

APIs

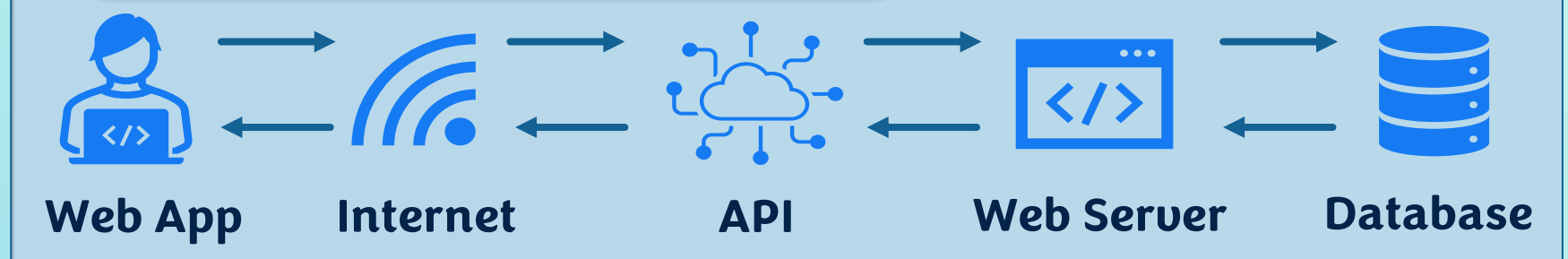
Application Programming Interface

In the context of
information security

APIs are mechanisms that enable two software components to communicate with each other using a set of definitions and protocols ¹



How an API works



“STIX and TAXII are standards developed in an effort to improve the prevention and mitigation of cyber-attacks. STIX states the “what” of threat intelligence, while TAXII defines “how” that information is relayed. Unlike previous methods of sharing, STIX and TAXII are machine-readable and therefore easily automated. ²

*STIX/TAXII Was Developed From a
Need for a Threat Intelligence
Sharing Standard ²*

According to Anomali,
STIX & TAXII improves
security by:

STIX

- Structured Threat Information eXpression
- Developed by MITRE and OASIS CTI Technical Committee
- Adopted as an international standard
- Designed to be shared via TAXII but can be shared by other means



TAXII

- Trusted Automated eXchange of Intelligence Information
- Defines how cyber threat information can be shared
- Designed to support STIX information by defining an API that aligns with common sharing models

Extending the
capabilities of current
threat intelligence
sharing

Balancing the
response with
proactive detection

Encouraging a
holistic approach to
threat intelligence

References

1: AWS. (n.d.). *What is an API?* AWS. Retrieved January 15, 2023, from <https://aws.amazon.com/what-is/api/>

2: Anomali. (n.d.). *What are STIX/TAXII Standards?* Anomali. Retrieved January 15, 2023, from <https://www.anomali.com/resources/what-are-stix-taxii>