42crunch

CyberProof
A UST Global Company

4 May 2022

Actively Monitor and Defend Your APIs with 42Crunch and the Azure Sentinel Platform

Colin Domoney

API Security Research Specialist & Developer Advocate

Saggie Haim

Cloud Security Solutions Architect Team Leader

Introduction

About the Speakers

Colin Domoney

API Security Research Specialist & Developer Advocate

42Crunch

Saggie Haim

Cloud Security Solutions Architect Team Leader

CyberProof

Agenda

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

APIs under attack

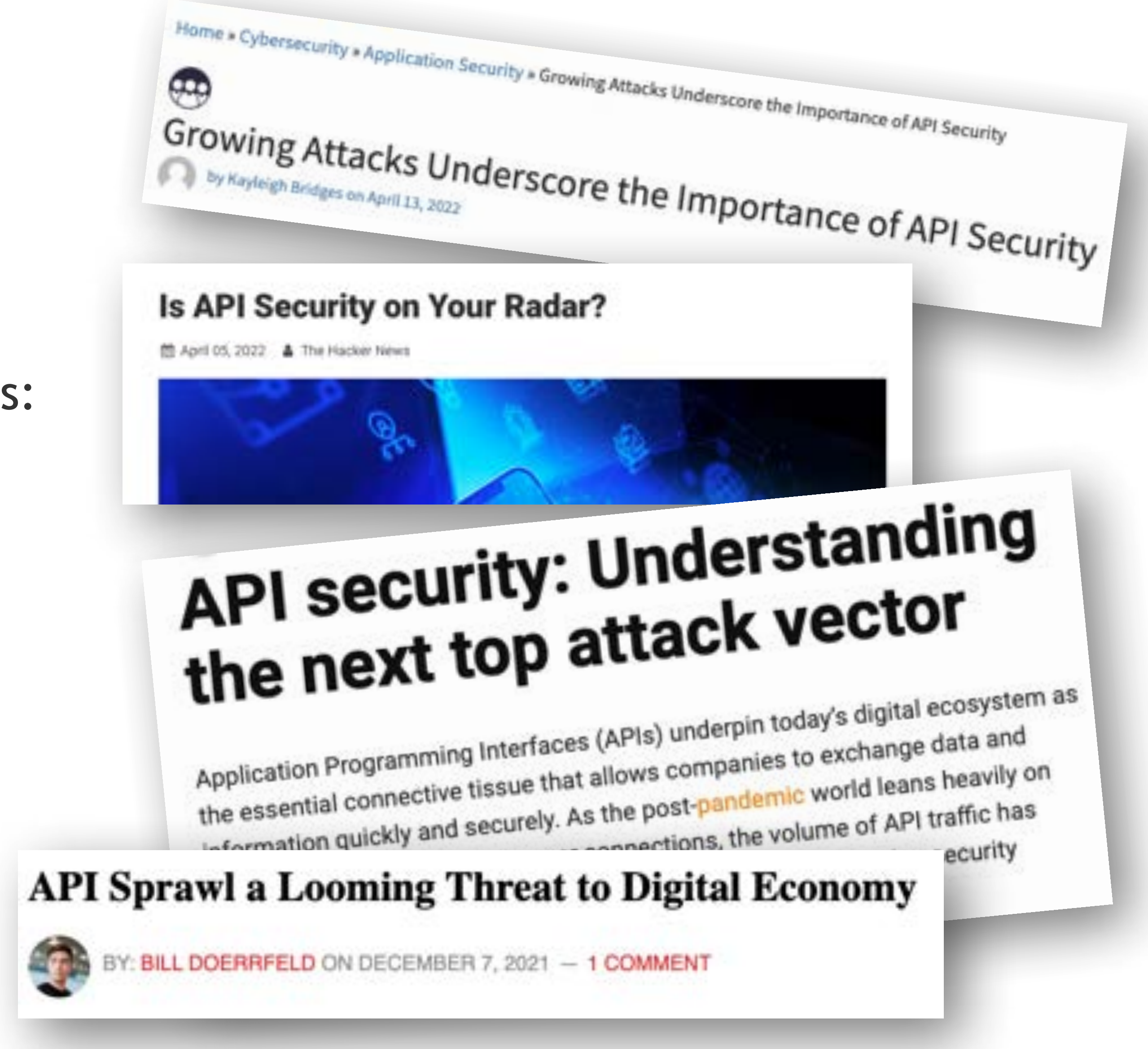
Why, what, who

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



Home » Cybersecurity » Application Security » Growing Attacks Underscore the Importance of API Security

Growing Attacks Underscore the Importance of API Security

by Kayleigh Bridges on April 13, 2022

Is API Security on Your Radar?

April 05, 2022 The Hacker News

API security: Understanding the next top attack vector

Application Programming Interfaces (APIs) underpin today's digital ecosystem as the essential connective tissue that allows companies to exchange data and information quickly and securely. As the post-pandemic world leans heavily on connections, the volume of API traffic has ecurity

API Sprawl a Looming Threat to Digital Economy

BY: BILL DOERRFELD ON DECEMBER 7, 2021 — 1 COMMENT

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.

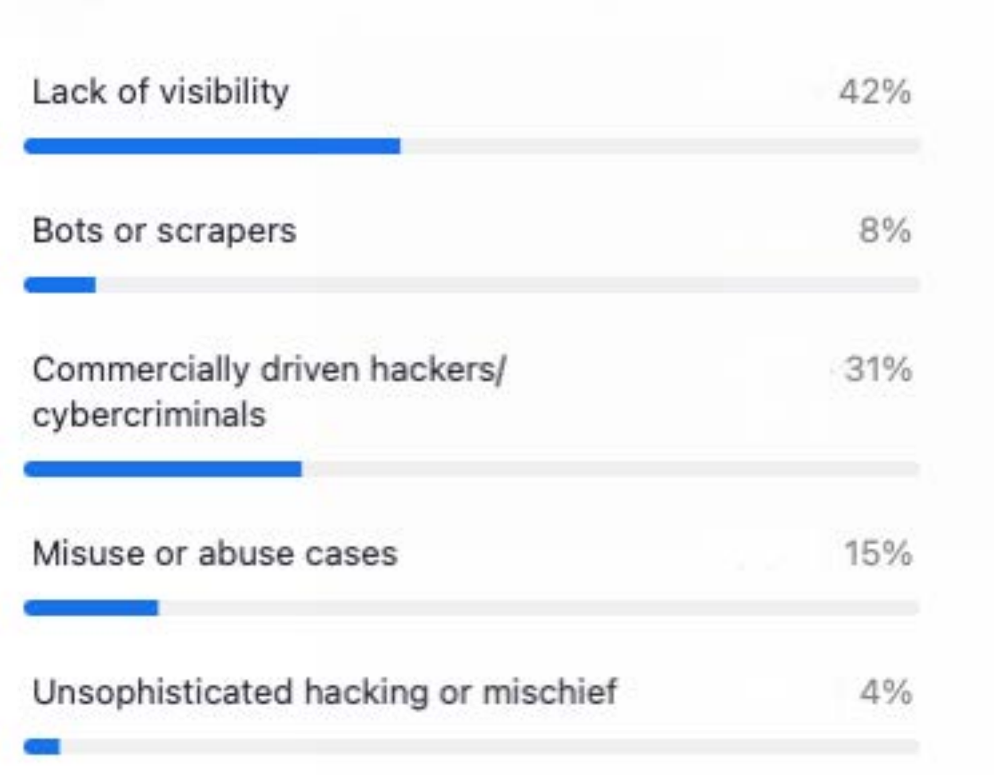
Question One:

What is the #1 threat against your organization’s APIs? (single choice)

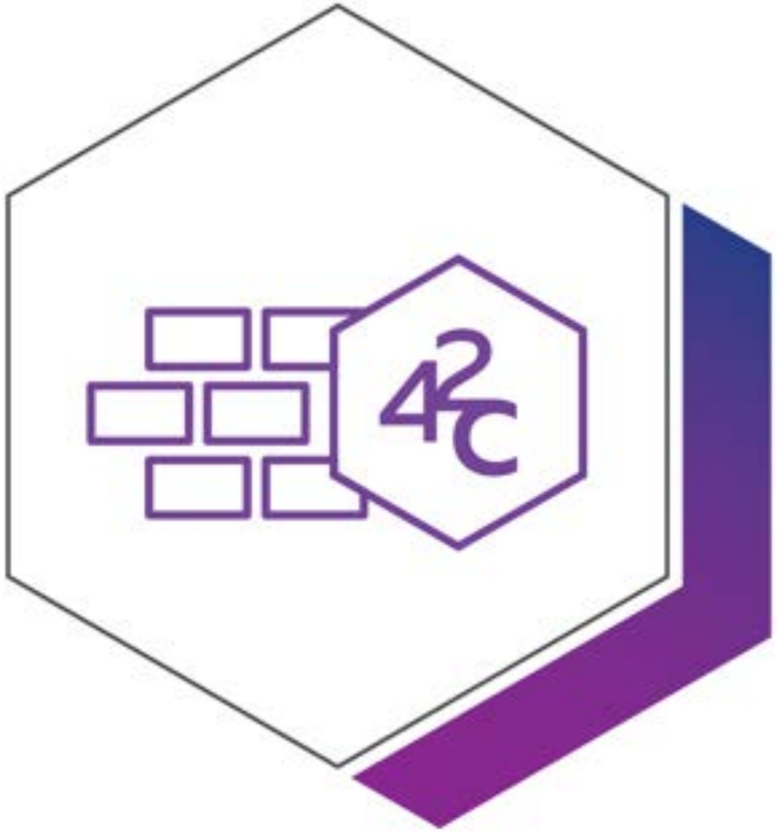
1. Lack of visibility
2. Bots or scrapers
3. Commercially driven hackers/cybercriminals
4. Misuse or abuse cases
5. Unsophisticated hacking or mischief

Question One:

What is the #1 threat against your organization’s APIs? (single choice)



Lack of visibility	42%
Bots or scrapers	8%
Commercially driven hackers/ cybercriminals	31%
Misuse or abuse cases	15%
Unsophisticated hacking or mischief	4%



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

INNOVATION

16 Industry Experts Share Tips For Creating A Security-First Tech Company

Expert Panel® Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

15am EDT

When Security Meets Development: The DevSecOps Conundrum

The DevSecOps journey is well worth undertaking because it
development, and ensure quality products.

Home » Security Boulevard (Original) » The Benefits of Shift Left Security

The Benefits of Shift Left Security

by Lucjan Zaborowski on March 25, 2022

The challenges with Shift-Left

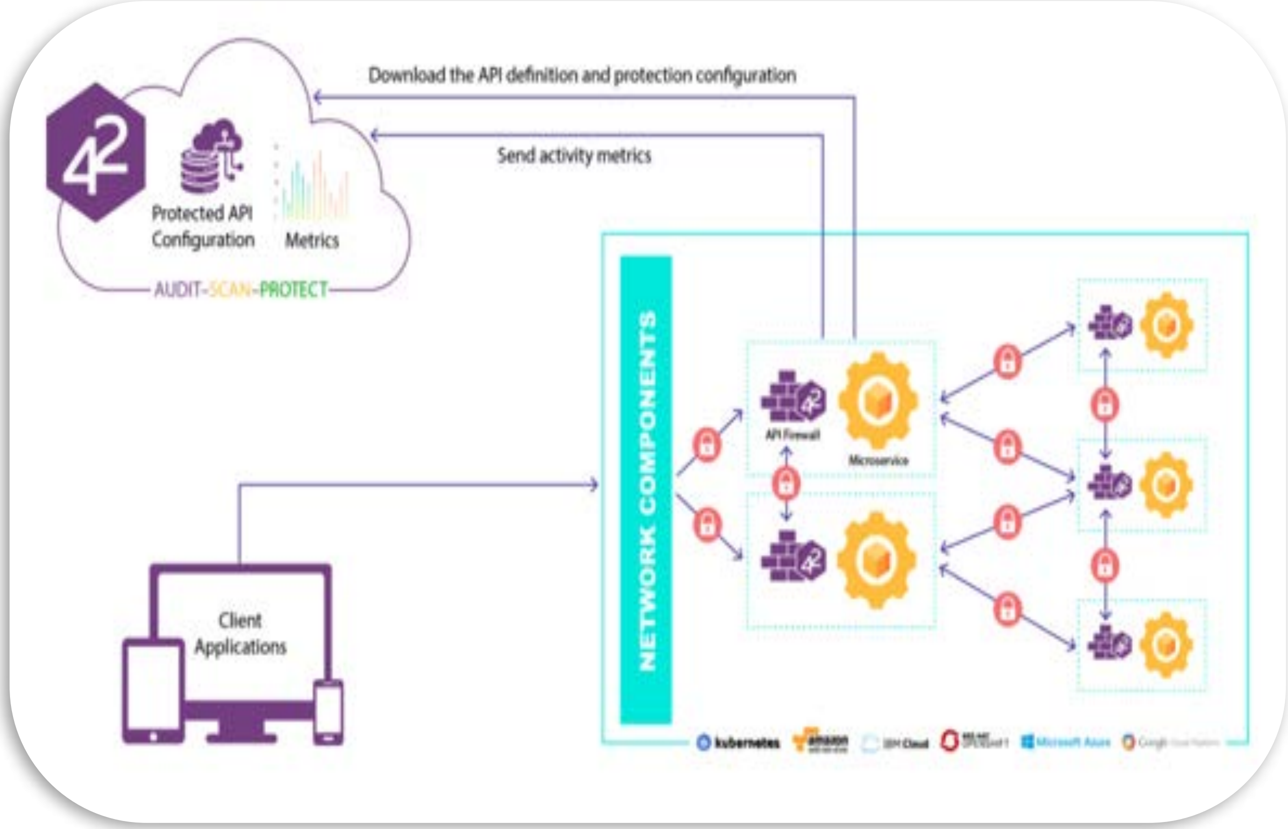
- Lack of established **DevOps process**
- **Legacy systems**
- **Shadow IT, “Frankenstein” APIs**
- **3rd party or partner APIs**
- **“Code-first” development** (lack of OAS definitions)

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

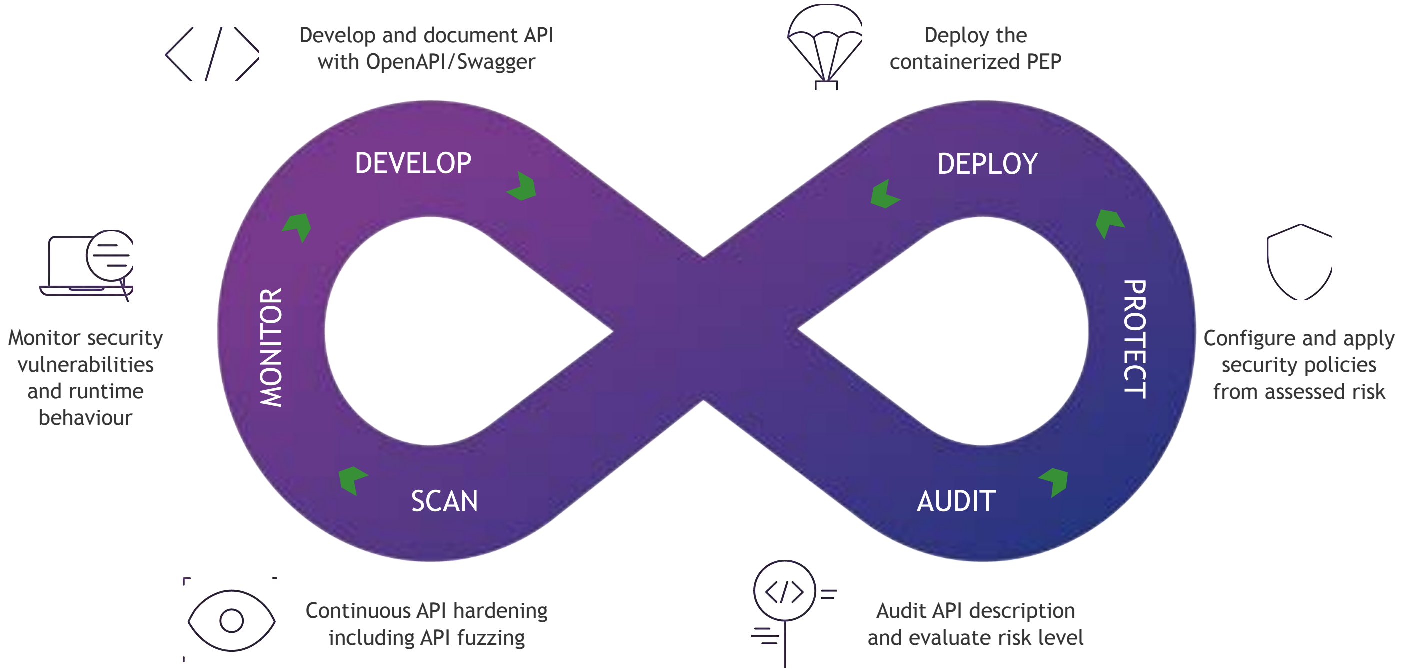
AUTOMATE & SCALE API SECURITY TO PROTECT YOUR APIs

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.*


Develop and document API with OpenAPI/Swagger
Deploy the containerized PEP
DEVELOP
DEPLOY
Monitor security vulnerabilities and runtime behaviour
MONITOR
PROTECT
Configure and apply security policies from assessed risk
SCAN
AUDIT
Continuous API hardening including API fuzzing
Audit API description and evaluate risk level

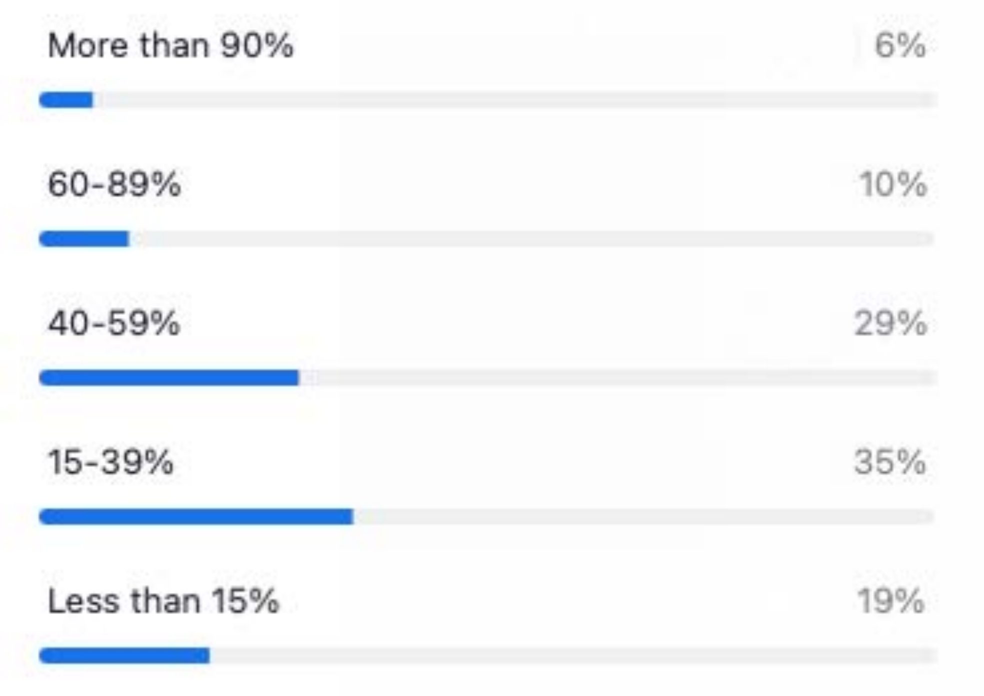
Question Two:

How many of your APIs are built ‘design-first’ i.e. via an OAS definition?

1. Nearly all of them (More than 90%)
2. Most of them (60 to 89%)
3. About half of them (40 to 59%)
4. A few of them (15 to 39%)
5. Hardly any of them (Less than 15%)

Question Two:

How many of your APIs are built 'design-first' i.e. via an OAS definition?



More than 90%	6%
60-89%	10%
40-59%	29%
15-39%	35%
Less than 15%	19%

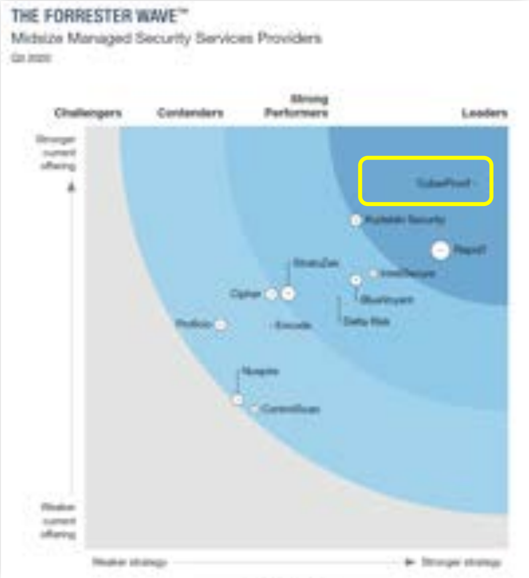
CyberProof

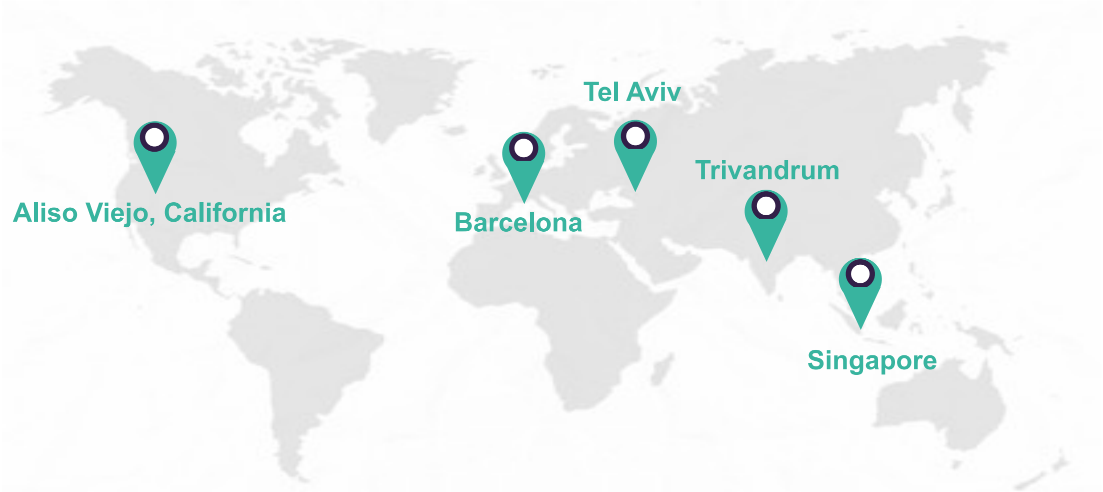
Cyberproof overview

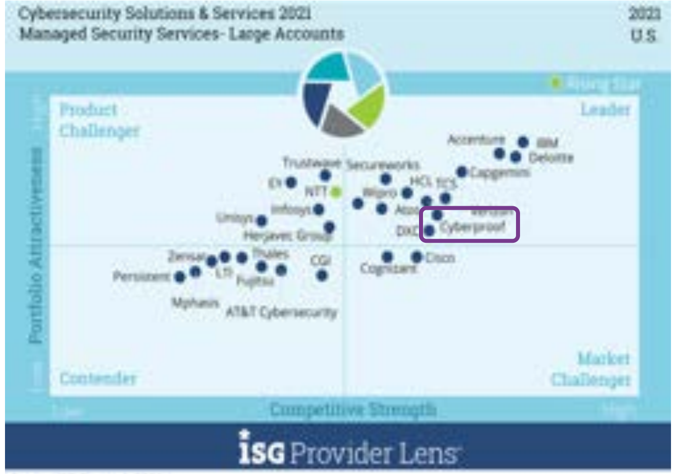
Saggie Haim

Cyberproof is a trailblazer in threat detection and response services

- **600 + Employees** Globally are ready to scale
- **Named a Leader** by Forrester in both 2018 and 2020 Midsize Managed Security Services Market
- **Named a Leader in NA in 2021 Rising Star in France by ISG** in Managed Security Services Market
- **Former 8200 Unit of Israeli Defense Forces (IDF) and Counter-Espionage** threat intelligence, threat hunting and forensics investigations operate in Tel Aviv SOC
- Tier 1&2 operate from **CREST & ISO27001 Certified SOCs** in Trivandrum (India), Barcelona, and Singapore. Ready to open SOC in rural US location.

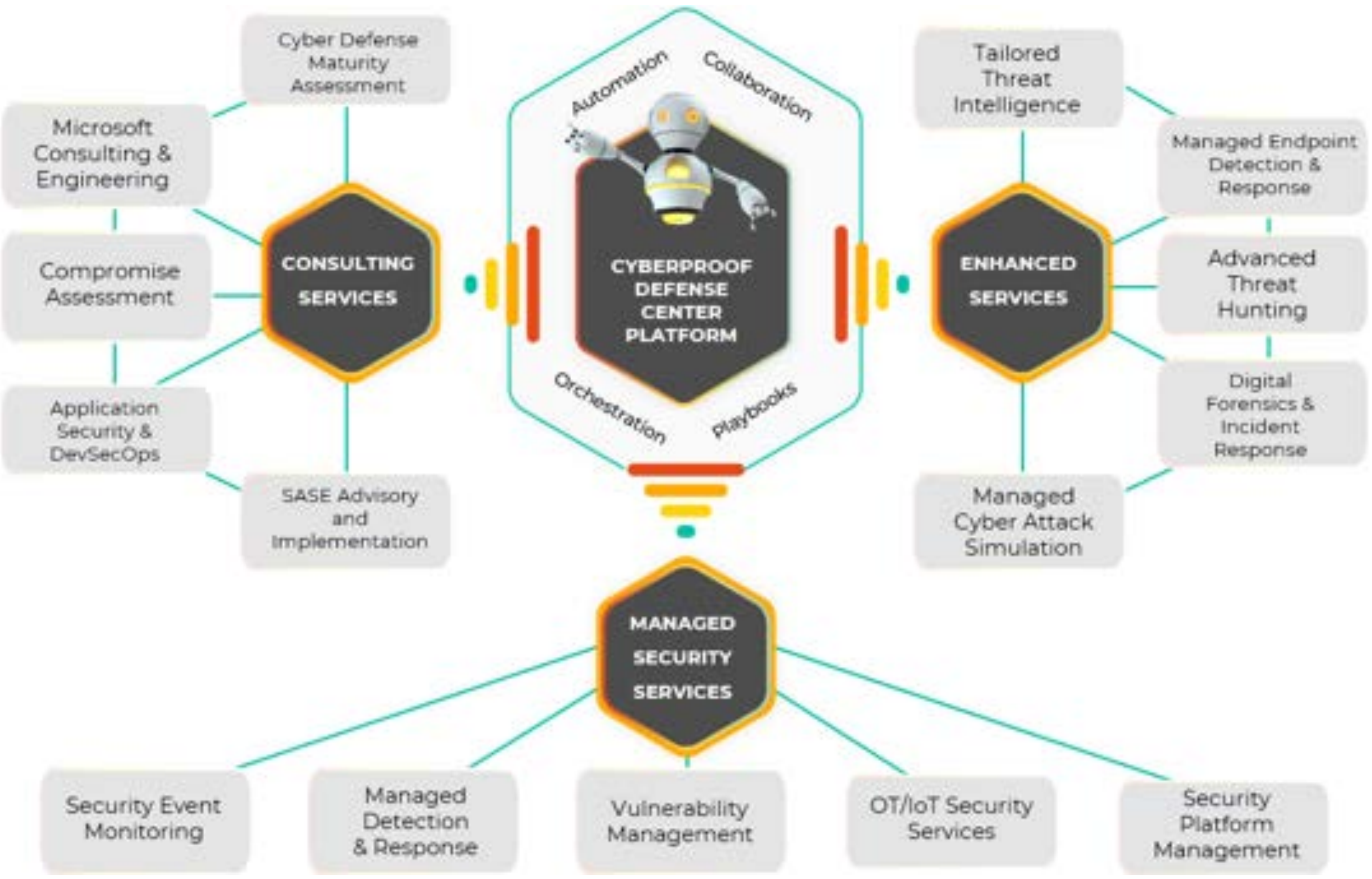






Source: ISG Research 2021

Our Portfolio


Cyber Defense Maturity Assessment
Microsoft Consulting & Engineering
Compromise Assessment
Application Security & DevSecOps
SASE Advisory and Implementation
CONSULTING SERVICES
Automation
Collaboration
CYBERPROOF DEFENSE CENTER PLATFORM
Orchestration
playbooks
Tailored Threat Intelligence
Managed Endpoint Detection & Response
Advanced Threat Hunting
Digital Forensics & Incident Response
Managed Cyber Attack Simulation
ENHANCED SERVICES
MANAGED SECURITY SERVICES
Security Event Monitoring
Managed Detection & Response
Vulnerability Management
OT/IoT Security Services
Security Platform Management

CDC Platform: Cloud-native orchestration, collaboration and automation platform which enables the delivery of our services

Managed Services: Foundational services to provide 24x7 security monitoring, detection and response

Enhanced services: Proactive, specialized services to reduce your attack exposure

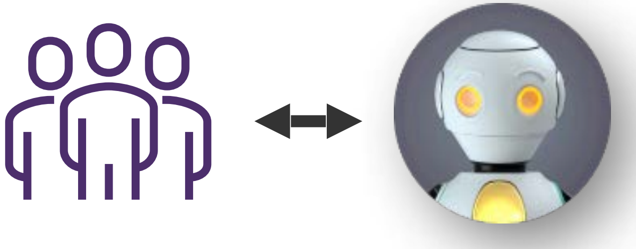
Consulting services: Strategic and technical guidance provided by experienced consultants and architects to help you measurably reduce risk

How We've Innovated To Solve Customer Challenges

"Help shift my own staff onto higher impact activities"

Where Bot Meets Human

Our virtual analyst, SeeMo, acts as an extension of your team – automating alert triage and enrichment and responding to analyst requests



"Need transparency into daily SOC activities with clear KPIs"

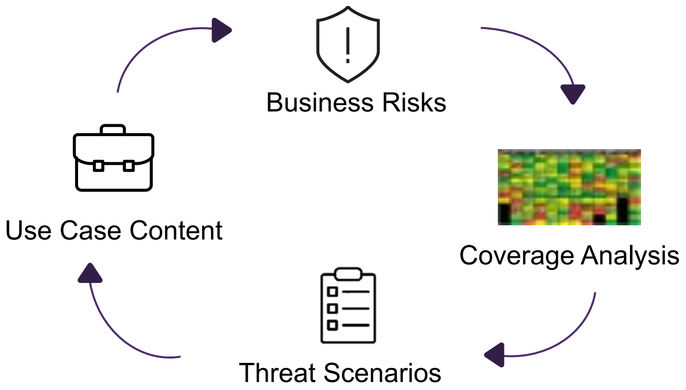
The CDC: One Platform for Collaborative Security Operations

Integration and orchestration of your security technologies and transparency of who is doing what for you

"Need to fill detection gaps & focus on the right threats"

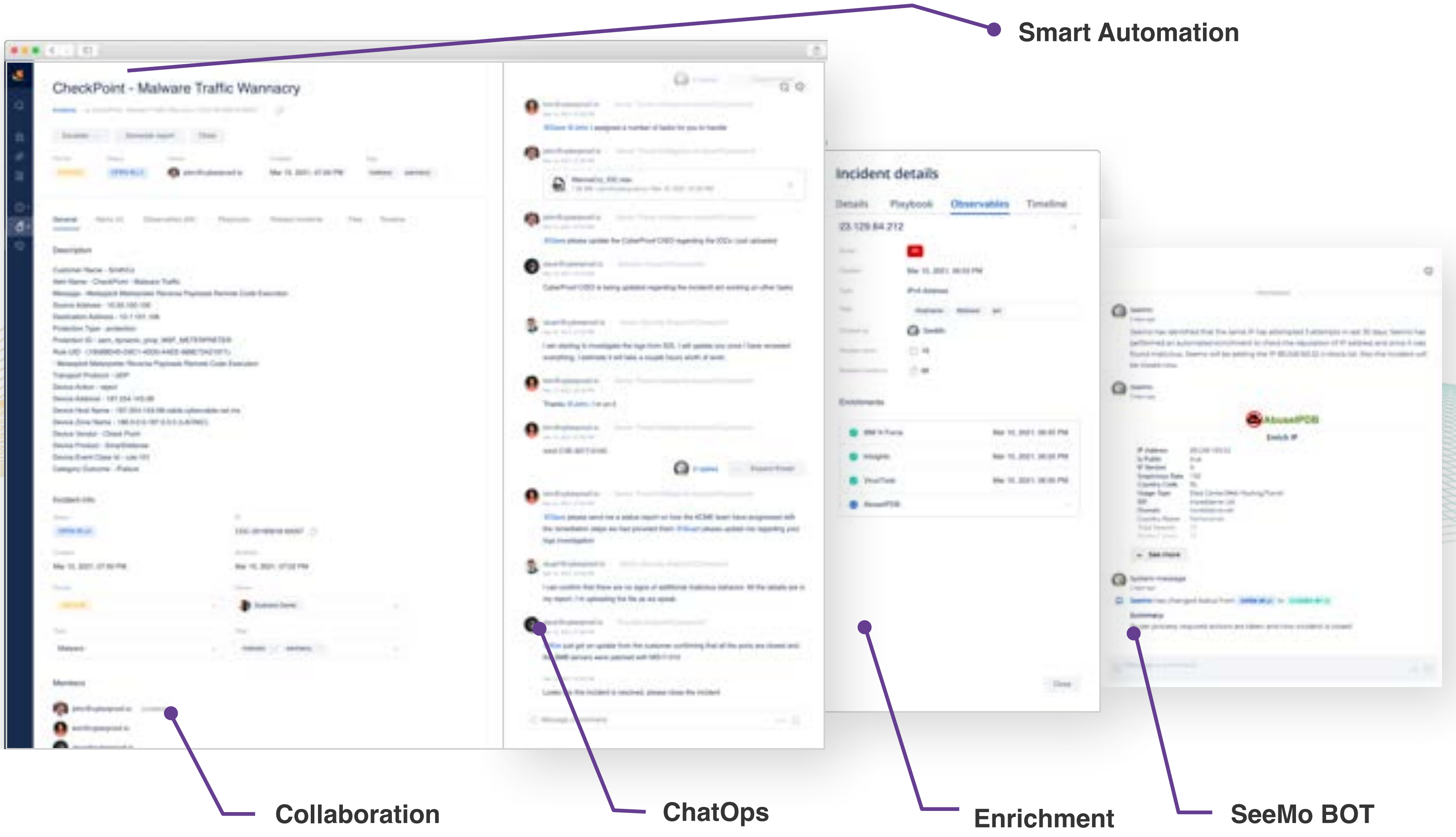
Use Case Factory: Continuously Optimizing Use Cases aligned to Risk

Continuous definition, delivery and optimization of use case content aligned to your business risks and threat profile



Cyberproof DefenSe Center (CDC) Platform

is one environment for COLLABORATIVE security operations



CheckPoint - Malware Traffic Wannacry

Incident details

23.129.84.212

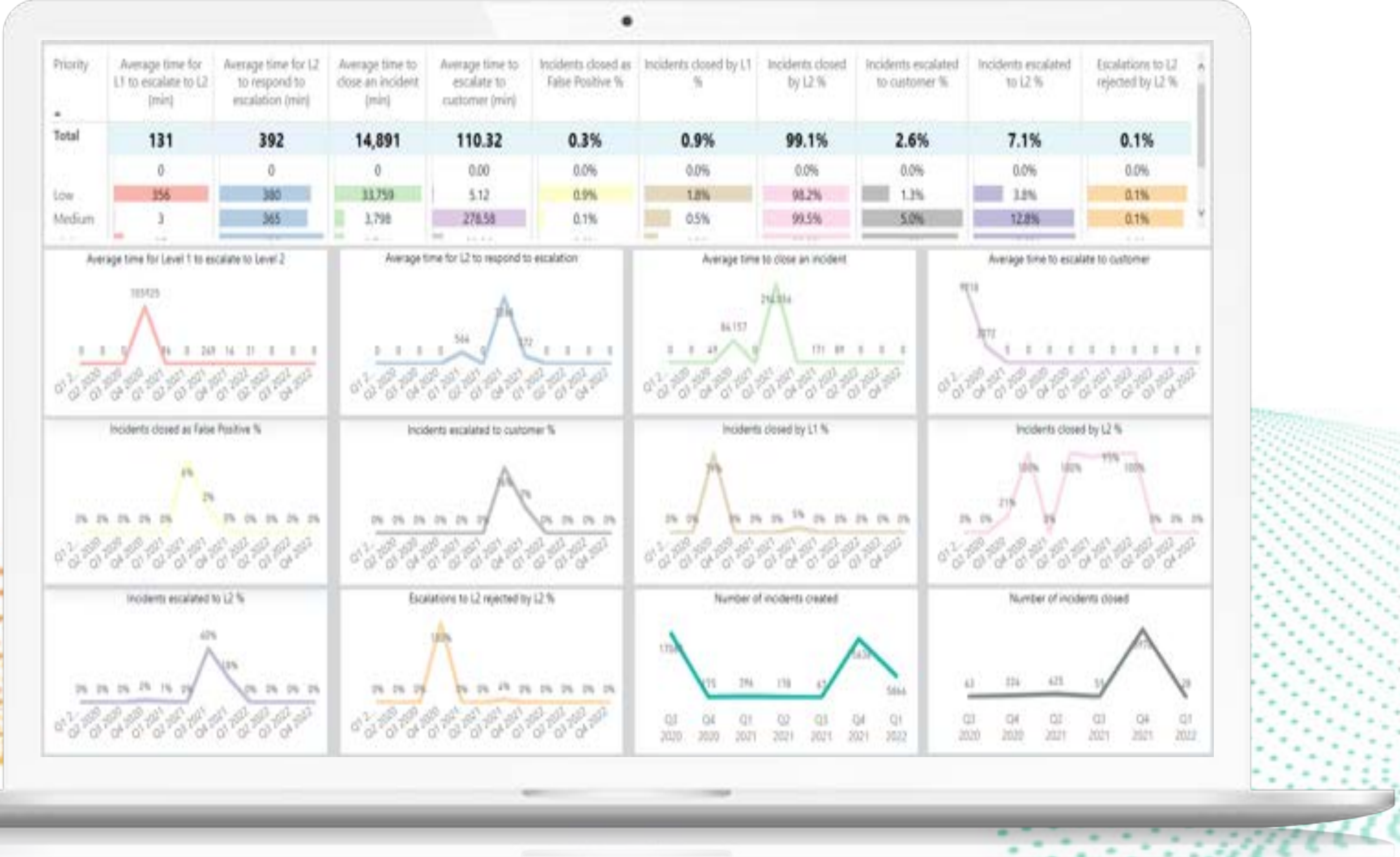
Digital Playbooks

Incident prioritization

KPI-Based Reporting

Incidents Performance KPIs

Effectiveness and Accuracy	Time and Efficiency	Continuous Improvement	Risk Measurement
▪ No. of alerts & incidents ▪ Percentage of incidents ▪ Percentage of false positives	▪ Time to acknowledge alert ▪ Time to triage incident ▪ Mean time to respond	▪ Reduce false positive ▪ Automation percentage ▪ Avg. time to close incident	▪ Coverage gap analysis ▪ Use Case roadmap ▪ Estimated risk exposure



Priority	Average time for L1 to escalate to L2 (min)	Average time for L2 to respond to escalation (min)	Average time to close an incident (min)	Average time to escalate to customer (min)	Incidents closed as False Positive %	Incidents closed by L1 %	Incidents closed by L2 %	Incidents escalated to customer %	Incidents escalated to L2 %	Escalations to L2 rejected by L2 %
Total	131	392	14,891	110.32	0.3%	0.9%	99.1%	2.6%	7.1%	0.1%
	0	0	0	0.00	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Low	356	380	33,759	5.12	0.9%	1.8%	98.2%	1.3%	3.8%	0.1%
Medium	3	365	3,798	278.58	0.1%	0.5%	99.5%	5.0%	12.8%	0.1%

Average time for Level 1 to escalate to Level 2
Average time for L2 to respond to escalation
Average time to close an incident
Average time to escalate to customer
Incidents closed as False Positive %
Incidents escalated to customer %
Incidents closed by L1 %
Incidents closed by L2 %
Incidents escalated to L2 %
Escalations to L2 rejected by L2 %
Number of incidents created
Number of incidents closed

Seemo, our virtual analyst, is the future

SeeMo works with human analysts as part of the SOC team to see things humans cannot see, do useful tasks to reduce workload and the time required to respond to an incident and minimize the damage from attack

Smart Enrichment

Enriching events and alerts by proactively fetching information from external threat intelligence and vulnerability data sources

Extracts observables

Automates non-intrusive steps in digitized playbooks

Anticipates Attacks

Looks for patterns in event and alert data to identify patterns and inform analysts (2022)

Accelerates response

Automates non-intrusive steps in digitized playbooks

Creates and prioritizes incidents

Automatically creating incidents based on alerts and their contexts, as well as insights

Responds to analyst requests

Can be asked to verify alerts, collect more information or fetch specific information from integrated sources

CyberProof Use Case Factory Capabilities

CyberProof has a dedicated team for Use Case production, that maps different scenarios & create/update Use Cases on ongoing basis.

DEDICATED TEAM

Includes detection rule development, advanced analytics, custom playbook, integrations, testers etc.

500+ CUSTOM USE CASES

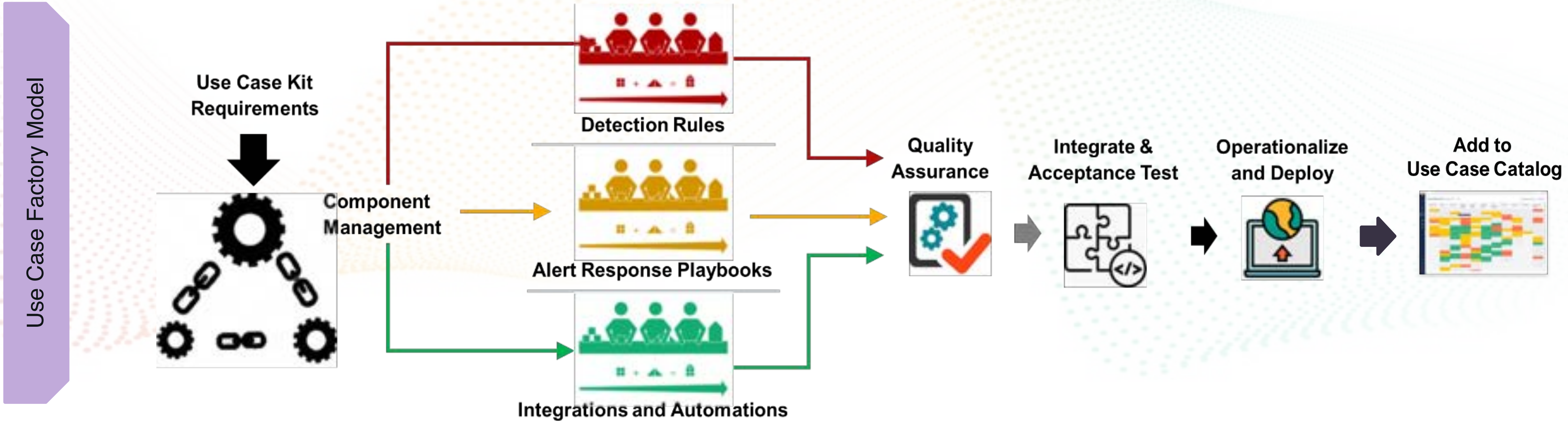
Designed, built, tested and operationalized custom use cases for number of enterprise clients

FORRESTER LEADER

Emerging Next Gen Service Provider, ranked highest on R&D, innovation & threat detection & response abilities

DEDICATED UCF SERVICE

We offer Use Case Factory as part of our service, with measurable service improvement indicators



Use Case Factory Model

Use Case Kit Requirements

Component Management

Detection Rules

Alert Response Playbooks

Integrations and Automations

Quality Assurance

Integrate & Acceptance Test

Operationalize and Deploy

Add to Use Case Catalog

CyberProof use case catalog

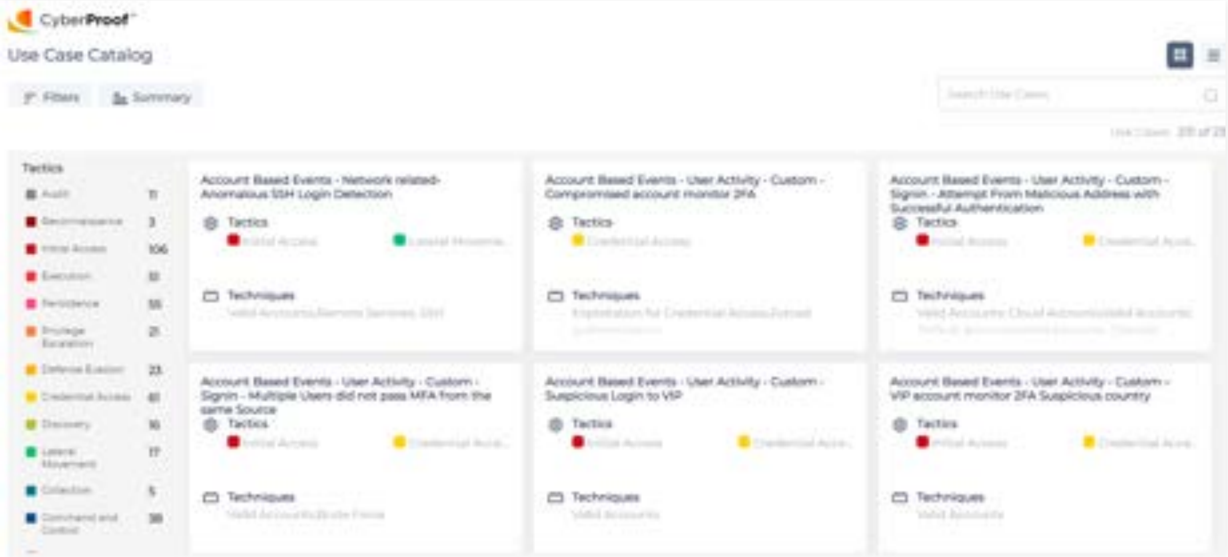
A central repository where use cases are grouped under MITRE tactics and techniques

New use cases are continuously added to the catalogue based on cyber threat trends

Customers can easily select use cases based on their MITRE capability gaps

A use case kit contains a detection rule and corresponding incident response playbook.

Customers can also request for Custom Use Cases to be built, per their technology ecosystem & Risk profile



Account Based Events - Network related- Anomalous SSH Login Detection

Tactics: Initial Access, Lateral Moveme...

Techniques: Valid Accounts,Remote Services: SSH

Account Based Events - User Activity - Custom - Compromised account monitor 2FA

Tactics: Credential Access

Techniques: Exploitation for Credential Access,Forced [illegible]

Account Based Events - User Activity - Custom - Signin - Attempt From Malicious Address with Successful Authentication

Tactics: Initial Access, Credential Acce...

Techniques: Valid Accounts: Cloud Accounts,Valid Accounts: [illegible]

Account Based Events - User Activity - Custom - Signin - Multiple Users did not pass MFA from the same Source

Tactics: Initial Access, Credential Acce...

Techniques: Valid Accounts,Brute Force

Account Based Events - User Activity - Custom - Suspicious Login to VIP

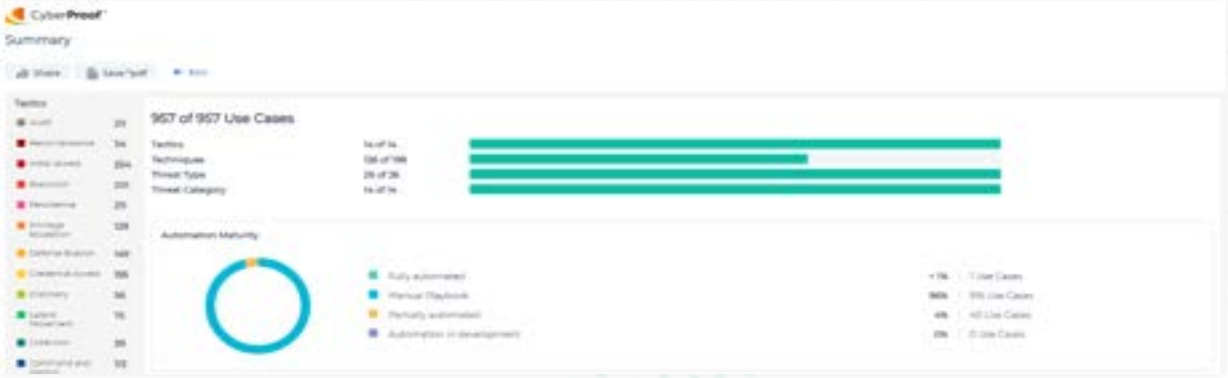
Tactics: Initial Access, Credential Acce...

Techniques: Valid Accounts

Account Based Events - User Activity - Custom - VIP account monitor 2FA Suspicious country

Tactics: Initial Access, Credential Acce...

Techniques: Valid Accounts

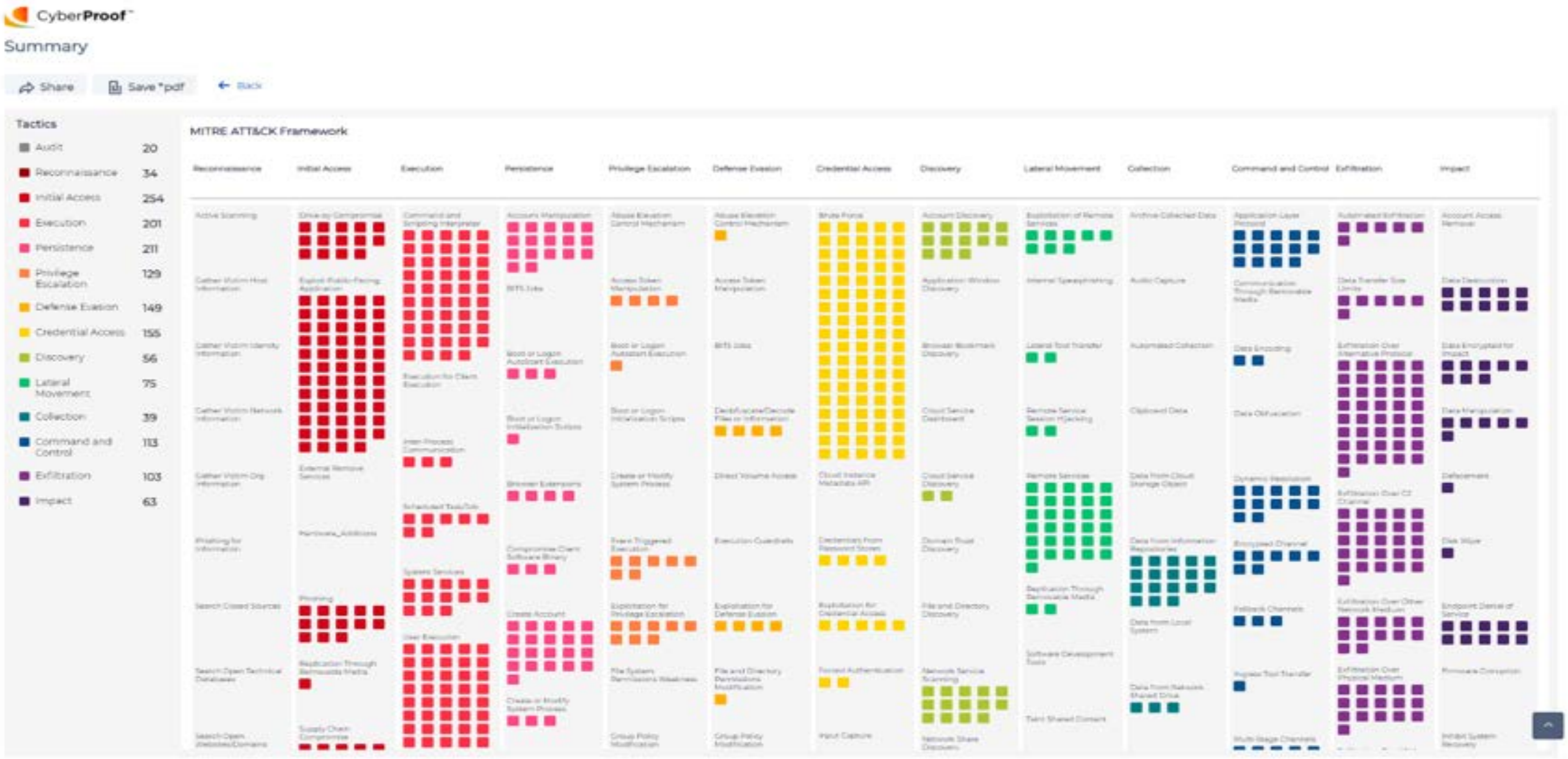


957 of 957 Use Cases

Tactics	14 of 14	
Techniques	[illegible]	
Threat Type	[illegible]	
Threat Category	14 of 14	

Fully automated	<1%	7 Use Cases
Manual Playbook	96%	[illegible] Use Cases
Partially automated	4%	40 Use Cases
Automation in development	0%	0 Use Cases

CyberProof UC catalog – MITRE ATT&CK mapping snapshot



Summary

Tactics

■	Audit	20
■	Reconnaissance	34
■	Initial Access	254
■	Execution	201
■	Persistence	211
■	Privilege Escalation	129
■	Defense Evasion	149
■	Credential Access	155
■	Discovery	56
■	Lateral Movement	75
■	Collection	39
■	Command and Control	113
■	Exfiltration	103
■	Impact	63

MITRE ATT&CK Framework

Reconnaissance: Active Scanning; Gather Victim Host Information; Gather Victim Identity Information; Gather Victim Network Information; Gather Victim Org Information; Phishing for Information; Search Closed Sources; Search Open Technical Databases; Search Open Websites/Domains

Initial Access: Drive-by Compromise; Exploit Public-Facing Application; External Remote Services; Hardware_Additions; Phishing; Replication Through Removable Media; Supply Chain Compromise

Execution: Command and Scripting Interpreter; Exploitation for Client Execution; Inter-Process Communication; Scheduled Task/Job; System Services; User Execution

Persistence: Account Manipulation; BITS Jobs; Boot or Logon Autostart Execution; Boot or Logon Initialization Scripts; Browser Extensions; Compromise Client Software Binary; Create Account; Create or Modify System Process

Privilege Escalation: Abuse Elevation Control Mechanism; Access Token Manipulation; Boot or Logon Autostart Execution; Boot or Logon Initialization Scripts; Create or Modify System Process; Event Triggered Execution; Exploitation for Privilege Escalation; File System Permissions Weakness; Group Policy Modification

Defense Evasion: Abuse Elevation Control Mechanism; Access Token Manipulation; BITS Jobs; Deobfuscate/Decode Files or Information; Direct Volume Access; Execution Guardrails; Exploitation for Defense Evasion; File and Directory Permissions Modification; Group Policy Modification

Credential Access: Brute Force; Cloud Instance Metadata API; Credentials from Password Stores; Exploitation for Credential Access; Forced Authentication; Input Capture

Discovery: Account Discovery; Application Window Discovery; Browser Bookmark Discovery; Cloud Service Dashboard; Cloud Service Discovery; Domain Trust Discovery; File and Directory Discovery; Network Service Scanning; Network Share Discovery

Lateral Movement: Exploitation of Remote Services; Internal Spearphishing; Lateral Tool Transfer; Remote Service Session Hijacking; Remote Services; Replication Through Removable Media; Software Deployment Tools; Taint Shared Content

Collection: Archive Collected Data; Audio Capture; Automated Collection; Clipboard Data; Data from Cloud Storage Object; Data from Information Repositories; Data from Local System; Data from Network Shared Drive

Command and Control: Application Layer Protocol; Communication Through Removable Media; Data Encoding; Data Obfuscation; Dynamic Resolution; Encrypted Channel; Fallback Channels; Ingress Tool Transfer; Multi-Stage Channels

Exfiltration: Automated Exfiltration; Data Transfer Size Limits; Exfiltration Over Alternative Protocol; Exfiltration Over C2 Channel; Exfiltration Over Other Network Medium; Exfiltration Over Physical Medium

Impact: Account Access Removal; Data Destruction; Data Encrypted for Impact; Data Manipulation; Defacement; Disk Wipe; Endpoint Denial of Service; Firmware Corruption; Inhibit System Recovery

The rise of Security analytics platforms

"...cloud-delivered **security analytics platforms** that provide **custom detections** will dictate which providers will **lead the pack**. Vendors that can provide customization, **MITRE ATT&CK mapping**, and SaaS delivery position themselves to successfully deliver **improved detection, faster investigations**, and flexibility to their customers."

Based on Forrester report

Azure Sentinel – A cloud-native security analytics platform

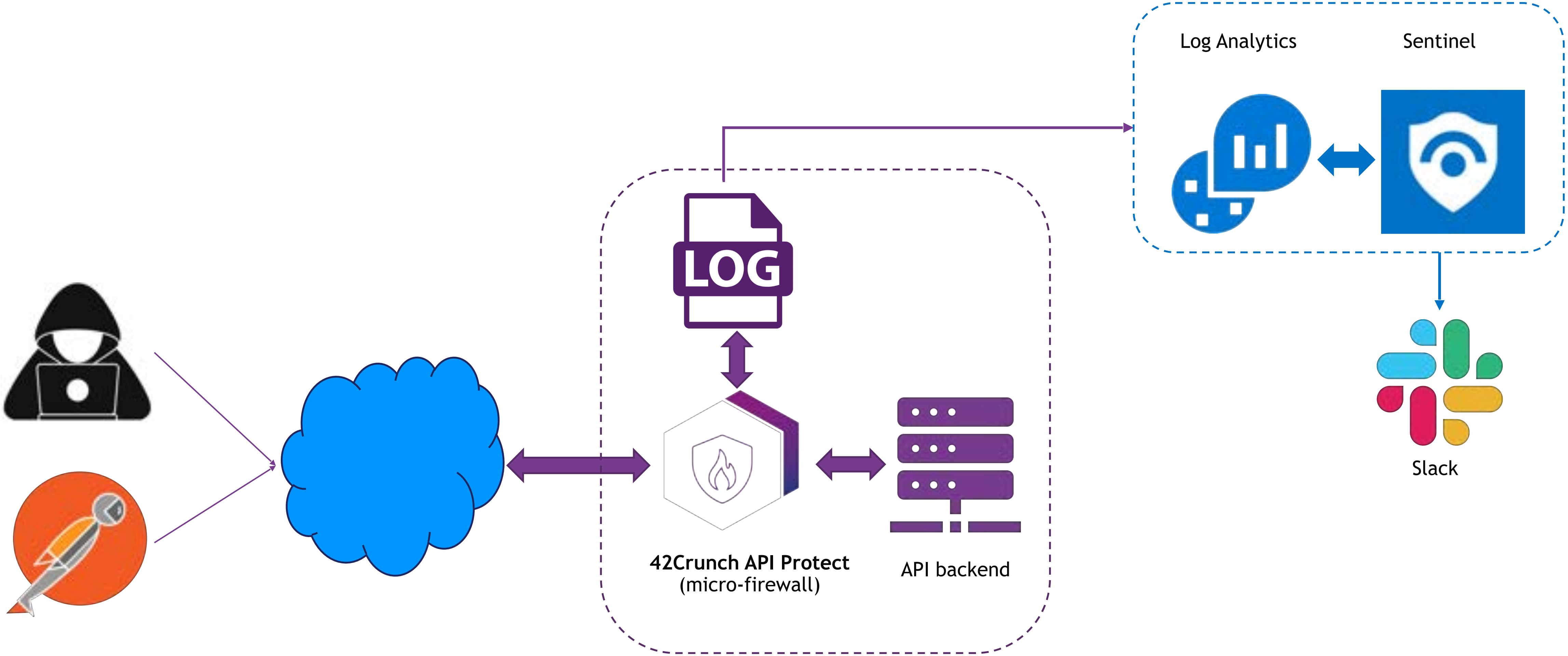
Microsoft is shifting Azure Sentinel from being a traditional SIEM, to a **Security Analytics Platform** in the **Microsoft XDR** stack.

Azure Sentinel offers:

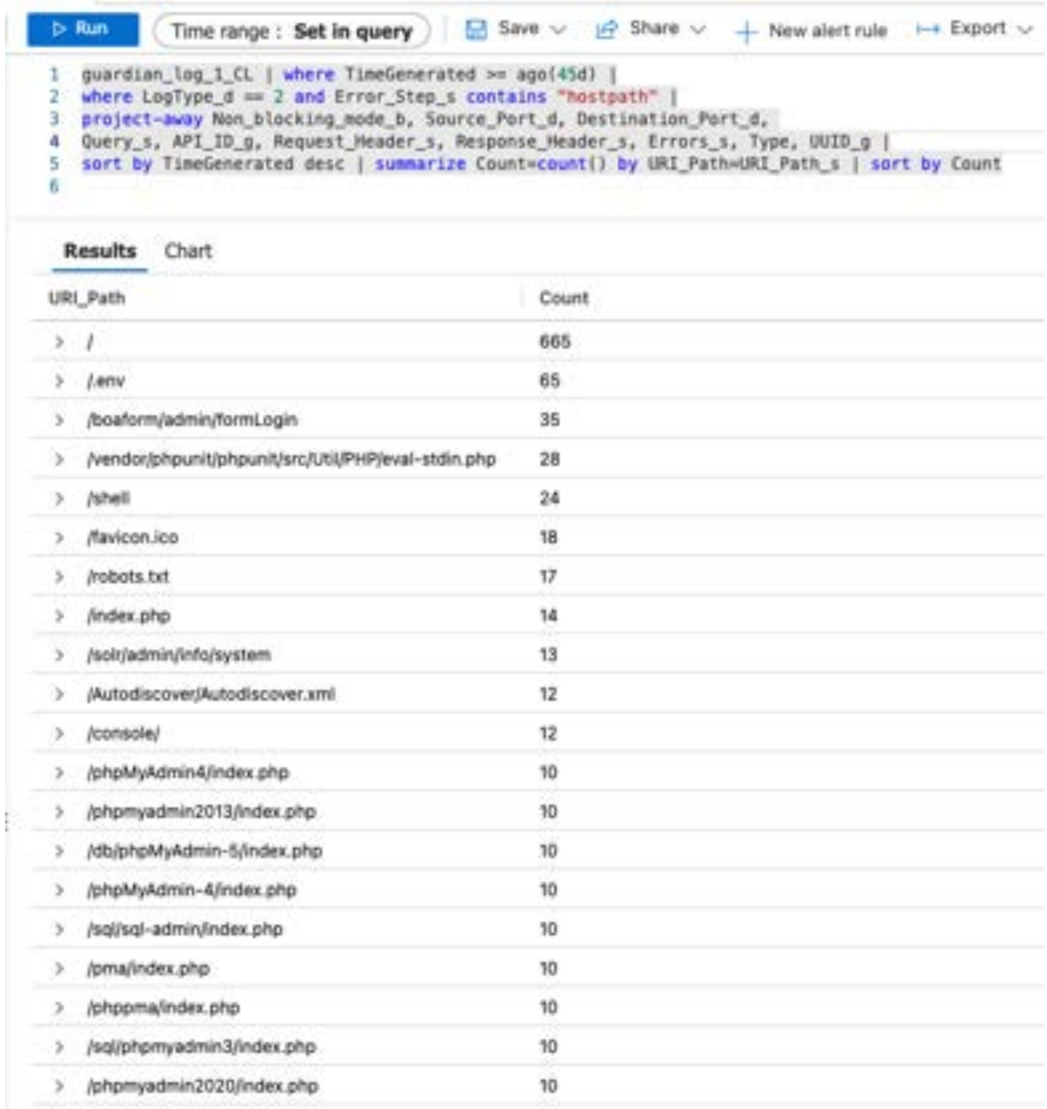
- SIEM
- SOAR
- Threat Intelligence
- Threat Hunting solutions
- UEBA
- Azure Arc integration

Live demo

Demo environment architecture



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

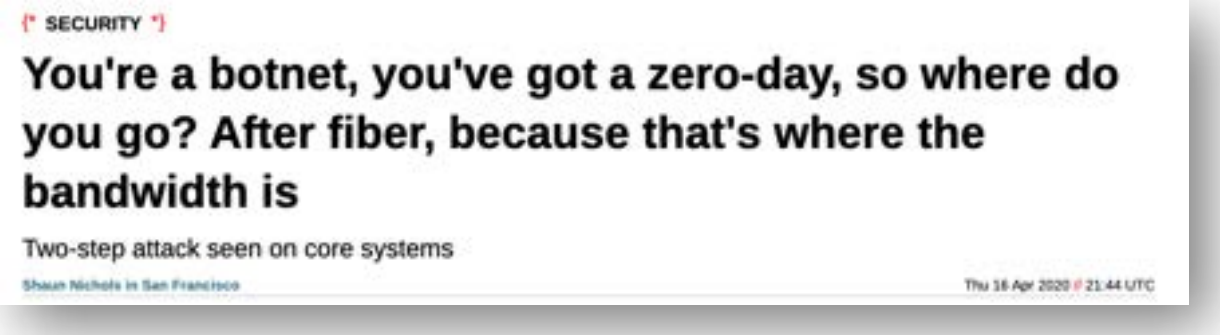


```
guardian_log_1_CL | where TimeGenerated >= ago(45d) |
where LogType_d == 2 and Error_Step_s contains "hostpath" |
project-away Non_blocking_mode_b, Source_Port_d, Destination_Port_d,
Query_s, API_ID_g, Request_Header_s, Response_Header_s, Errors_s, Type, UUID_g |
sort by TimeGenerated desc | summarize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

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



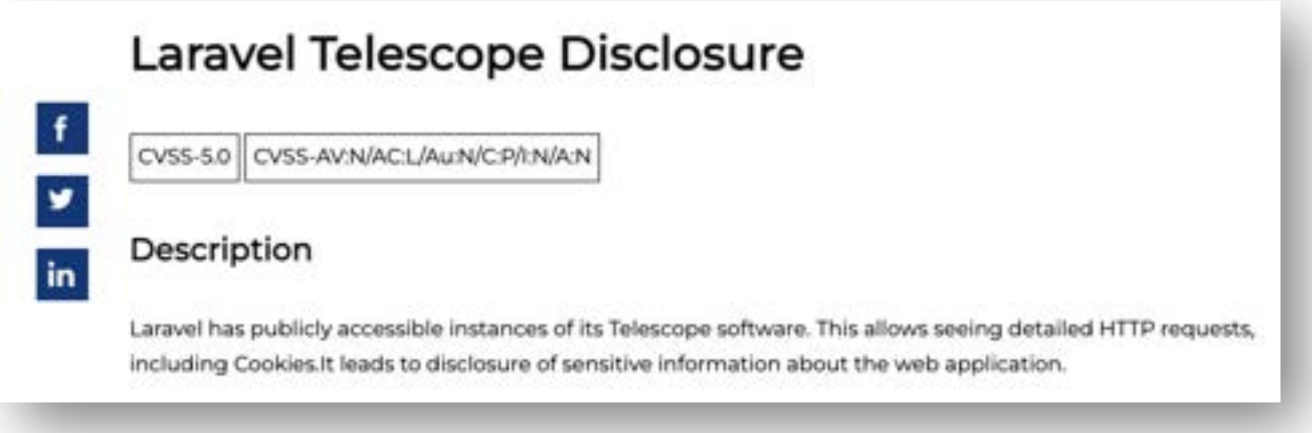
{* SECURITY *}

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/



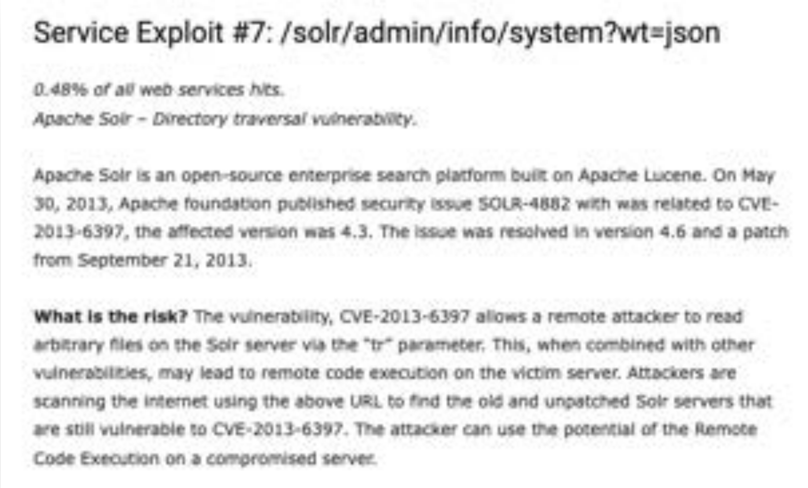
Laravel Telescope Disclosure

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



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/

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 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.

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”

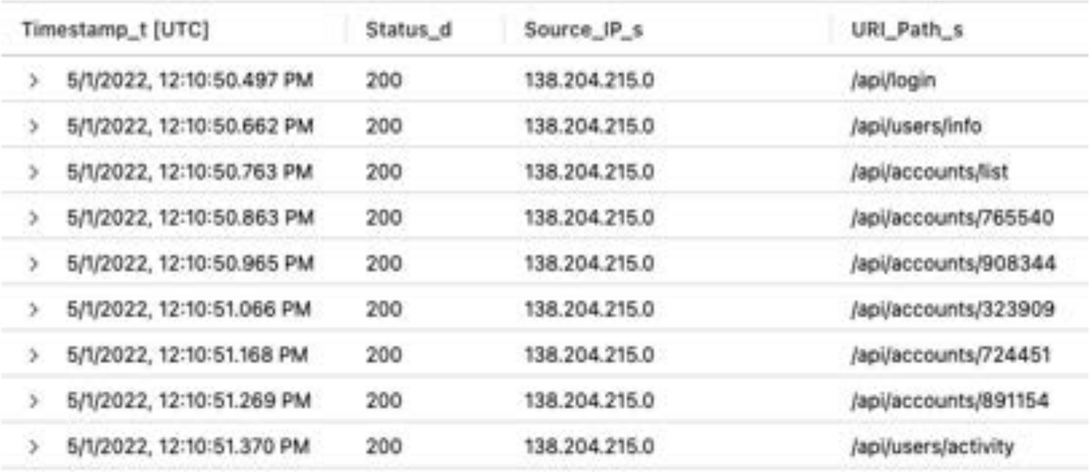
Attack Technique

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 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

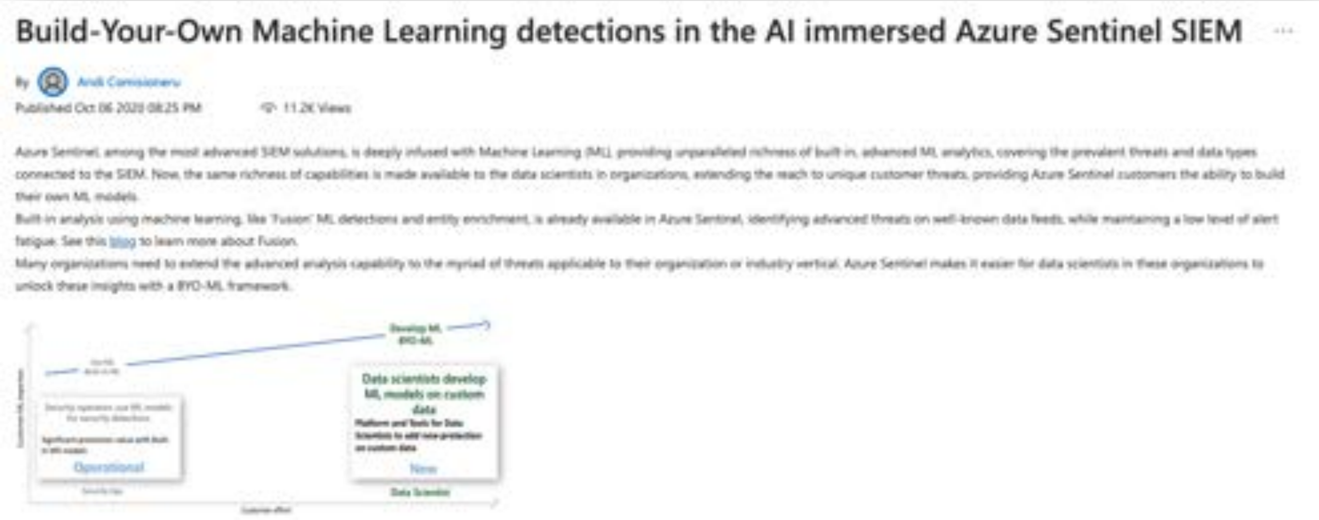
API developers should use well-proven JWT client libraries to fully validate JWTs.

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.

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.

Develop ML
BYO-ML
Data scientists develop ML models on custom data
Platform and Tools for Data Scientists to add new protection on custom data
New
Data Scientist
Operational
Customer effort

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.

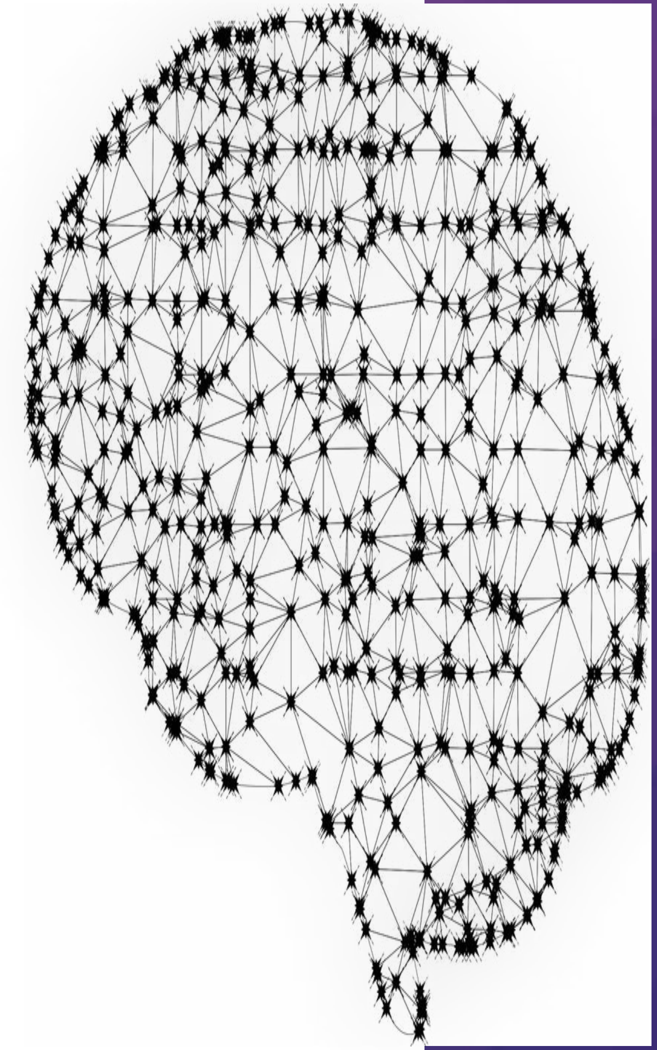
Hot fixes

If emerging threats are detected in real-time a protection can be ‘patched’ into the OAS definition and immediately redeployed – almost instant hot fixes !

Question Three:

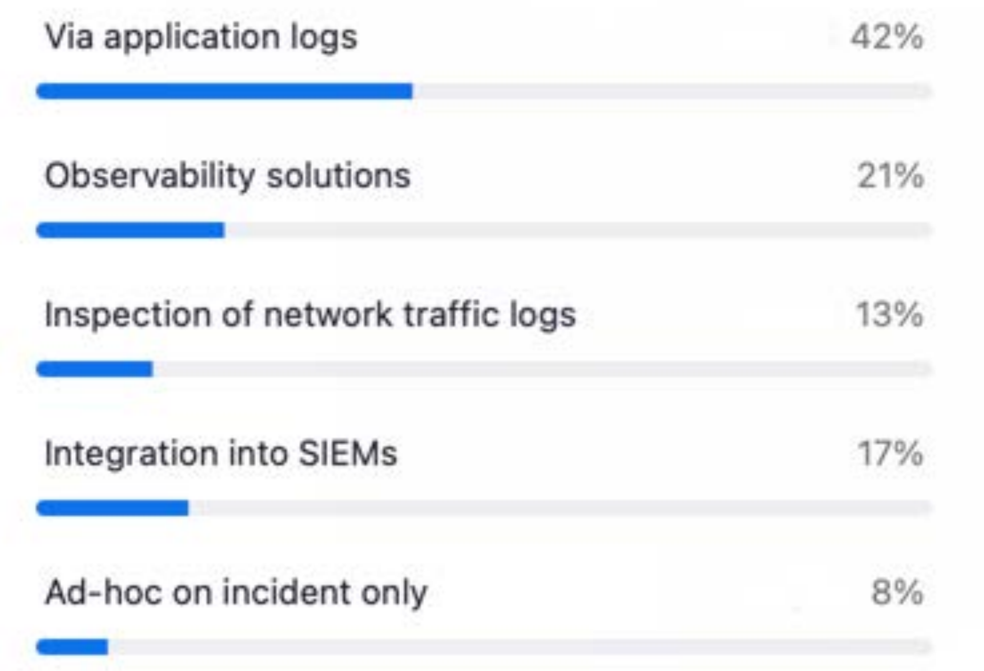
How is your organization currently monitoring your APIs for threats?

1. Via application logs
2. Observability solutions
3. Inspection of network traffic logs
4. Integration into SIEMs
5. Ad-hoc on incident only

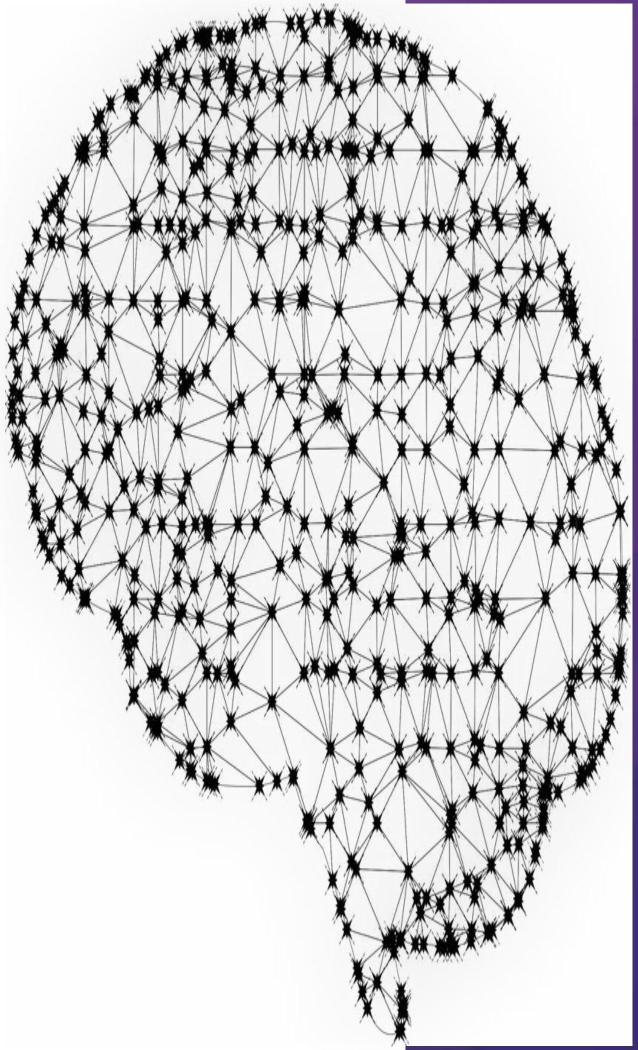


Question Three:

How is your organization currently monitoring your APIs for threats?



Via application logs	42%
Observability solutions	21%
Inspection of network traffic logs	13%
Integration into SIEMs	17%
Ad-hoc on incident only	8%



Learning more

APISecurity.io

https://apisecurity.io/

42Crunch GitHub

https://github.com/42Crunch/azure-sentinel-integration

Upcoming News

Further Activities

Gluecon: Colorado May 18-19

“Automating API Security with Security as Code”

glue 2022 conference

Gartner Security & Risk Management: Maryland June 7 -10

API Security Showcase: William Dupre, Dionisio Zumerle

Gartner Security & Risk Management Summit

June 7 - 10, 2022 | National Harbor, MD

APIsecurity.io Weekly Newsletter

https://apisecurity.io/

OpenAPI Editor - Free Download

https://42crunch.com/resources-free-tools/

42crunch

CyberProof
A UST Global Company

4 May 2022

Actively Monitor and Defend Your APIs with 42Crunch and the Azure Sentinel Platform

Colin Domoney

API Security Research Specialist & Developer Advocate

Saggie Haim

Cloud Security Solutions Architect Team Leader