued to security products via automation.

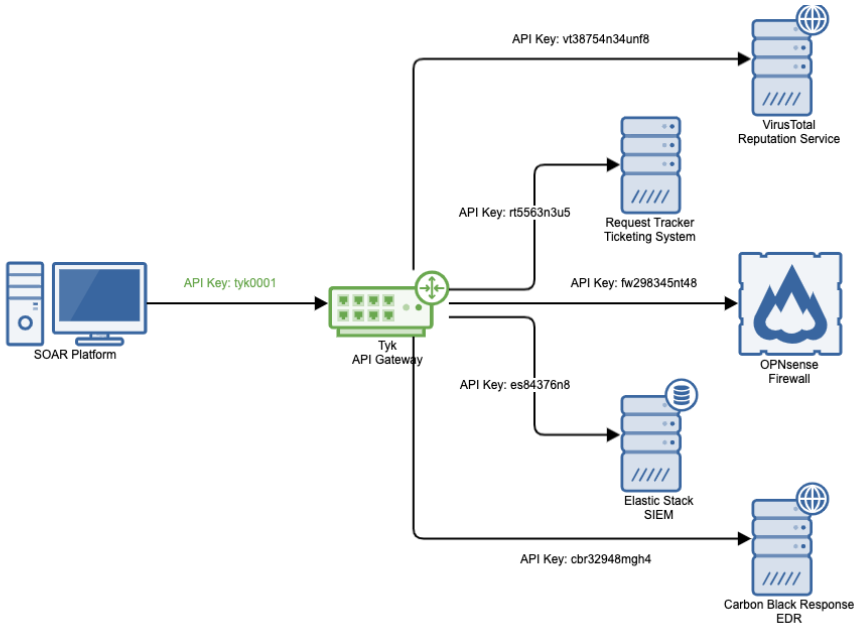
In the experiments, API security issues were detected based on four main attributes of the API request: Who, Where, What, and When. The “Who” attribute was the requester. The “Where” attribute was the source of the request, typically determined by a user's IP address. The “What” attribute was the requested API action found in the URL path, such as blocking an IP address. The “When” attribute represented the time of day a request was made, or the number of times a request was made within a timeframe. The table below summarizes the issues detected based on the four API request attributes, the possible cause of each issue, and the responses that were demonstrated in the experiments.

| Who | Where | What | When | Possible Cause | Response |
|---|---|---|---|---|---|
| Invalid | N/A | N/A | N/A | API request not authenticated | Block API request |
| Valid | Invalid | Valid | N/A | Analyst using wrong workstation | Block API request<br>Investigate API key |
| Valid | Invalid | Invalid | N/A | API key compromised | Block API request<br>Revoke API key & create new API key |
| Valid | Valid | Invalid | N/A | API request invalid for given role | Block API request<br>Investigate API key |
| Valid | Valid | Valid | Invalid | API request exceeds rate-limit/quota<br>Anomalous API requests | Block API request<br>Investigate API key |

The figure below shows how a SOAR platform would typically manage separate API keys for different tools and services:




In IACD's API security experiments, a virtual enterprise was created containing multiple security products and services in the enterprise, controlled by a SOAR platform, with API keys managed by an API gateway:




The Tyk API Gateway was configured as a proxy to the APIs for the various tools in the virtual enterprise:

- OPNsense Firewall
- Carbon Black Endpoint Detection and Response (EDR) product
- VirusTotal malware reputation service
- Elastic Stack Security Information and Event Manager (SIEM)
- Request Tracker Ticketing System

The API gateway managed the API keys and their usage from a central location, enabling greater visibility and analysis of the API key usage. The introduction of an API gateway to manage the API keys on behalf of security automation has the following benefits:

- Centralized management and recovery
- Consolidation of multiple APIs into a single API
- Standardization of authentication methods
- Logging and visualization of API requests
- Scalable and enhanced secure usage of APIs
- Application security policies and roles for API usage

In the experiment scenarios, IACD configured the Tyk API Gateway to log all data related to API requests to the Elastic Stack SIEM. This global visibility of API key usage enabled the analysis and detection of many forms of unauthorized and improper API key usage as described in the previous table.

Furthermore, integration of the API gateway with the SOAR platform demonstrated the ability to remediate the detected issues with API key usage. In the IACD experiments, the Tyk API Gateway sent actions to the Request Tracker ticketing system, where the SOAR platform could manage remediation actions taken in workflows, such as investigating suspicious API key usage and revoking compromised API keys. The API gateway could enforce security policies and automatically block any API requests failing authentication or violating policy.

Through its API security experimentation, IACD demonstrated the benefits of integrating an API gateway with SOAR technology to secure the orchestration and automation process. An API gateway is one possible solution for securing automation; there are potentially other solutions that could also help better secure automation environments. For more information on SOAR technologies, API security, and other experiments, please see the resources in the References section and visit https://www.iacdautomate.org.

# References

[1] IACD. (2019, October). “Insights for secure API usage in conjunction w/ security automation & orchestration”. BSides DC. Retrieved from https://www.youtube.com/watch?v=NHicNfM8cF8