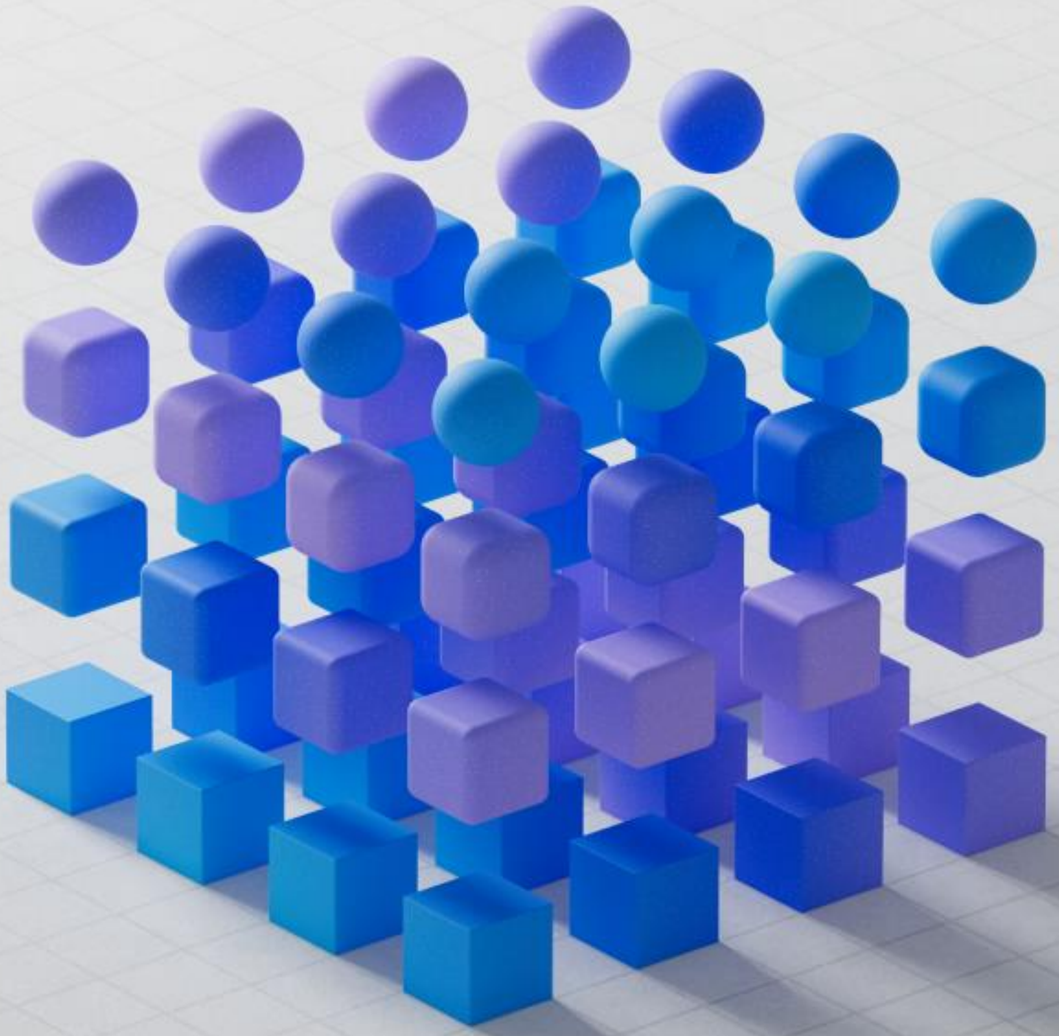
Microsoft

Azure Developers

APIs in Action



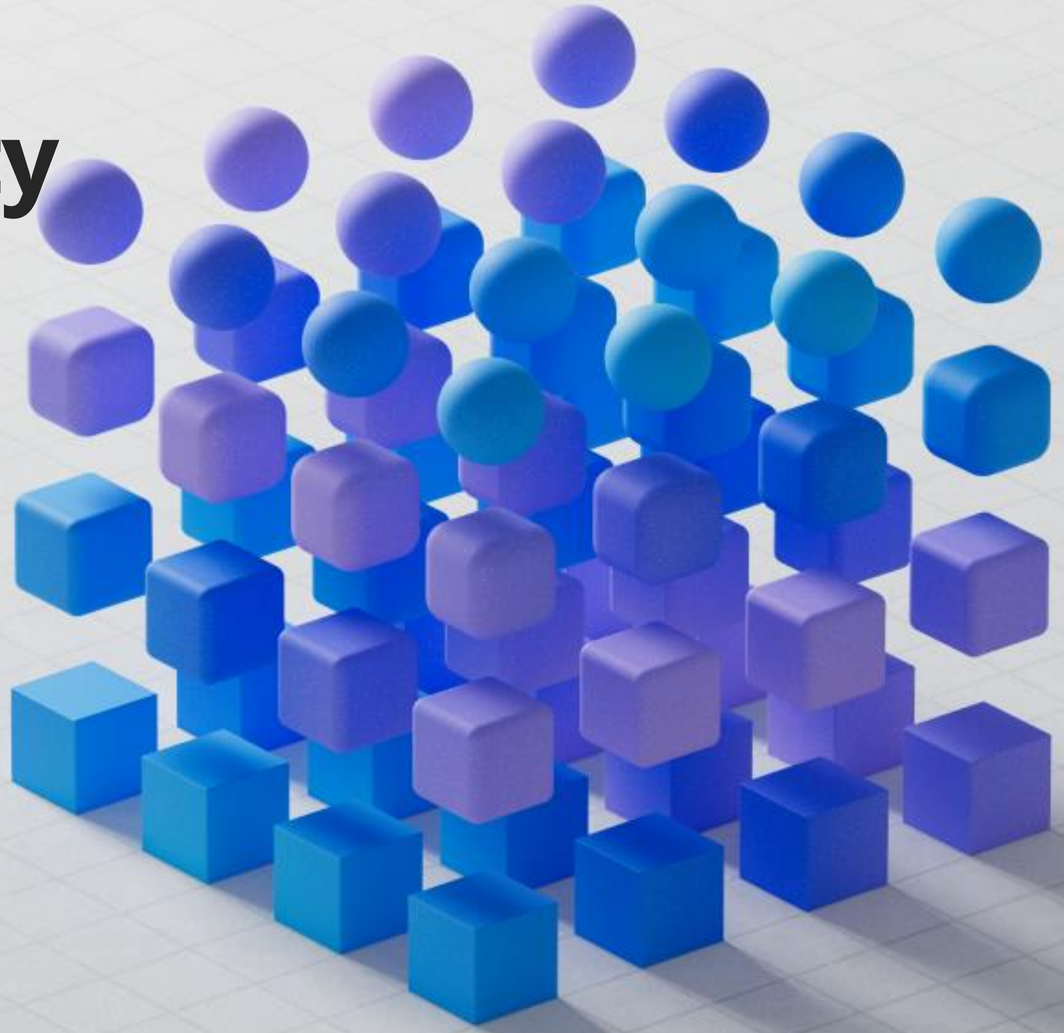
February 28, 2024

Microsoft

APIs in Action, February 2024

Enhance your API security posture with Microsoft Defender for APIs

Massimo Crippa



API attacks are on the rise

APIs are everywhere » 83% of the internet traffic is driven by APIs[1]

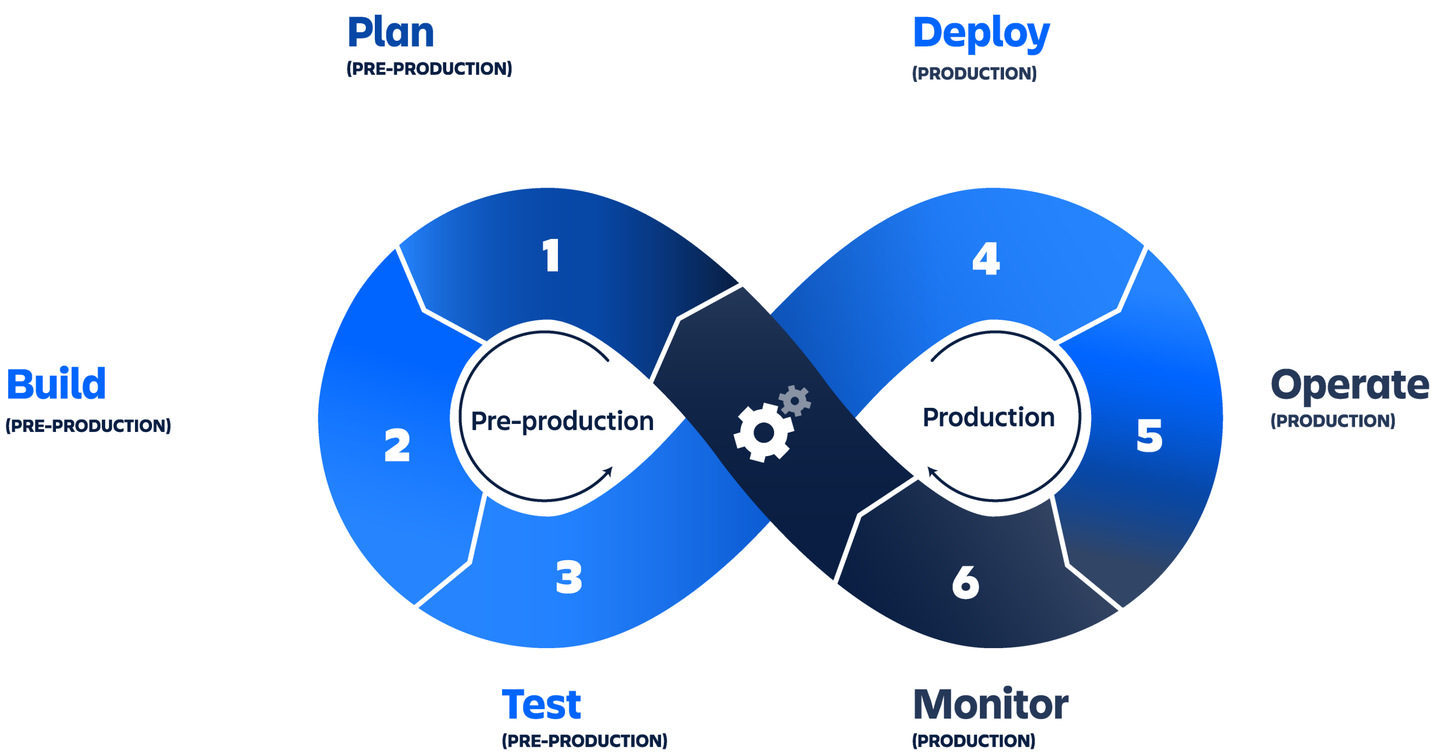
APIs data breaches has grown » 90% of web applications will expose attack surfaces via APIs[2]

API security has emerged as a significant business issue » 59% have experienced application rollout delays resulting from security issues identified in APIs[3]

1 – Akamai state of internet Security Report
2 – Gartner report : API Security what you need to do to protect your APIs
3 - Salt Security : State of API Security 2023

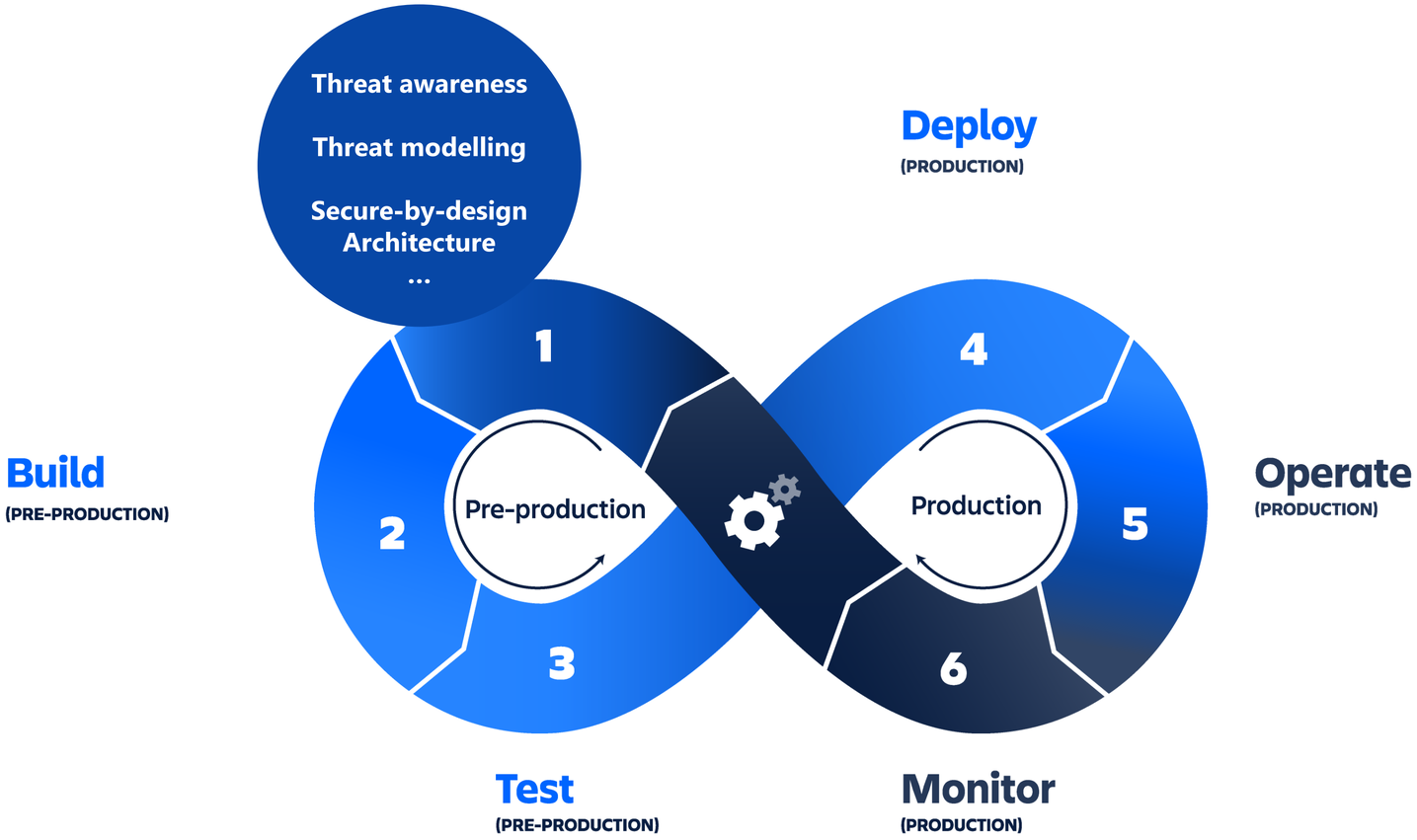
Security is the first concern of every enterprise

Bring together preventive and runtime security models



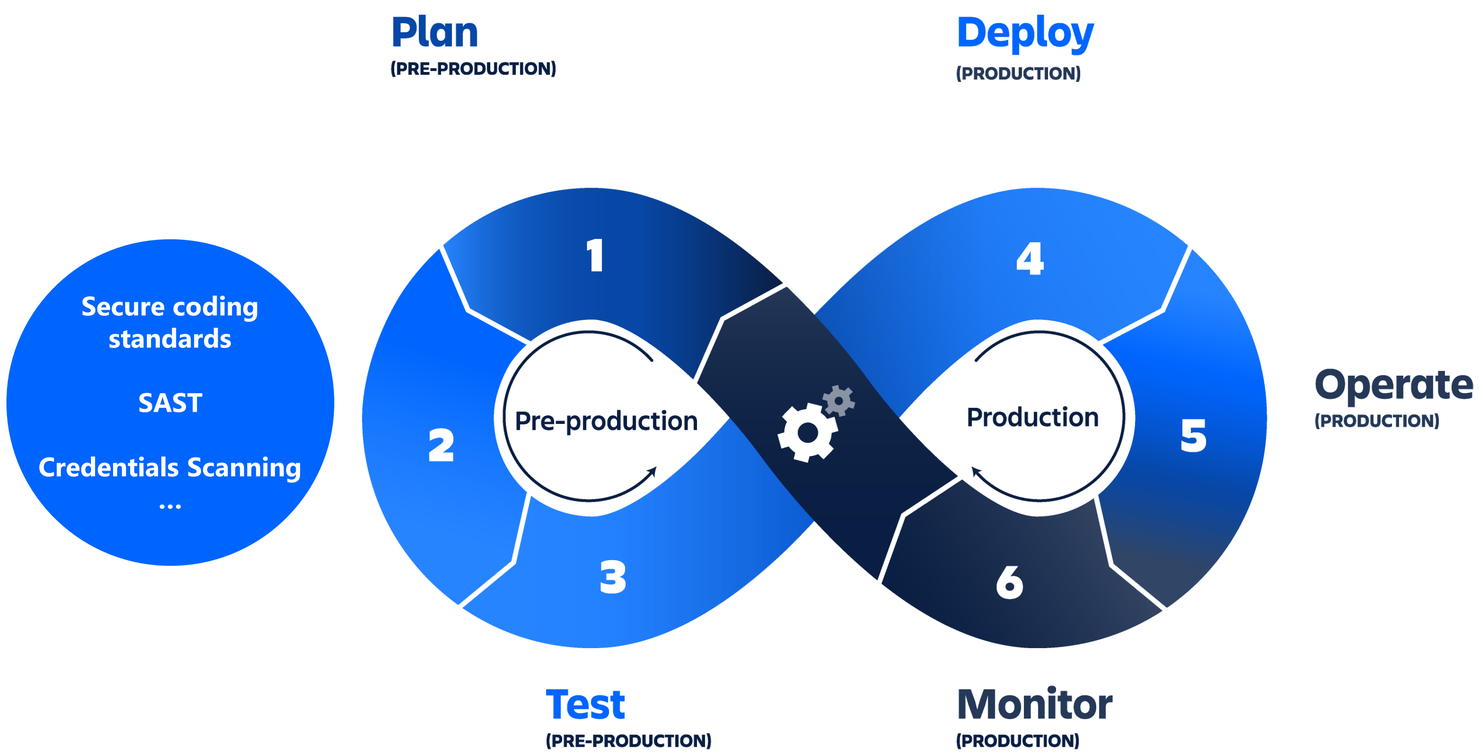
Security is the first concern of every enterprise

Bring together preventive and runtime security models

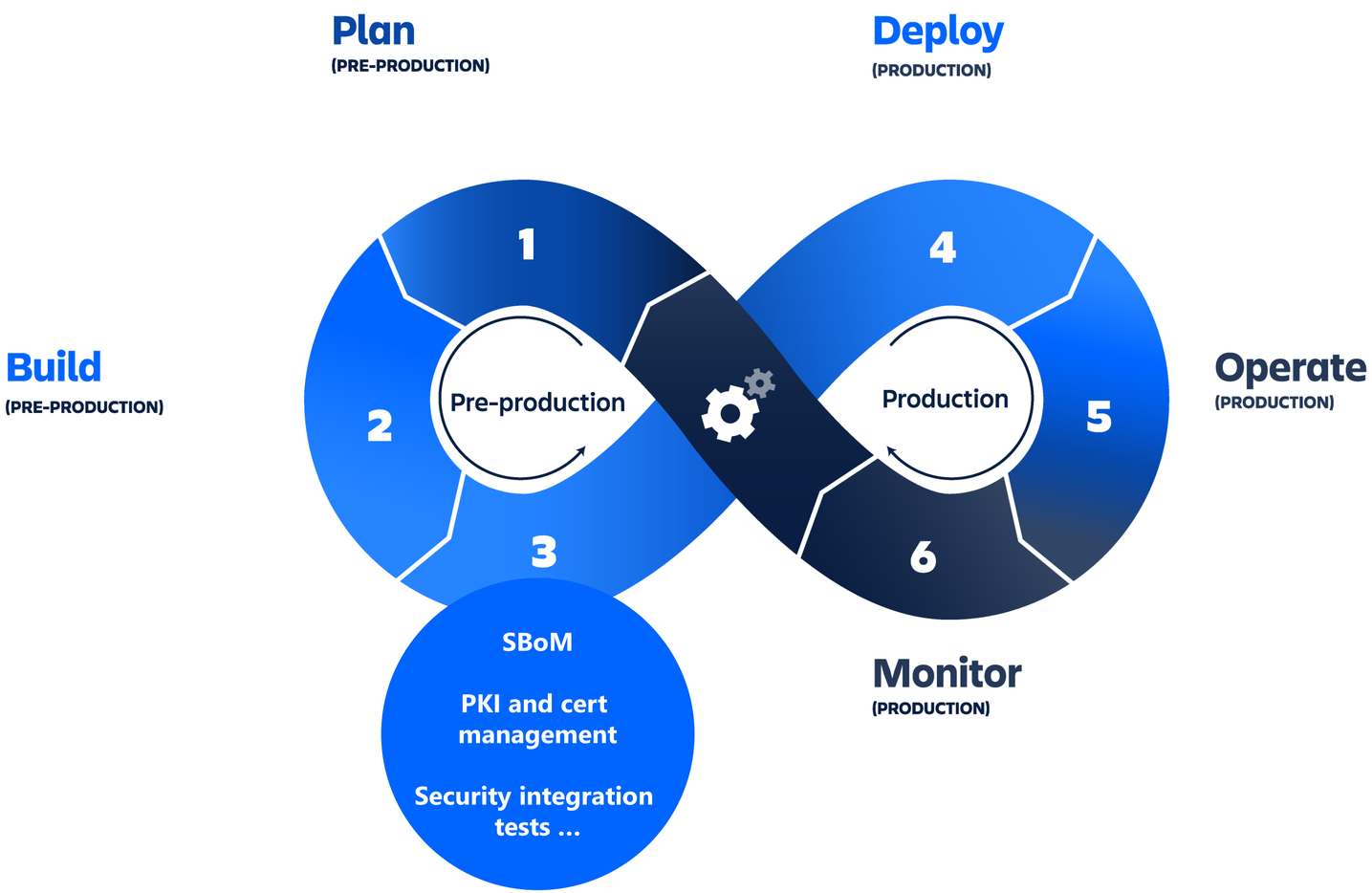


Security is the first concern of every enterprise

Bring together preventive and runtime security models

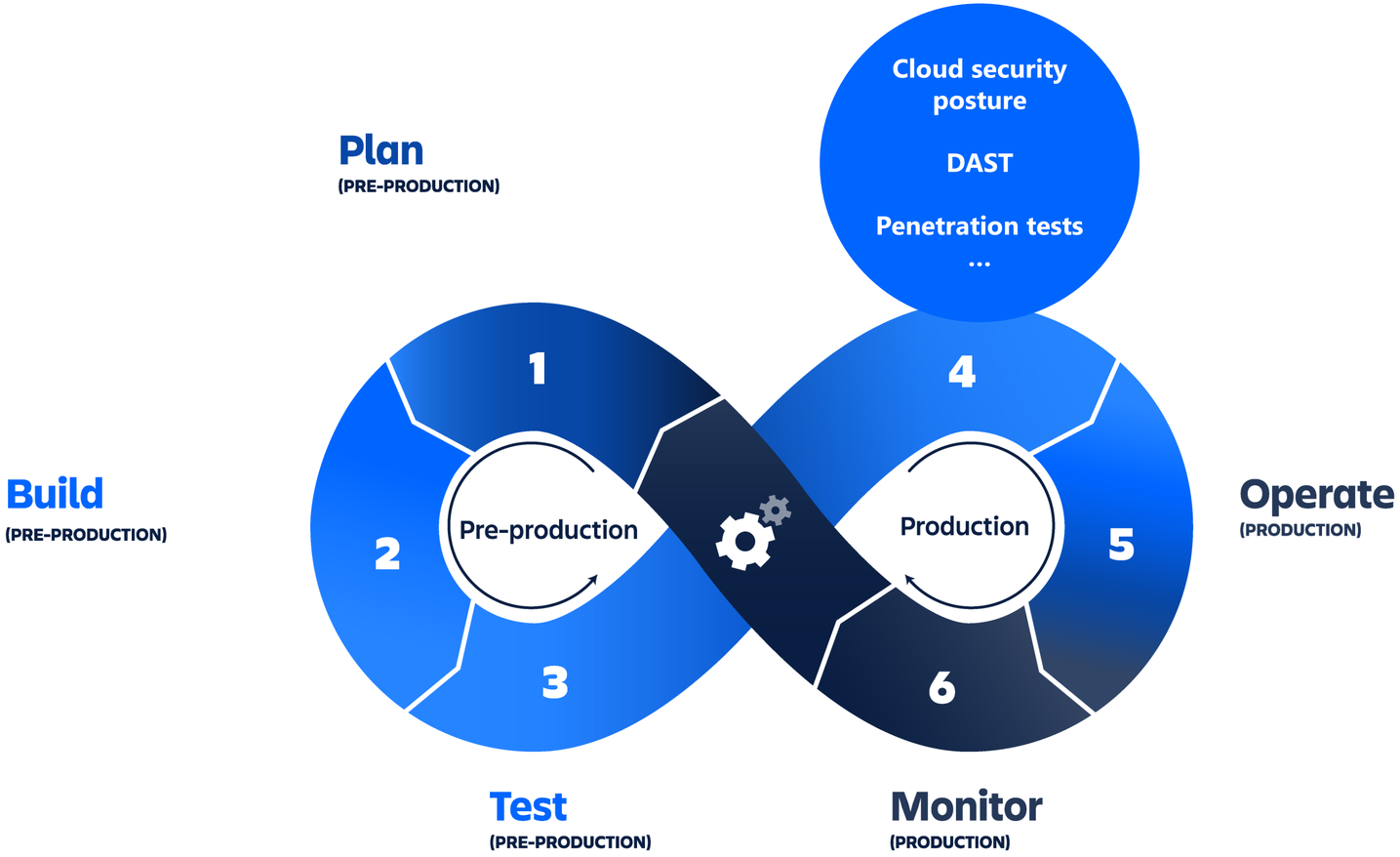


Security is the first concern of every enterprise



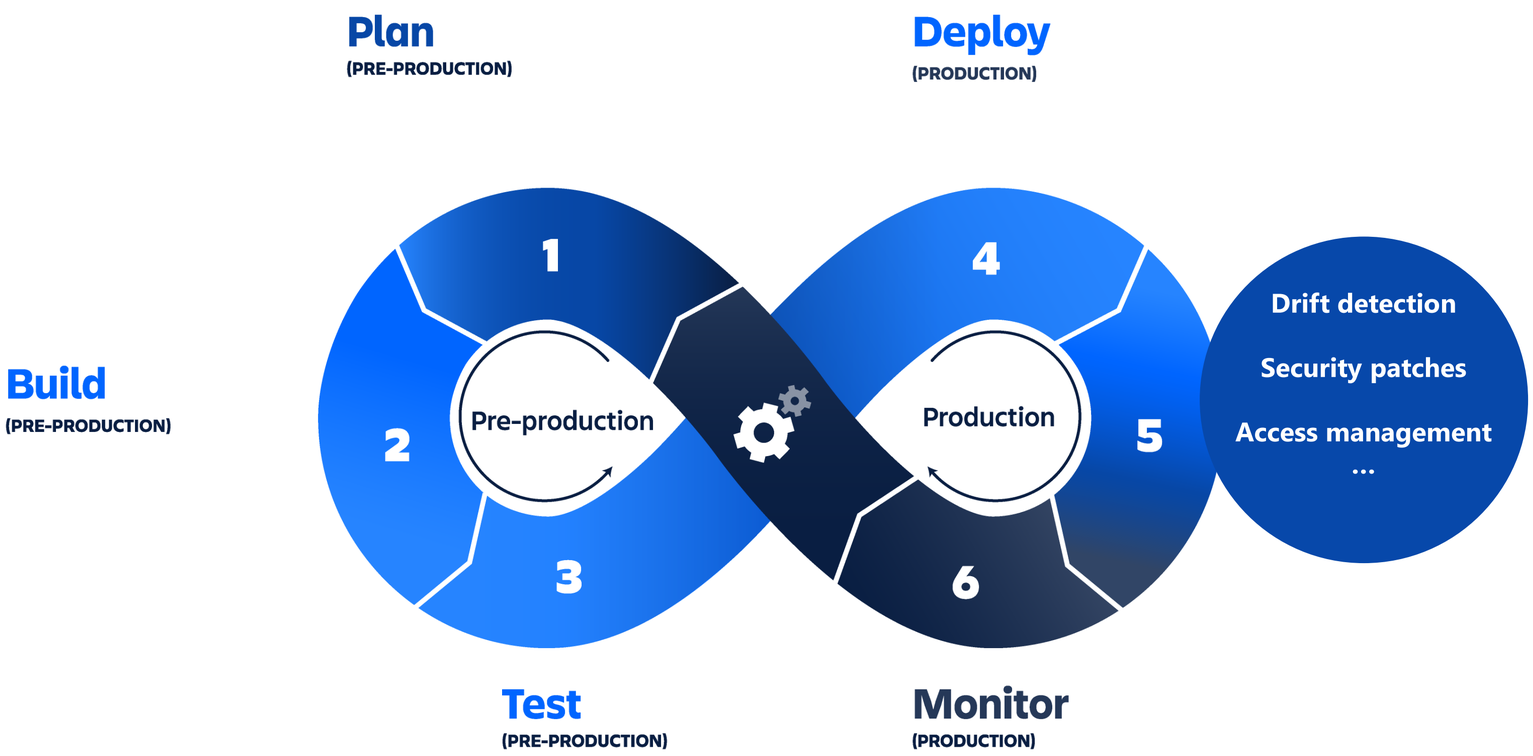
Security is the first concern of every enterprise

Bring together preventive and runtime security models



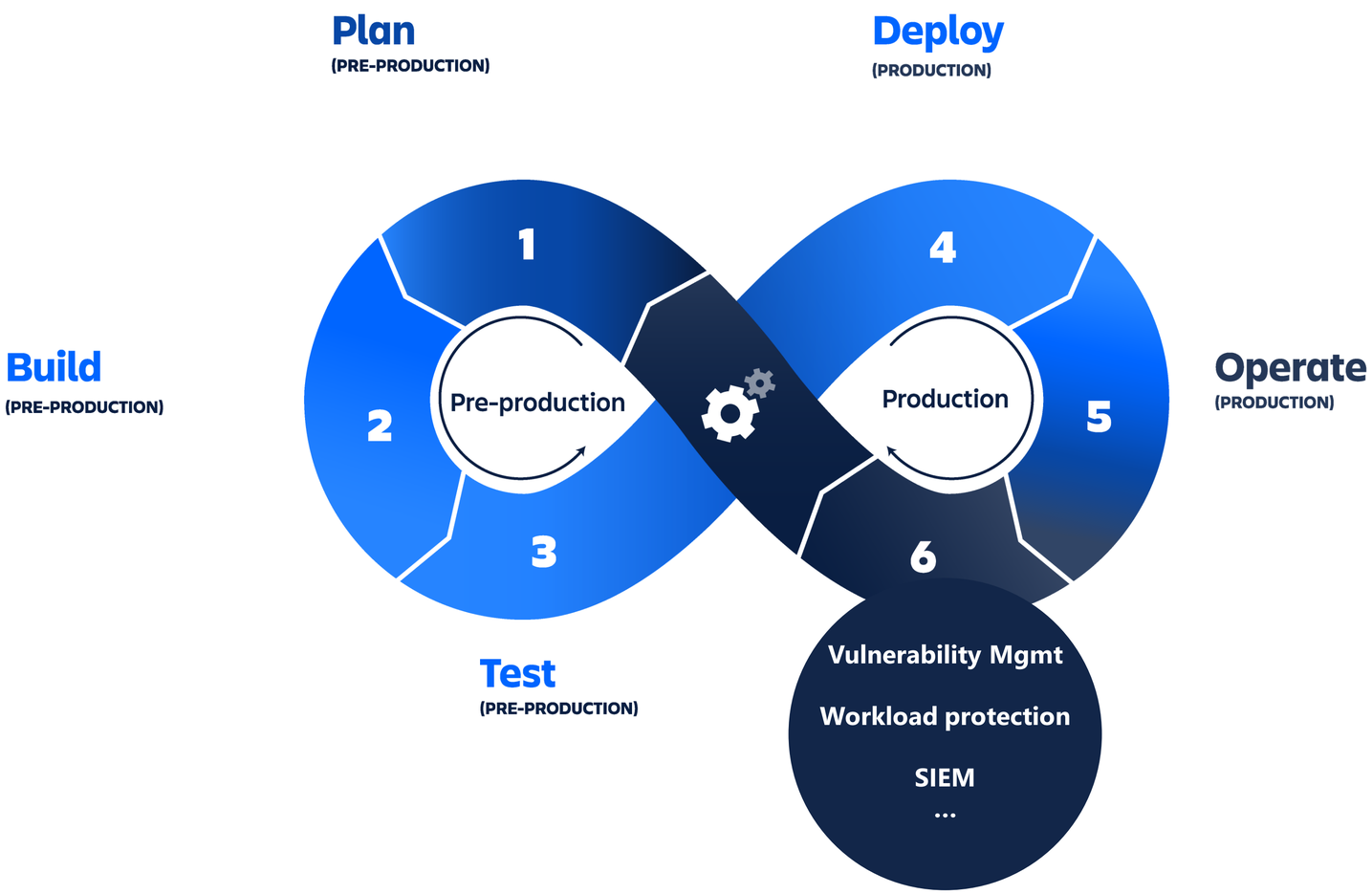
Security is the first concern of every enterprise

Bring together preventive and runtime security models

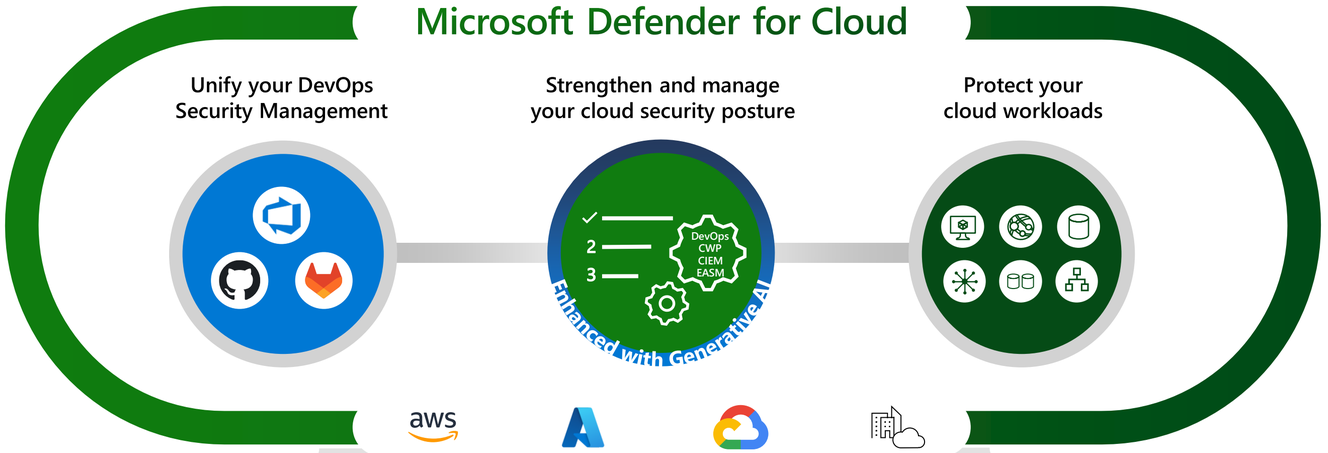


Security is the first concern of every enterprise

Bring together preventive and runtime security models



Access CNAPP capabilities in Microsoft Defender for Cloud



Integrated insights

- Application security
- External attack surface and Internet exposure
- Cloud entitlement and access permissions
- Sensitive data protection
- Network segmentation

SecOps integrations

- SIEM
- Native-XDR
- Workflow automation
- Ticketing and collaboration

Microsoft approach to API runtime security

Discovery

- Discover the APIs, classify and understand their security posture.

Protection

- Controls put in place based on best practices. Harden API configuration.

Detection

- Analysing API calls for suspicious behaviour

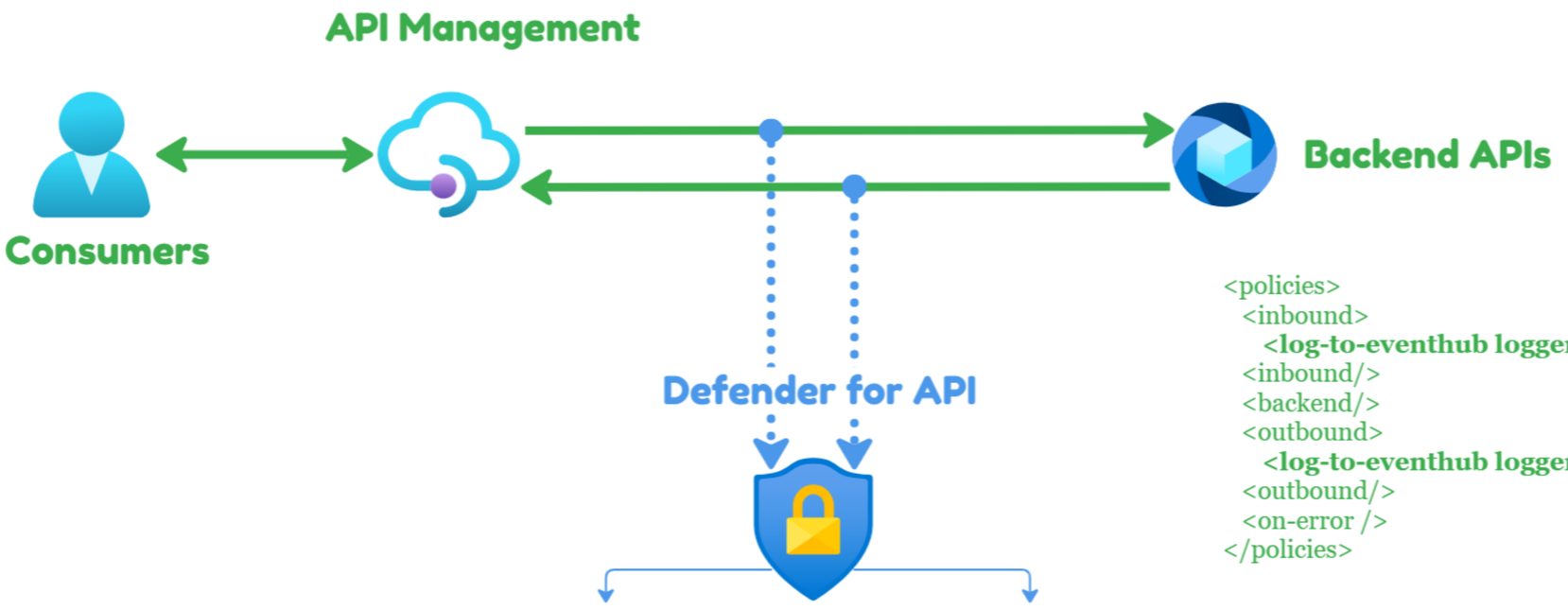
Response

- Recommends remediations methods for vulnerabilities found.

Defender for APIs : Azure API Management integration

Defender for APIs : how does it work?

Transparently mirror traffic to Defender backend




```
<policies>
  <inbound>
    <log-to-eventhub logger-id="indbound-logger">
  <inbound/>
  <backend/>
  <outbound>
    <log-to-eventhub logger-id="outbound-logger">
  <outbound/>
  <on-error />
</policies>
```

API Security Posture

- Baseline configuration check
- Authentication check
- Sensitive data security insights

API Advanced Threat protection

- Machine learning based detection
- Threat Intel based detection
- Continuous monitoring and protection for OWASP API top 10

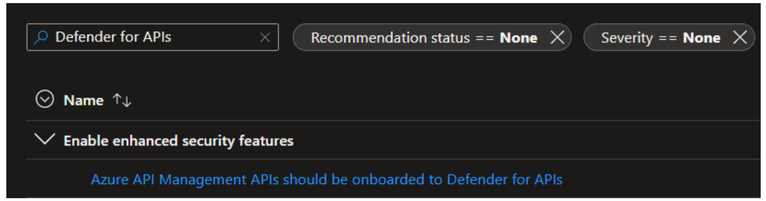
Defender for APIs : how to onboard an API?

- Enable Defender for APIs

  (Defender / Environment Settings / Defender plans)

- Onboard an API Management instance

  (Defender / Recommendations)



- Analyse

  (Defender / Workload Protections / API Security)

Our scenario

4 weeks traffic observation

400M+

Observed traffic

1.21TiB

Data Transfer

60+

Countries

5M

Distinct IP addresses

What did we learn?

Defender for APIs : API security posture

Classify APIs that handle sensitive data and supporting risk prioritization

94% of organizations say the most important API security feature is the ability to identify APIs with sensitive data[1]

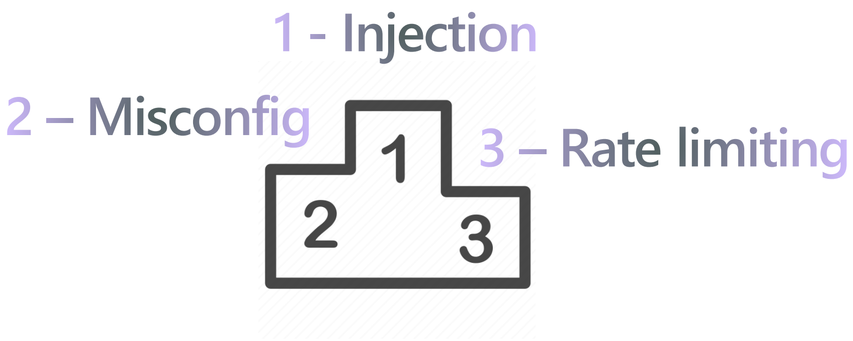
30 Days unused	Authentication	External traffic observed date (UTC)	Data classifications
Active	Authenticated		Azure Storage Account Key (Generic)
Active	Authenticated		EU National Identification Number
Active	Authenticated		International Banking Account Number (IBAN)
Awaiting data	Awaiting data	Awaiting data	
Awaiting data	Awaiting data	Awaiting data	
Active	Authenticated		

1 - PaloAlto Report : Securing the API Attack Surface 2023

Defender for APIs : API security posture

Harden API configurations and assess APIM gateway for security best practice controls

23% **The second most common OWASP TOP 10 API attack is #7 Security Misconfiguration** [1]



API Management security assessment :

- APIM minimum version
- Named value integration with KeyVault
- Check whether the certificate validation follow best practices.
- Avoid all-scope subscription keys.
- Backend authentication
- … more

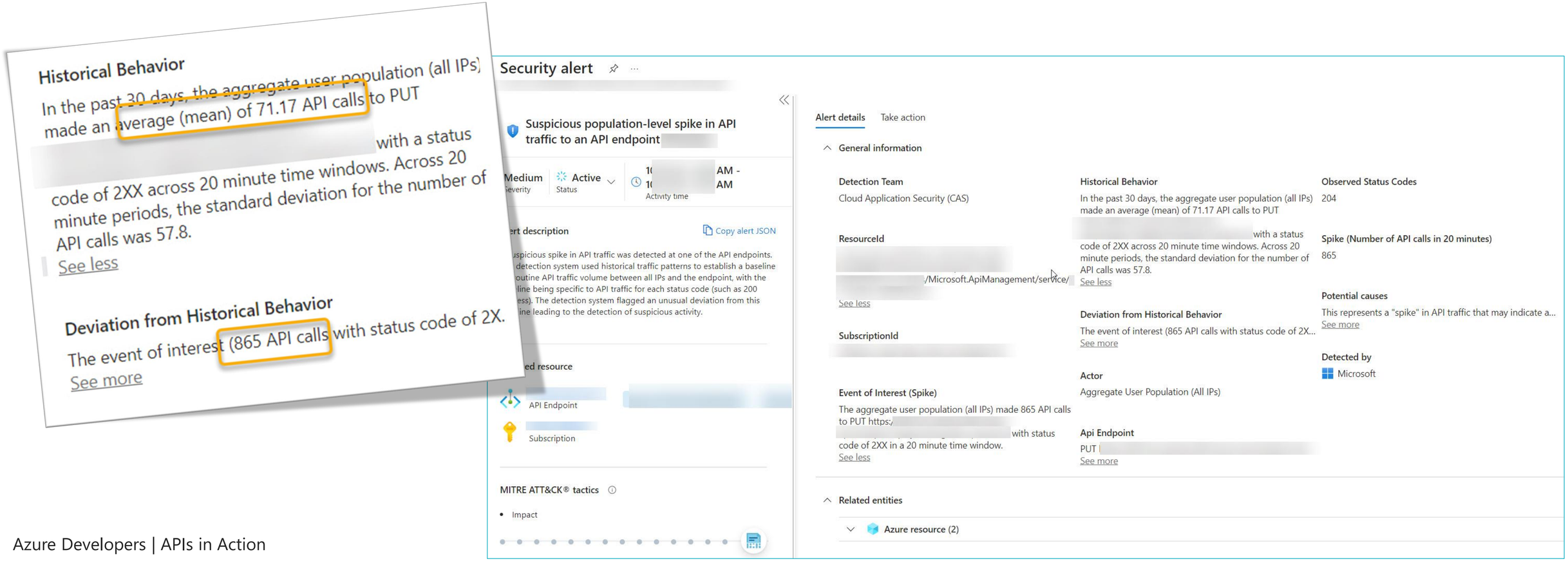
1 - Salt Security : State of API Security 2023

Defender for APIs : Advanced threat protection scenarios

- Detect spike in API requests to a single endpoint

OWASP TOP 10 API Targeted vulnerabilities:

- Lack of rate limiting
- Broken user level authentication

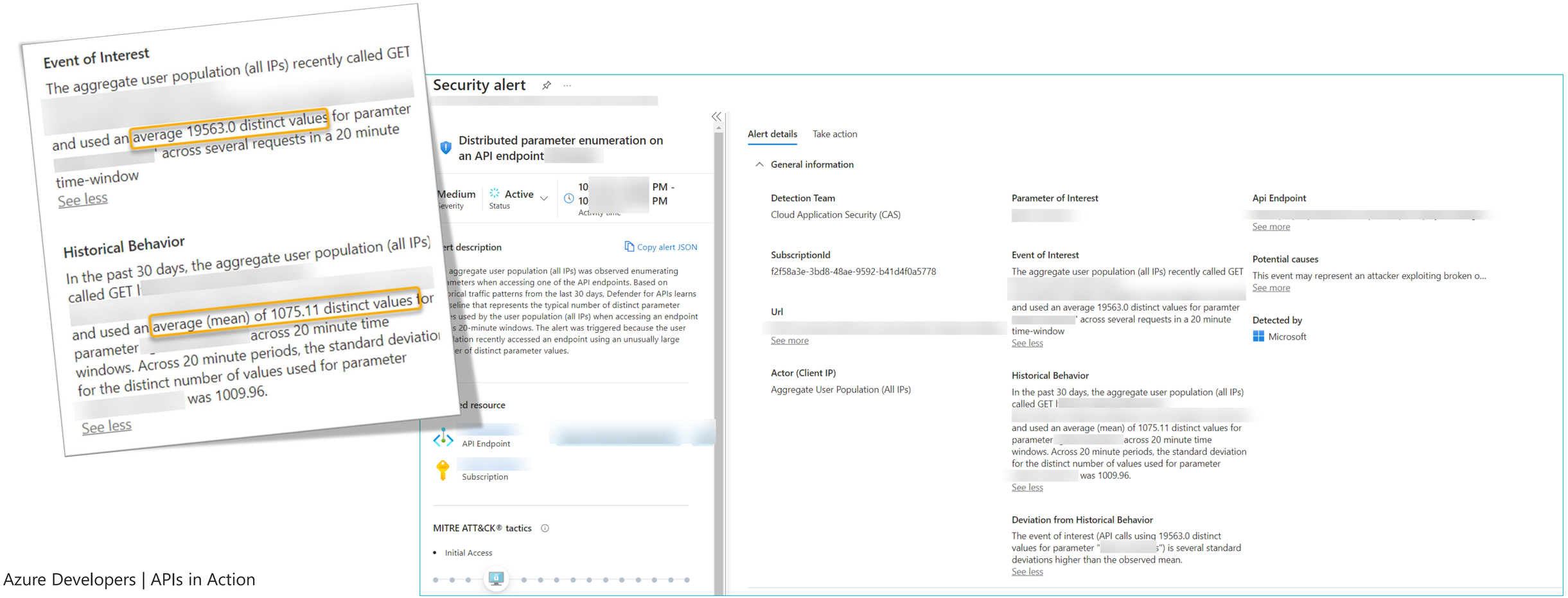


Defender for APIs : Advanced threat protection scenarios

- Users enumerate through API's parameters to expose sensitive information

OWASP TOP 10 API Targeted vulnerabilities:

- **Broken object level authentication**



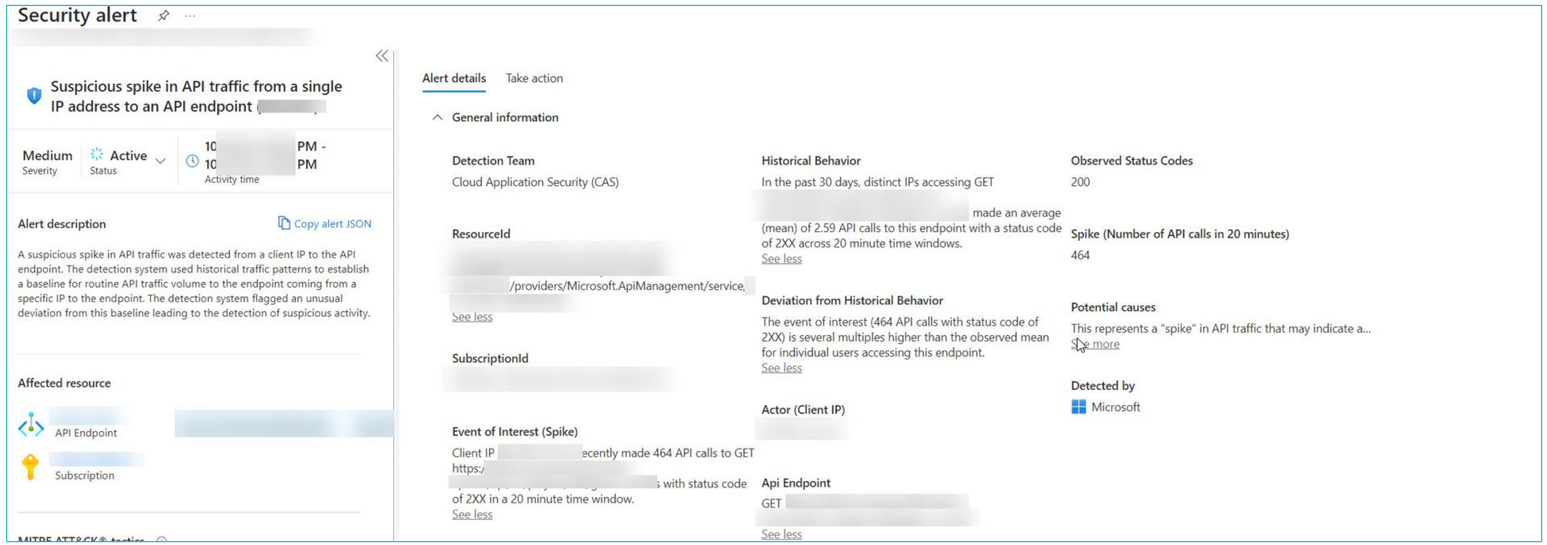
Defender for APIs : Microsoft threat intelligence

- IPs that Microsoft threat intelligence has associated with suspicious activities

OWASP TOP 10 API Targeted vulnerabilities:

- Lack of rate limiting

Severity	Alert name	Affected resource	Resource Group	Activity start time (UTC
High	API Endpoint access from suspicious IP			
High	API Endpoint access from suspicious IP			
High	API Endpoint access from suspicious IP			
High	API Endpoint access from suspicious IP			



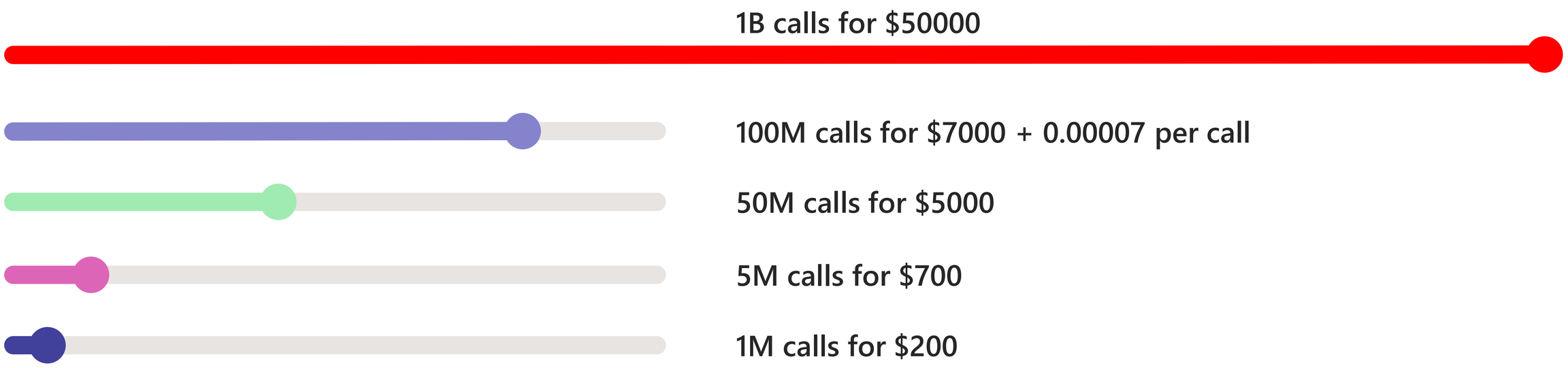
Defender for APIs : Advanced threat protection scenarios

- Detect spike in API requests to a single endpoint
- Detect unusually large API payload
- Detect parameter enumeration
- Detect spikes by a single identity
- Detect unseen parameters
- Malicious IP Address
- Suspicious User-Agents
- Access from TOR exit node
- …

Broken Authentication
Broken Object Level Authorization
Lack of Resource & Rate Limiting
Injection
Excessive Data Exposure
Security Misconfiguration
Improper Inventory Management
…

Defender for APIs : business model

- Pay per pack of APIs + overage (per transaction)



Defender for APIs : GDPR model

Data is retained within the geo boundary. For EU customers, data does not leave the EU boundaries.

- IP addresses are retained for a period of 30 days.
- API request and response bodies are retained for a period of 48 hours (only used for the data classification capability).

The raw HTTP traffic logs are processed by Microsoft backend systems.

- Only resulting metadata (e.g., data classifications, security insights) are displayed to the customer.
- In the case of security alerts, the security alerts themselves will contain the attributed “suspicious” IP address to be used by the customer SOC teams for investigation & remediation.

Defender for APIs does honour GDPR requirements.

- For GDPR DSR Delete requests – No data in-scope for GDPR is retained for longer than 30 days (i.e., all in-scope data already has a max retention for 30 days.
- For GDPR DSR Export requests – Only applicable to in-scope data retained >48 hrs. (i.e., only the IP address).

Thank you