42 crunch

31 January 2023

Protect Your APIs with Microsoft Azure Sentinel and 42Crunch Platforms

Colin Domoney

Chief Technology Evangelist

Introduction

About the Speaker

Colin Domoney

Chief Technology Evangelist

Editor of APISecurity.io
CyberProof, Veracode, CA, Deutsche Bank

Housekeeping Rules

- All attendees muted
- Questions via Q&A
- Recording will be shared
- Polling questions

Agenda

- APIs under attack — why, what, who
- 42Crunch approach to API security — Shift-Left, Shield-Right
- 42Crunch firewall — native API protection
- Live demo
  - 42Crunch protection micro-firewall demonstration
  - Detecting common attack scenarios
  - Sentinel walkthrough
- Benefits of the solution
- Questions and Answers

APIs under attack

Why, what, who

APIs are now the top attack vector

- Public APIs approaching **200 million**
- Most organizations are reliant on APIs
- **91% of organizations** experienced a security incident related to APIs in 2020

Additionally, APIs are a great target for attackers:

- They are easily **discoverable**
- They are well **documented**
- Attacks can be easily **automated**
- **Excellent tools** exist to automated attacks

https://devops.com/api-sprawl-a-looming-threat-to-digital-economy/

What is the threat to your APIs?

Who is attacking your APIs?

”Script kiddies”	Generally lower skilled attackers utilizing publicly available tools to attack APIs either for mischief or notoriety.
Scrapers and bots	Scrapers can exfiltrate data via APIs for reselling, and bot farms can launch sophisticated large-scale attacks against public APIs.
Hackers	This is the most dangerous attacker – highly skilled with advanced techniques. They are usually incentivized for financial gain or political/social motives.

The dangers in your API inventory

Shadow APIs	These APIs are invisible to the security team — usually built in a clandestine manner to meet urgent business requirements. Public cloud adoption has driven shadow IT and represents an unquantified risk to an organization.
Zombie APIs	This API is typically a deprecated or outdated API that remains active to support legacy systems. Often these APIs are not maintained or patched representing a significant risk to an organization.
Misconfigured APIs	Cloud infrastructure and frameworks have fueled API growth; however, the complexities of these environments often result in APIs that are misconfigured (insecure defaults, missing security controls, etc.)
“Frankenstein” APIs	Similar to shadow APIs, these are developed in a non-standard fashion often outside of standard governance and security processes resulting in increased risk.

Common API attack types

Bot Attacks

Bots are increasingly becoming a scourge of the security industry — and APIs are particularly vulnerable to attack given their lack of user interface.

Credential Stuffing Attacks

Any endpoint or authorization mechanism accepting a password as an input is susceptible to credential attacks using common password dictionaries. Defenses include rate limiting on such endpoints and multi-factor authentication.

API Discovery and Endpoint Enumeration

As a first stage, an adversary will attempt to gain knowledge of the APIs and their endpoints. This can range from relatively primitive methods such as the use of nmap to discover open connections, pen testing tools, etc

Account Takeover Attacks

Related to credential stuffing attacks is the broader topic of account takeover. Techniques here include the exploitation of password reset processes, which are often exposed as an API endpoint.

Denial-of-Service Attacks

The least subtle of API attacks is a simple denial-of-service attack intended to take an API offline by overloading the underlying servers. Botnets can launch massively parallelized attacks against an API.

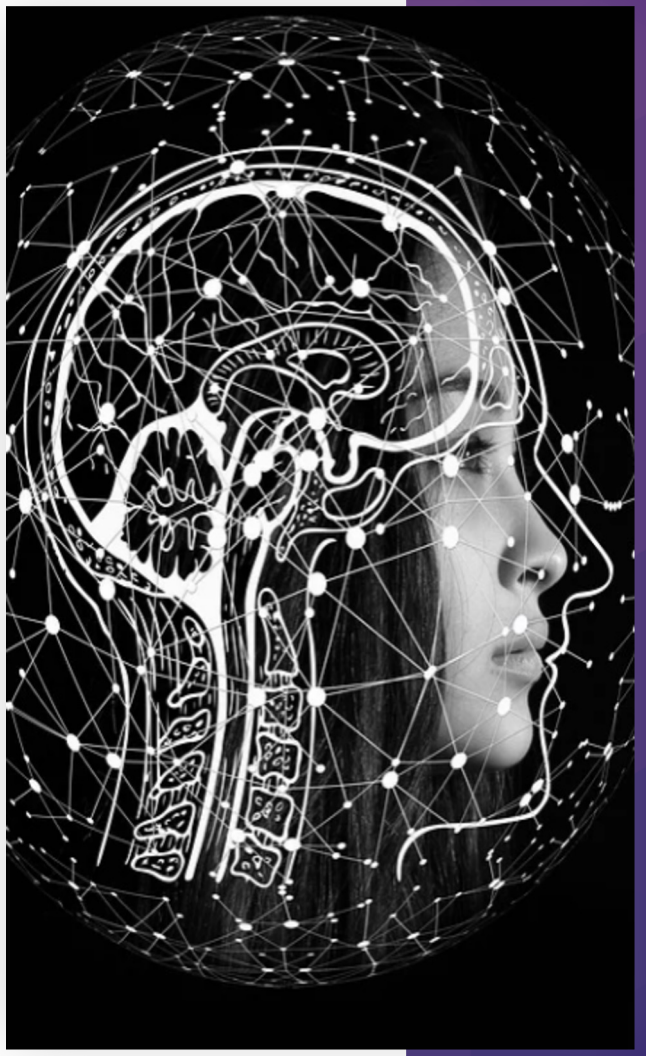
API Scraping and Pagination Attacks

APIs exist to serve data to end-users and websites. Using bots or scripts, it is possible to scrape APIs to effectively download the entire data store, which may derive the data owner of revenue streams. Typical examples include scraping price, availability info.

Question One:

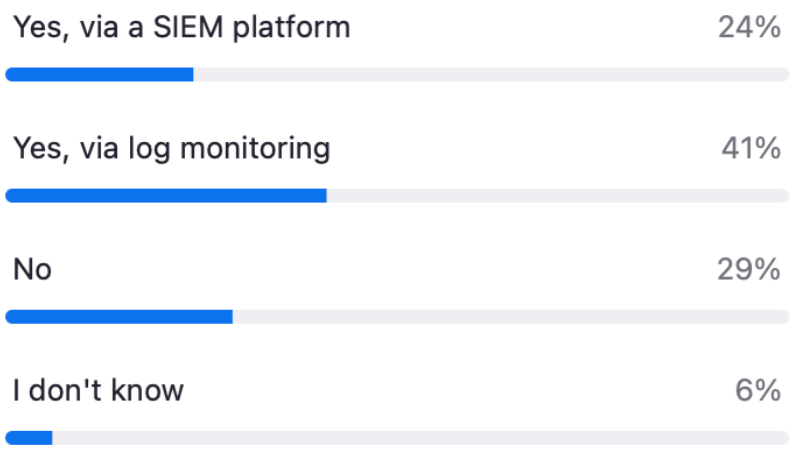
Are you currently monitoring your APIs in production?

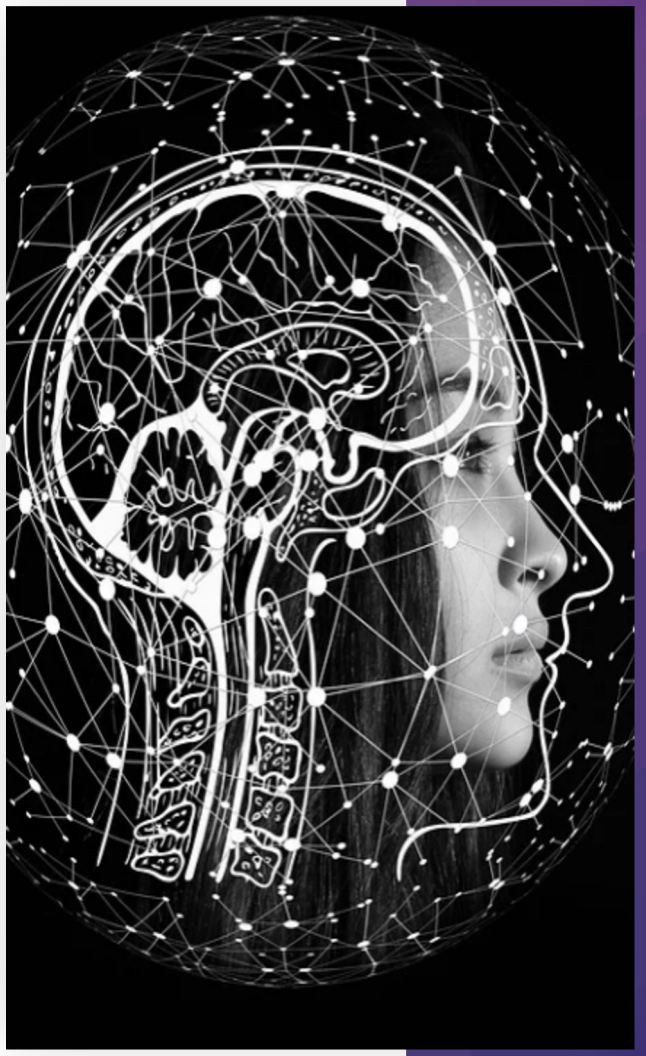
1. Yes, via a SIEM
2. Yes, via log monitoring
3. No
4. I don’t know



Question One:

Are you currently monitoring your APIs in production?





Our approach to API security

Shift-Left and Shield-Right

The benefits of Shift-Left for API security

- **Reduced cost** of deployment and rework
- **Reduced risk exposure** due to early elimination of vulnerabilities
- **Improved developer awareness** of security concerns and best practice
- **Secure by design**, rather than by testing

The challenges with Shift-Left

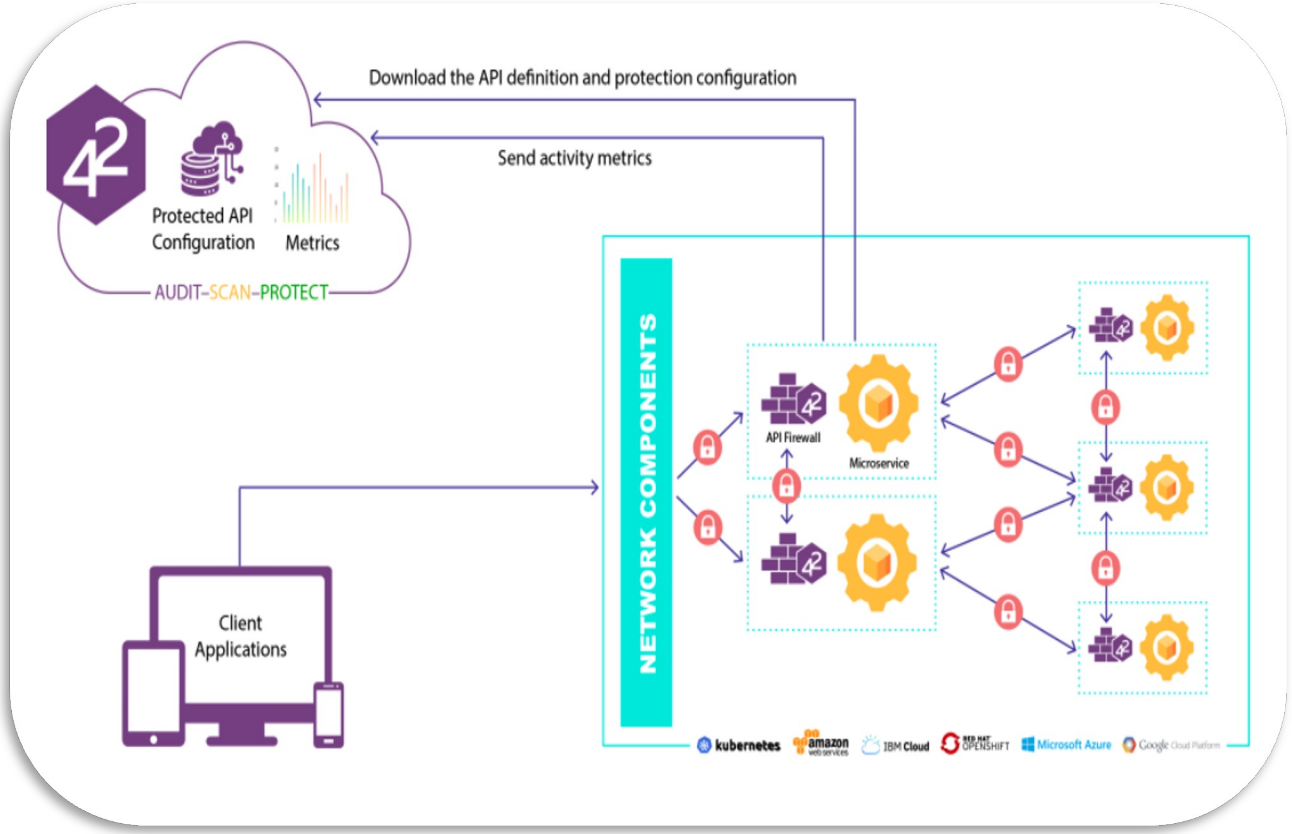
- Lack of established **DevOps process**
- **Legacy systems**
- **Shadow IT, “Frankenstein” APIs**
- **3rd party or partner APIs**
- **“Code-first” development** (lack of OAS definitions)

Protecting at runtime with Shield-Right

42Crunch protection micro-firewall offers:

- Acts as a reverse-proxy in front of API
- Protection of APIs according to OAS definition
- Designed for Cloud native deployments (K8S injection)
- Highly optimized for performance and footprint
- Provide additional capabilities such as:
  - Rate limiting
  - Security headers
  - JWT validation

and provides visibility via central logging to 42Crunch or SIEM platforms



Continuous API Security

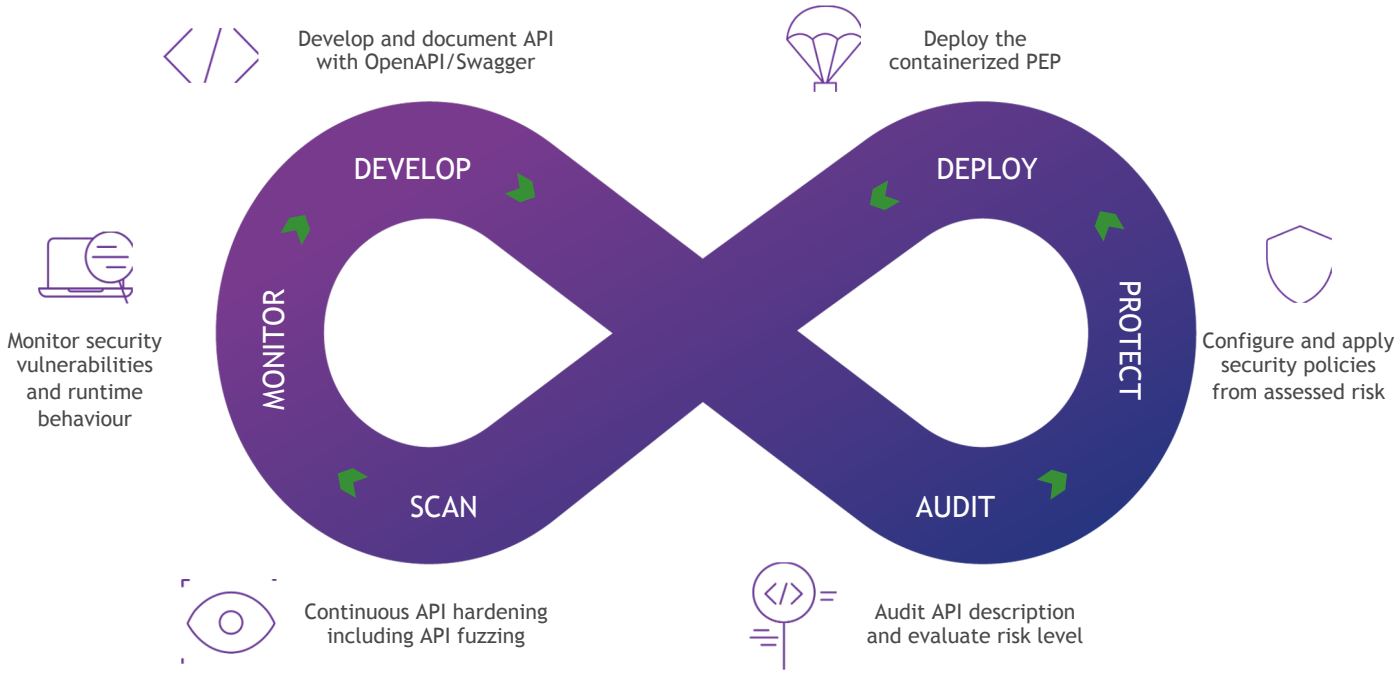
AUTOMATE & SCALE API SECURITY TO PROTECT YOUR APIs

SHIFT LEFT

- Growing recognition of need to include security at design time
- *Security as code for a seamless DevSecOps experience*
- *Embed and **automate security** in the API development CI/CD pipeline.*

SHIELD RIGHT

- *Security teams retain control and visibility of the **enforcement** of API security policies.*
- ***Low-footprint** containerized PEP enforces all policies at runtime.*



What is Microsoft Sentinel?

"Microsoft Sentinel is a **cloud-native** security information and event manager **(SIEM)** platform that uses **built-in AI** to help **analyze large volumes of data** across an enterprise – **fast.**"

- First-class component of Microsoft Azure (and Office 365) – comes for free*
- Integrates frictionlessly with ALL Azure and O365 data sources
- Integrates with a wide-range of 3rd party components (i.e. F5, etc.)
- Uses Log Analytics as underlying data source (can ingest other sources via Log Analytics)
- Leverages Microsoft's strategic position:
  - Vast source of threat intelligence
  - Microsoft's AI/ML capabilities

What is Microsoft MISA?

42Crunch Expands Collaboration with Microsoft by Joining Microsoft Intelligent Security Association

Collaboration Consolidates End-to-End API Security Experience for the Enterprise

San Francisco, January 10, 2023

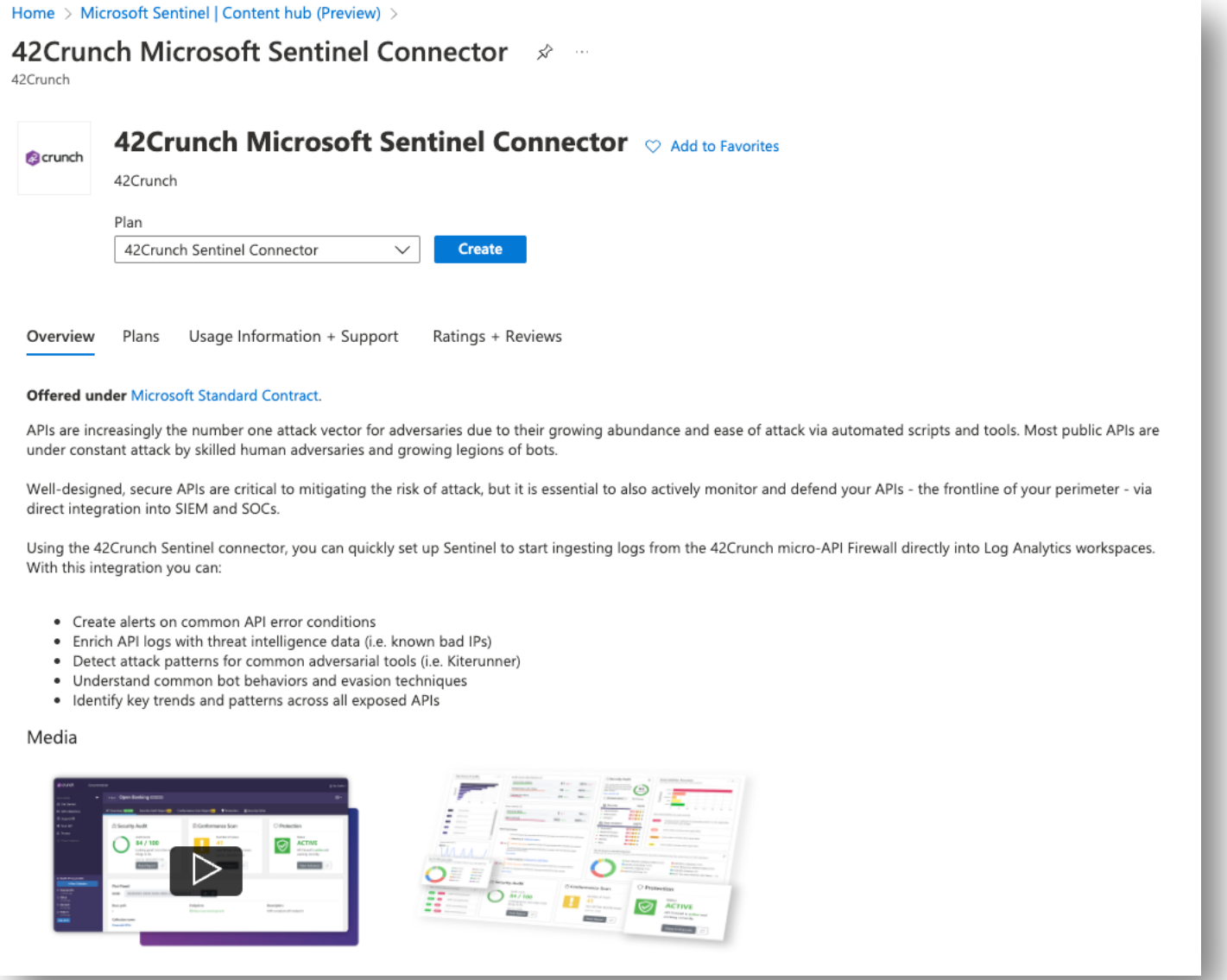
Member of
Microsoft Intelligent Security Association

Microsoft

The 42Crunch Sentinel integration

- Using the 42Crunch Sentinel connector, you can quickly set up Sentinel to start ingesting logs from the 42Crunch micro-API Firewall directly into Log Analytics workspaces. With this integration you can:

- Create alerts on common API error conditions
- Enrich API logs with threat intelligence data (i.e. known bad IPs)
- Detect attack patterns for common adversarial tools
- Understand common bot behaviors and evasion techniques
- Identify key trends and patterns across all exposed APIs



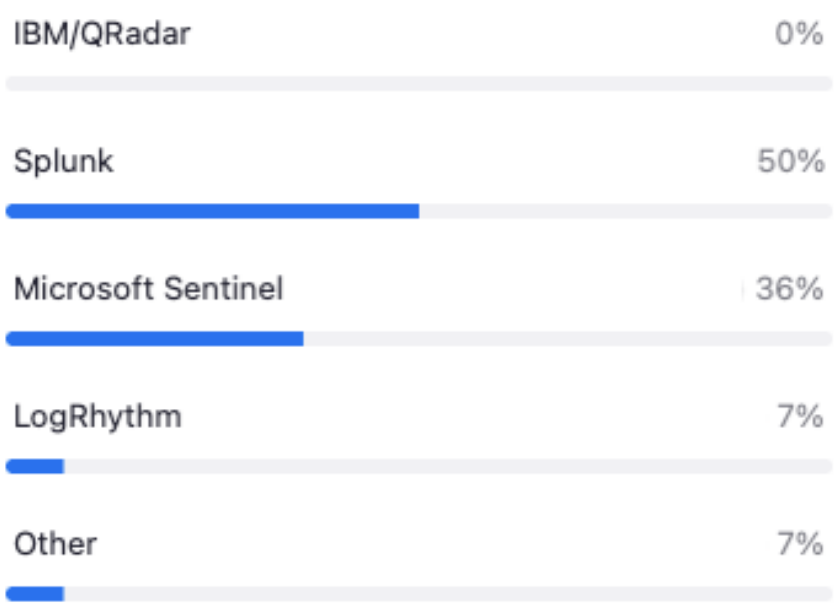
Question Two:

If you are using a SIEM, which one?

1. IBM / QRadar
2. Splunk
3. Microsoft Sentinel
4. LogRhythm
5. Other

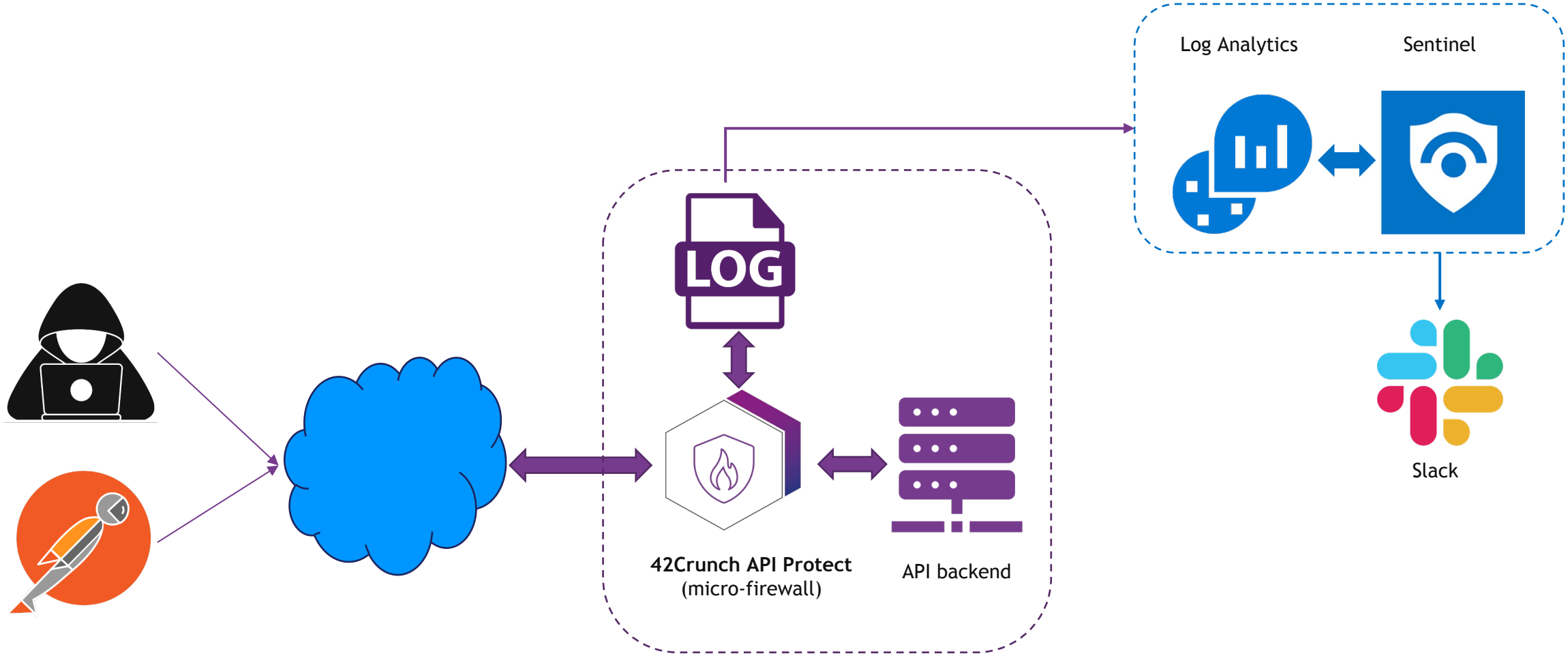
Question Two:

If you are using a SIEM, which one?



Live demo

Demo environment architecture



What attacks did we see on our API “honeypot”?

Run | Time range : **Set in query** | Save | Share | New alert rule | Export

```
guardian_log_1_CL | where TimeGenerated >= ago(45d) |
where LogType_d == 2 and Error_Step_s contains "hostpath" |
project-away Non_blocking_mode_b, Source_Port_d, Destination_Port_d,
Query_s, API_ID_g, Request_Header_s, Response_Header_s, Errors_s, Type, UUID_g |
sort by TimeGenerated desc | summarize Count=count() by URI_Path=URI_Path_s | sort by Count
```

Results Chart

URI_Path	Count
/	665
/.env	65
/boaform/admin/formLogin	35
/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php	28
/shell	24
/favicon.ico	18
/robots.txt	17
/index.php	14
/solr/admin/info/system	13
/Autodiscover/Autodiscover.xml	12
/console/	12
/phpMyAdmin4/index.php	10
/phpmyadmin2013/index.php	10
/db/phpMyAdmin-5/index.php	10
/phpMyAdmin-4/index.php	10
/sql/sql-admin/index.php	10
/pma/index.php	10
/phppma/index.php	10
/sql/phpmyadmin3/index.php	10
/phpmyadmin2020/index.php	10

- .env files
- PHP files – phpMyAdmin, WordPress, SQL
- Git config
- AWS secrets
- Shell execution
- Common gateway file execution
- Directory enumeration (/home, /root)
- JavaScript file execution
- Login attempts

Evidence of active scanning for recent vulnerabilities

{* SECURITY *}

You're a botnet, you've got a zero-day, so where do you go? After fiber, because that's where the bandwidth is

Two-step attack seen on core systems

Shaun Nichols in San Francisco

Thu 16 Apr 2020 // 21:44 UTC

https://www.theregister.com/2020/04/16/fiber_routers_under_fire/

Service Exploit #7: /solr/admin/info/system?wt=json

0.48% of all web services hits.
Apache Solr – Directory traversal vulnerability.

Apache Solr is an open-source enterprise search platform built on Apache Lucene. On May 30, 2013, Apache foundation published security issue SOLR-4882 with was related to CVE-2013-6397, the affected version was 4.3. The issue was resolved in version 4.6 and a patch from September 21, 2013.

What is the risk? The vulnerability, CVE-2013-6397 allows a remote attacker to read arbitrary files on the Solr server via the "tr" parameter. This, when combined with other vulnerabilities, may lead to remote code execution on the victim server. Attackers are scanning the internet using the above URL to find the old and unpatched Solr servers that are still vulnerable to CVE-2013-6397. The attacker can use the potential of the Remote Code Execution on a compromised server.

https://blog.radware.com/security/2020/12/the-top-web-service-exploits-in-2020/

Laravel Telescope Disclosure

CVSS-5.0 | CVSS-AV:N/AC:L/Au:N/C:P/I:N/A:N

Description

Laravel has publicly accessible instances of its Telescope software. This allows seeing detailed HTTP requests, including Cookies.It leads to disclosure of sensitive information about the web application.

https://beaglesecurity.com/blog/vulnerability/laravel-telescope-disclosure.html

Scenario One — Account takeover

Attack Technique

An attacker tries to find registration or password reset APIs and tries to brute force these by guessing the reset codes.

- Submit to registration endpoint with guessed account details
- Submit to reset endpoint with guessed reset codes

Detection Strategy

Detect access to sensitive reset/register API endpoints, and fine excessive 403 errors on these endpoints.

Scenario Two — Password cracking

Attack Technique

Similar to the previous scenario, this relatively simplistic technique involves trying to guess a user's login details using a dictionary attack. Attackers may try to subvert detection by using a botnet to mask IP addresses.

Detection Strategy

The best protection against this attack is to apply rate limiting to any endpoints allowing account login.

The detection strategy is relatively simple — identify a large occurrence of 403 errors against a login endpoint in a given time window.

Scenario Three — Kiterunner detection

Attack Technique

Kiterunner is a popular reconnaissance tool used by attackers to enumerate endpoints of an unknown API. This tool uses extensive lists of popular API endpoints and attempts to scan and/or brute force access to them sequentially.

Detection Strategy

For an API protected by the 42Crunch firewall a Kiterunner attack will generate a large number (in the thousands) of 404 errors with a path mapping error. These can easily be detected on Sentinel to alert as a suspected Kiterunner reconnaissance.

Scenario Four — Anomaly detection

Attack Technique

If an attacker is unfamiliar with an API (as typical in a discovery or reconnaissance stage) they will have to attempt to discover and map the API behavior to map out the functionality.

Detection Strategy

APIs are usually exercised in a standard manner by consuming applications. This usually results in a well-understood, repeatable usage pattern.

To detect misuse or abuse it is possible to track the APIs access to deviations from usual usage patterns and flag these for review.

Scenario Five — “BOLA”

Attack Technique

Broken-object level authorization is one of the most notorious API vulnerabilities allowing access to records (objects) not owned by the caller.

Typically an attack attempts to guess object IDs and to see if poorly implemented authorization methods allow this unwanted access. Attacks may involve guessing IDs or sequencing through a range of possible values.

Detection Strategy

BOLA is a challenging vulnerability to protect and detect. A crude approach could model the usual API access and when excessive access to objects is observed to trigger as a potential issue.

Timestamp_t [UTC]	Status_d	Source_IP_s	URI_Path_s
> 5/1/2022, 12:10:50.497 PM	200	138.204.215.0	/api/login
> 5/1/2022, 12:10:50.662 PM	200	138.204.215.0	/api/users/info
> 5/1/2022, 12:10:50.763 PM	200	138.204.215.0	/api/accounts/list
> 5/1/2022, 12:10:50.863 PM	200	138.204.215.0	/api/accounts/765540
> 5/1/2022, 12:10:50.965 PM	200	138.204.215.0	/api/accounts/908344
> 5/1/2022, 12:10:51.066 PM	200	138.204.215.0	/api/accounts/323909
> 5/1/2022, 12:10:51.168 PM	200	138.204.215.0	/api/accounts/724451
> 5/1/2022, 12:10:51.269 PM	200	138.204.215.0	/api/accounts/891154
> 5/1/2022, 12:10:51.370 PM	200	138.204.215.0	/api/users/activity

Scenario Six — Suspicious login

Attack Technique

Account takeover is one of the most pervasive threats. Typically adversaries will attempt to login either via their network or VPNs/TOR nodes.

Detection Strategy

Suspicious login activity is a standard protection offered on Azure Sentinel and Azure AD.

In this example it is possible to simulate a basic detection of suspicious login – in this case if a login is detected on the same account from more than three different locations an alert is triggered.

Scenario Seven — API scraping

Attack Technique

This is more of an abuse case than an attack but still warrants detection for further investigation.

Typically, the technique involves excessive pagination of lists beyond what would normally be expected for end user UI based behavior ie. Paging from page 1 to very large numbers.

Detection Strategy

The protection is relatively simple — detect access to a URL supporting pagination and count the number of accesses within a given time window, and trigger if this exceeds a reasonable number.

Scenario Eight — Rate limiting

Attack Technique

Nothing subtle about this approach — an attacker brute forces an API endpoint trying to reset or guess a password.

Cleverer approaches will use back-off timers to avoid triggering detection.

Detection Strategy

The 42Cruch firewall has built-in support for rate limiting both globally and at operation level. If triggered the firewall with return a 429 for subsequent operation.

Using Sentinel it is possible to detect an excess of 429 responses and trigger an action to protect the API (and other infrastructure) at the network firewall level.

Scenario Nine — First-time access

Attack Technique

A user accesses an API from an IP address not previously seen on the system. Although not necessarily an attack this could be an indicator of some initial reconnaissance or discovery.

Detection Strategy

When a request is made to the system check if that IP address has previously been seen, say, in the last 7 days.

Scenario Ten — JWT validation

Attack Technique

JWTs are commonly used as an authorization mechanism and attackers use a variety of attacks against endpoints accepting tokens.

JWTs can be cloned or brute-forced in a similar manner to password cracking.

Detection Strategy

API developers should use well-proven JWT client libraries to fully validate JWTs.

The 42Crunch micro-firewall offers the capability to validate JWTs prior to passing them to the API backend. This is a high fidelity means of validating JWTs.

Scenario Eleven — Invalid host access

Attack Technique

Attackers typically scan or attack well known address ranges on popular ISPs and Cloud providers.

Detection Strategy

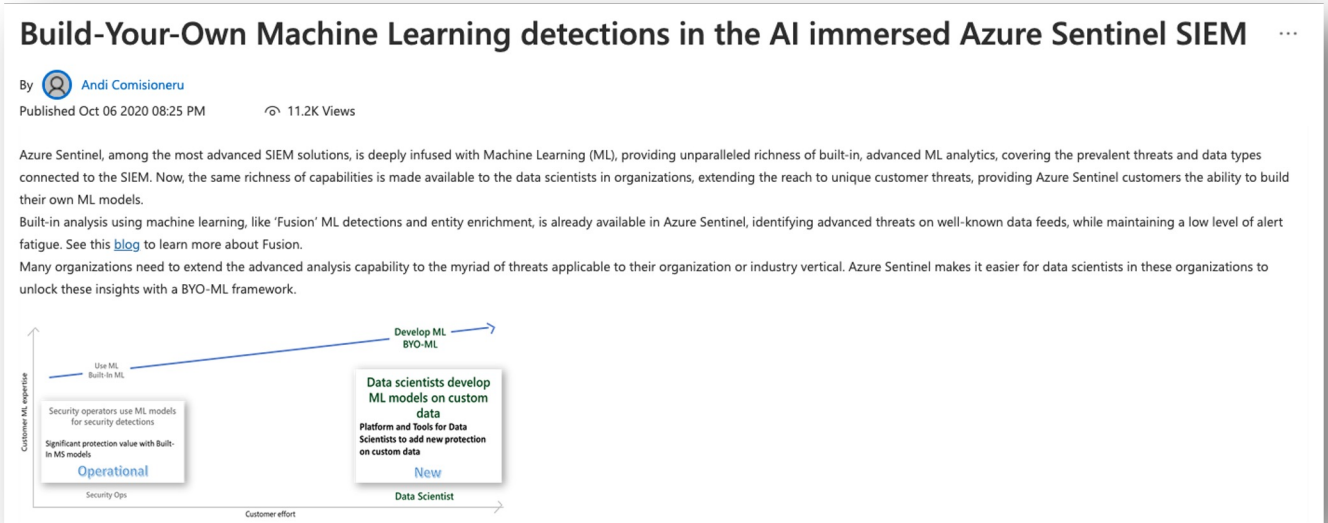
42Crunch micro-firewall block access from requests directed to IP address and requires a FQDN to access the protected API.

Attempted access with a “hostname mapping” error indicates access from an invalid/unknown client.

Use Cases / Benefits

Further enhancements and improvements

- Enrich IP address information to allow:
  - Geolocation
  - IP address threat intelligence (unknown IPs, TOR nodes, etc.)
- Automatically block/throttle attack IPs at network firewall level
- Integrate with Azure AD to disable or alert accounts under attack
- Leverage Azure ML capability to detect anomalous behavior
  - Attacks against known vulnerabilities
  - Business logic errors and abuse



Build-Your-Own Machine Learning detections in the AI immersed Azure Sentinel SIEM

By Andi Comisioneru
Published Oct 06 2020 08:25 PM 11.2K Views

Azure Sentinel, among the most advanced SIEM solutions, is deeply infused with Machine Learning (ML), providing unparalleled richness of built-in, advanced ML analytics, covering the prevalent threats and data types connected to the SIEM. Now, the same richness of capabilities is made available to the data scientists in organizations, extending the reach to unique customer threats, providing Azure Sentinel customers the ability to build their own ML models.

Built-in analysis using machine learning, like 'Fusion' ML detections and entity enrichment, is already available in Azure Sentinel, identifying advanced threats on well-known data feeds, while maintaining a low level of alert fatigue. See this blog to learn more about Fusion.

Many organizations need to extend the advanced analysis capability to the myriad of threats applicable to their organization or industry vertical. Azure Sentinel makes it easier for data scientists in these organizations to unlock these insights with a BYO-ML framework.

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/build-your-own-machine-learning-detections-in-the-ai-immersed/ba-p/1750920

Benefits and advantages

Cost reduction	Avoid duplication of costs associated with buying and operating a dedicated API security monitoring tool, and instead add to the value of your existing investment in SIEM/SOC solutions by enriching with API logs and alerts.
Accuracy	Using a dedicated API micro-firewall capable of inspecting API traffic at the API level (layer 7) against an OAS definition rather than relying on network traffic inspection (layer 4).
Simplicity	The biggest cost with security operations is the SOC operators and analysts. By surfacing API logs and alerts into existing SOCs avoid the complexity of operating a separate platform.
Integration	For Azure users direct integration with, for example, firewalls, NSGS, Azure AD, etc. implement protection and detections via API logs and alerts.
Hot fixes	If emerging threats are detected in real-time a protection can be ‘patched’ into the OAS definition and immediately redeployed — almost instant hot fixes !

Recent News

42Crunch Expands Collaboration with Microsoft by Joining Microsoft Intelligent Security Association

Collaboration Consolidates End-to-End API Security Experience for the Enterprise

San Francisco, January 10, 2023

Member of
Microsoft Intelligent Security Association

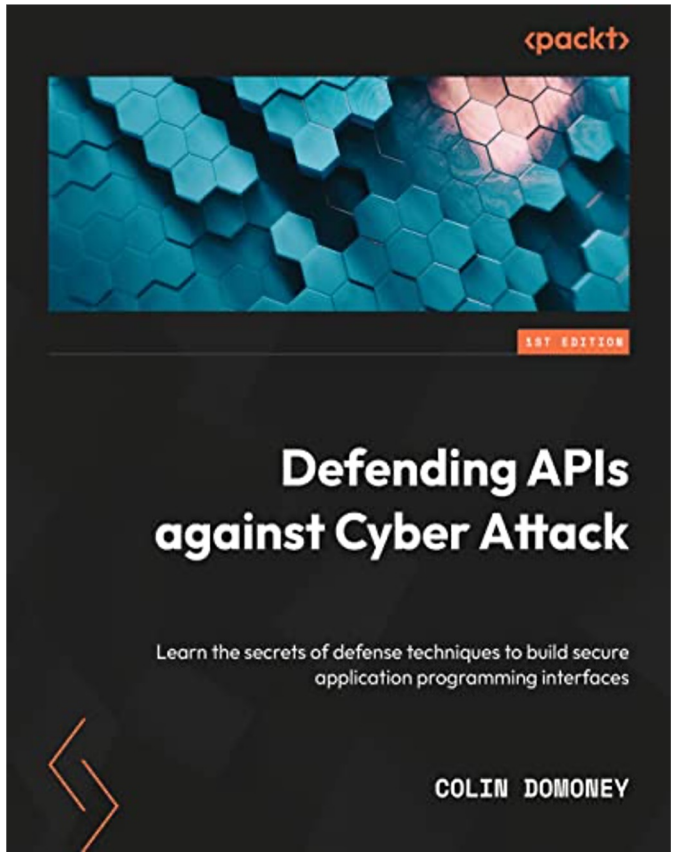
Microsoft

Learning more

#1 API Security Newsletter
APISecurity.io

https://apisecurity.io/

"Defending APIs against Cyber Attack"
by Colin Domoney

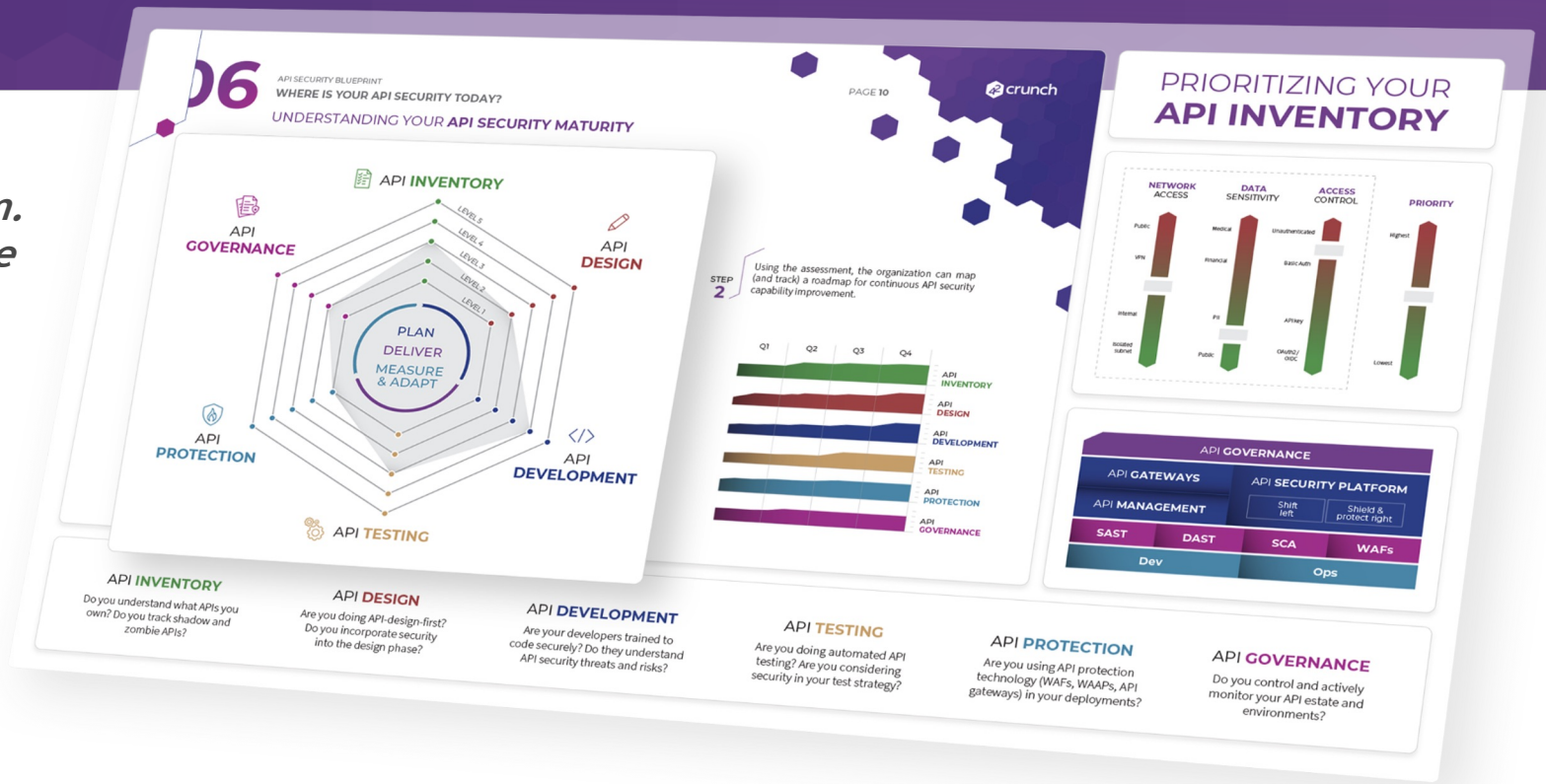


https://amzn.to/3fHp8Mz

Guide

API Security: A Blueprint for Success

- *Practical Guide on an API Security program.*
- *Map your enterprise's API security posture against 6 key domains.*
- *Champion the case for API Security.*



Download Guide here: https://42crunch.com/ebook-api-security-blueprint/

Events

Upcoming Events

Register to attend link
https://resources.github.com/github-at-cloudnativesecuritycon-2023/?