DETECTION AS CODE INNOVATION REPORT 2021

THE POWER OF COLLABORATIVE CYBER DEFENSE

Edition #2

www.socprime.com

THE POWER OF COLLABORATIVE CYBER DEFENSE

ANDRII BEZVERKHYI
Founder and CEO at SOC Prime

At SOC Prime, we are committed to our vision of transforming threat detection. Today we deliver Detection as Code operations enriched with CTI and the latest threat context based on MITRE ATT&CK® to 7,000 organizations from over 155 countries. Harnessing the power of collaborative cybersecurity expertise, we provide Threat Hunting, Detection Engineering, and Incident Detection enriching SOC operations with accelerated capability, improving efficiency, and supercharging SIEM, EDR, and XDR solutions with Sigma-enabled content.

We believe in a future where the capabilities of cyber defense teams match those of would-be attackers. Progressive organizations come to realize that keeping pace with threat actors is only possible with the power of collaborative cyber defense rather than individual teams' efforts. This Detection as Code report illustrates how collaboration between the SOC Prime Team, our Threat Bounty Program members, and the worldwide cybersecurity community can produce a monolithic base of knowledge and a driving force capable of combating attacks of any scale and sophistication. Together, we shape the future of cyber defense, where automated threat detection capabilities enable ultra-responsiveness to emerging threats at costs far less than the costs of attacks.

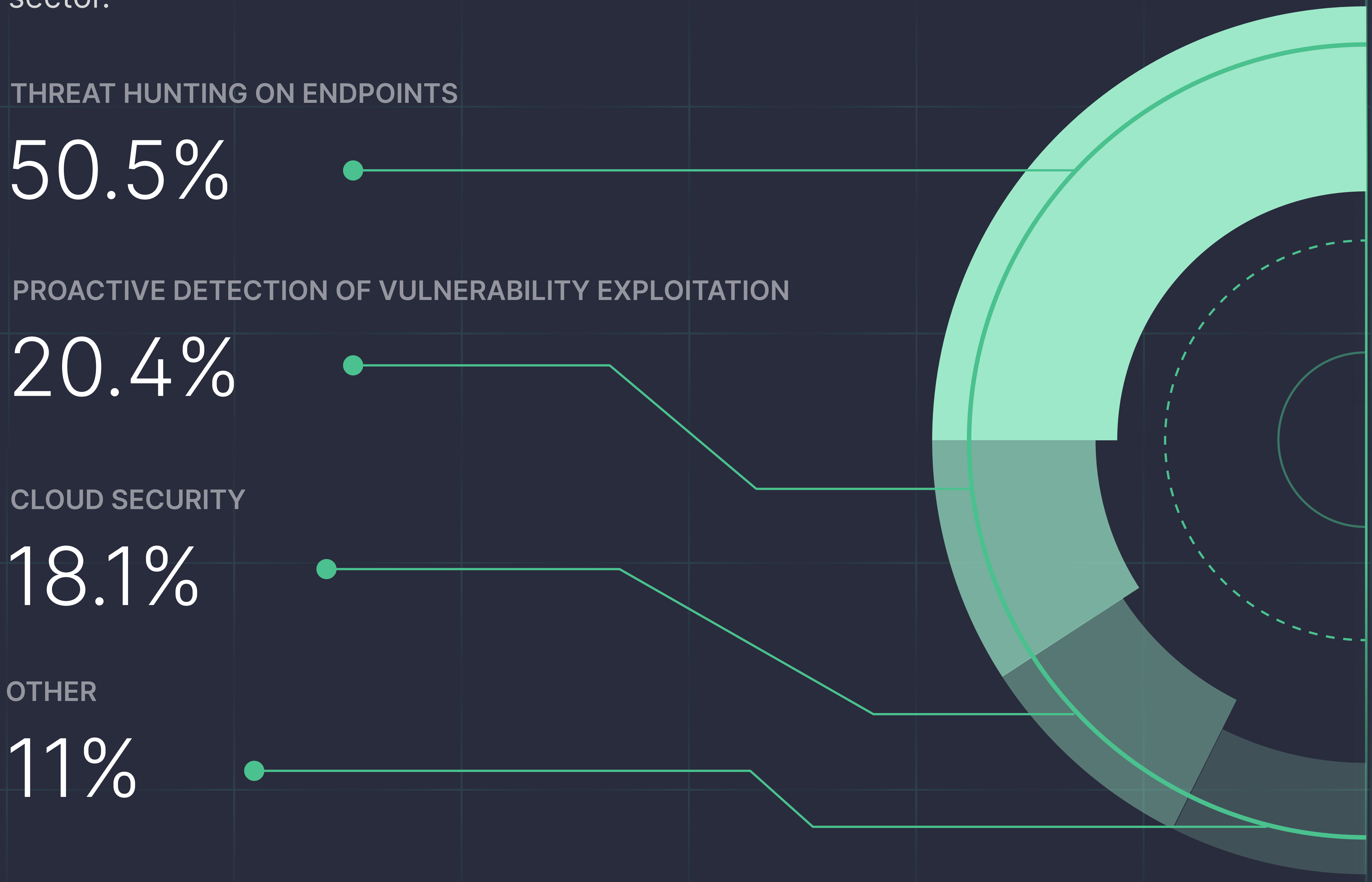
THREAT LANDSCAPE OF 2021: TRENDS, USE CASES, AND INSIGHTS

Cyber-attacks have been continuously on the rise accelerating not only in terms of vectors and volumes but also in terms of their impact and speed. Driven by the COVID-19 shift to online and cloud-based environments, the cyber threat landscape of 2020-2021 has adapted to the new reality growing in sophistication and scale and producing more advanced threats.

In view of growing cyber risks, the global cybersecurity community has come to realize the importance of collaborative efforts in analyzing and tracking adversary activities and confronting threats of such scale and complexity. On the following pages you can find the main trends in security use cases, an overview of top adversary tactics and techniques as per MITRE ATT&CK®, and insights into detection content consumption by industries, which illustrate the cyber threat landscape profile of 2021.

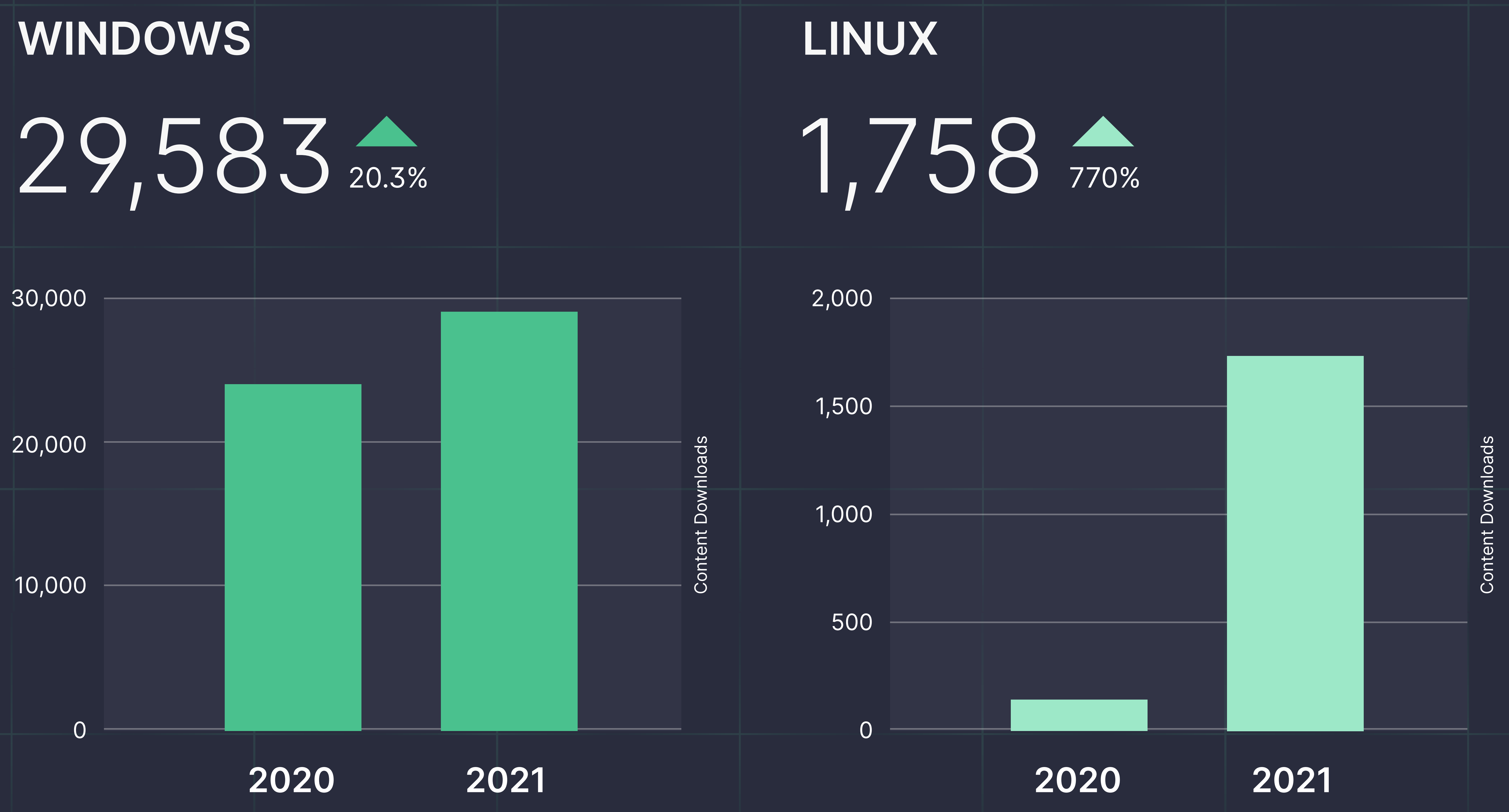
TRENDING SECURITY USE CASES OF 2021

SOC Prime's research indicates that in 2021 over half of all detection content addressed security use cases in the area of **Threat Hunting on Endpoints** (50.5%). This figure supports proactive mitigation aimed at confronting the growing ransomware trend. **Proactive Detection of Vulnerability Exploitation** and **Cloud Security** ranked as two other top content priorities in 2021, with the latter having considerably increased by 233% as compared with 2020. Collectively, these three security use cases covered 89% of all detection content consumed by SOC Prime users. SOC Prime's increasingly informed user community recognizes that proactive Threat Hunting operations can be significantly enhanced by leveraging detection content derived from collaborative cyber defense contribution. Apart from these three most dominant security use cases of 2021, other content consumption trends involved **Active Directory Security** and **Compliance** covering an additional 11% of all detection content downloads from SOC Prime's platform, illustrating a high demand for Azure Active Directory detections and compliance-specific use cases continuously utilized by financial institutions and organizations in the telecom sector.



THREAT HUNTING ON ENDPOINTS

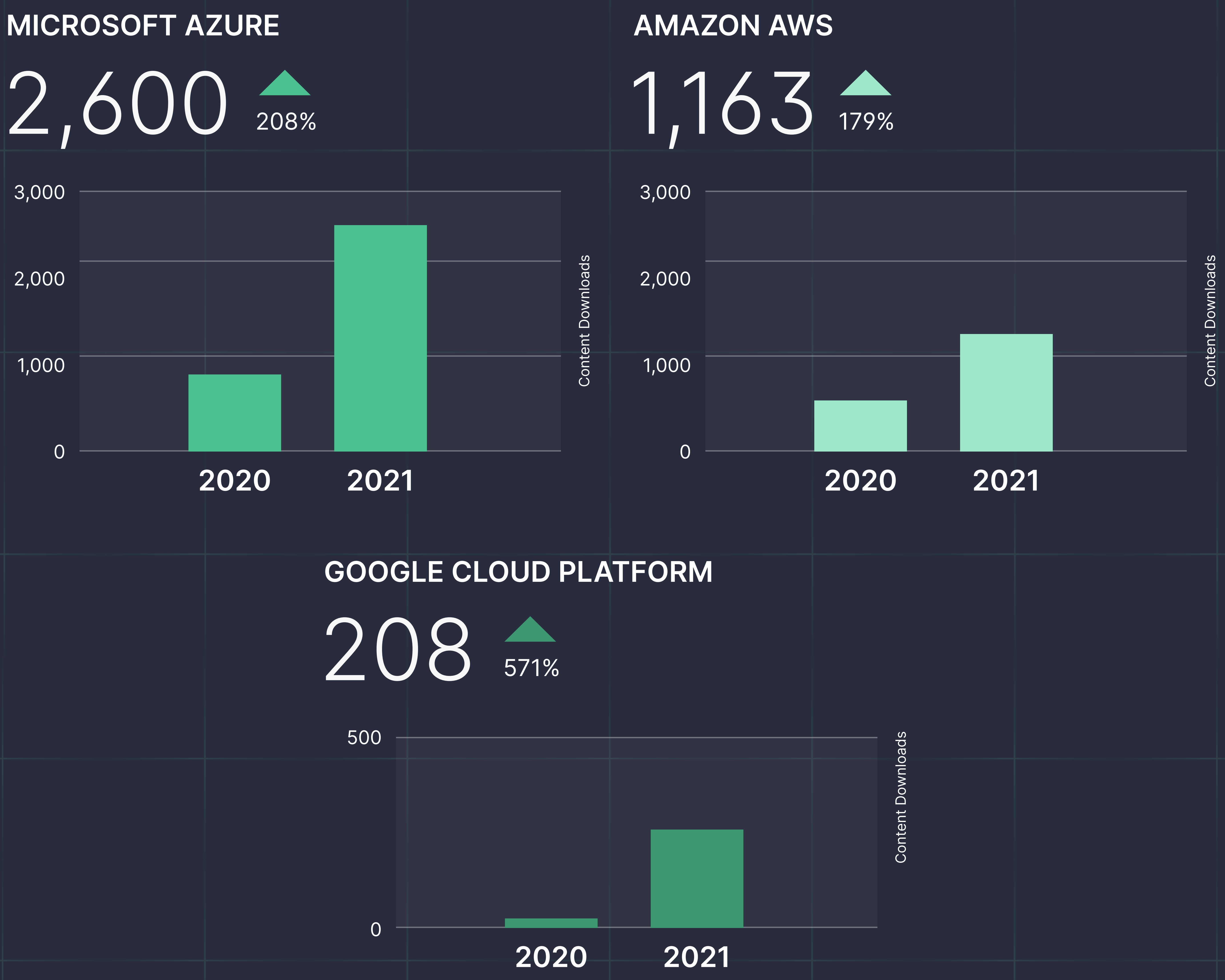
In 2021, **Threat Hunting on Endpoints** ranked the highest among other security use cases illustrating a growing demand for endpoint protection, specifically on Windows and Linux systems. Following this content consumption trend, we realize the need to build Threat Hunting based on endpoint telemetry, continuously expanding the detection coverage based on MITRE ATT&CK®. In 2021, the coverage of MITRE ATT&CK techniques and sub-techniques across all endpoints increased by 18.5% as compared with 2020, reaching 84%. Moreover, the year 2021 saw a significant rise in detection content consumption for Linux threats with content downloads increased by 770%, which points to a pressing need for endpoint protection against emerging cyber-attacks affecting Linux-based environments.



Threat Hunting on Endpoints Content Consumption Dynamics

CLOUD SECURITY

With organizations continuously switching to hybrid and cloud-based environments, cloud security is becoming of paramount concern, which illustrates a growing demand for detection algorithms representing this use case. The year 2021 saw immense growth in detection content consumption for the cloud content downloads for Microsoft Azure and for Amazon AWS increased by 208% and 179% respectively. Content downloads for Microsoft Azure increased by 208% and for Amazon AWS — by 179% respectively. Content downloads for Google Cloud Platform also significantly rose as compared with 2020 by 571% percent, displaying a growing interest in detection content tailored for this cloud-based solution and an overall rising trend for detection content needs addressing the **Cloud Security** use case.

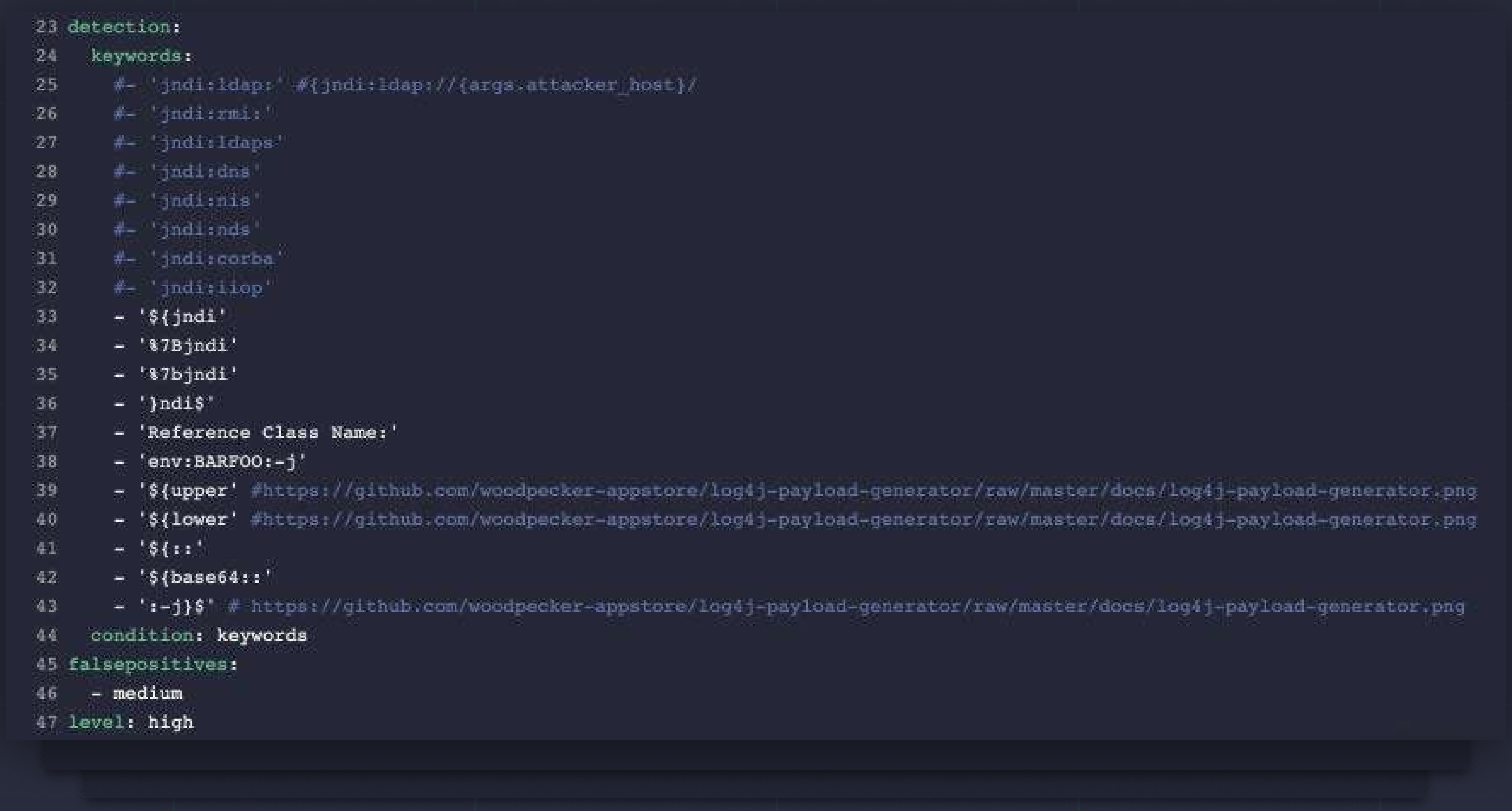


Cloud Security Content Consumption Dynamics

LOG4J VULNERABILITIES: COMBATING GLOBAL THREATS WITH COLLABORATIVE EXPERTISE

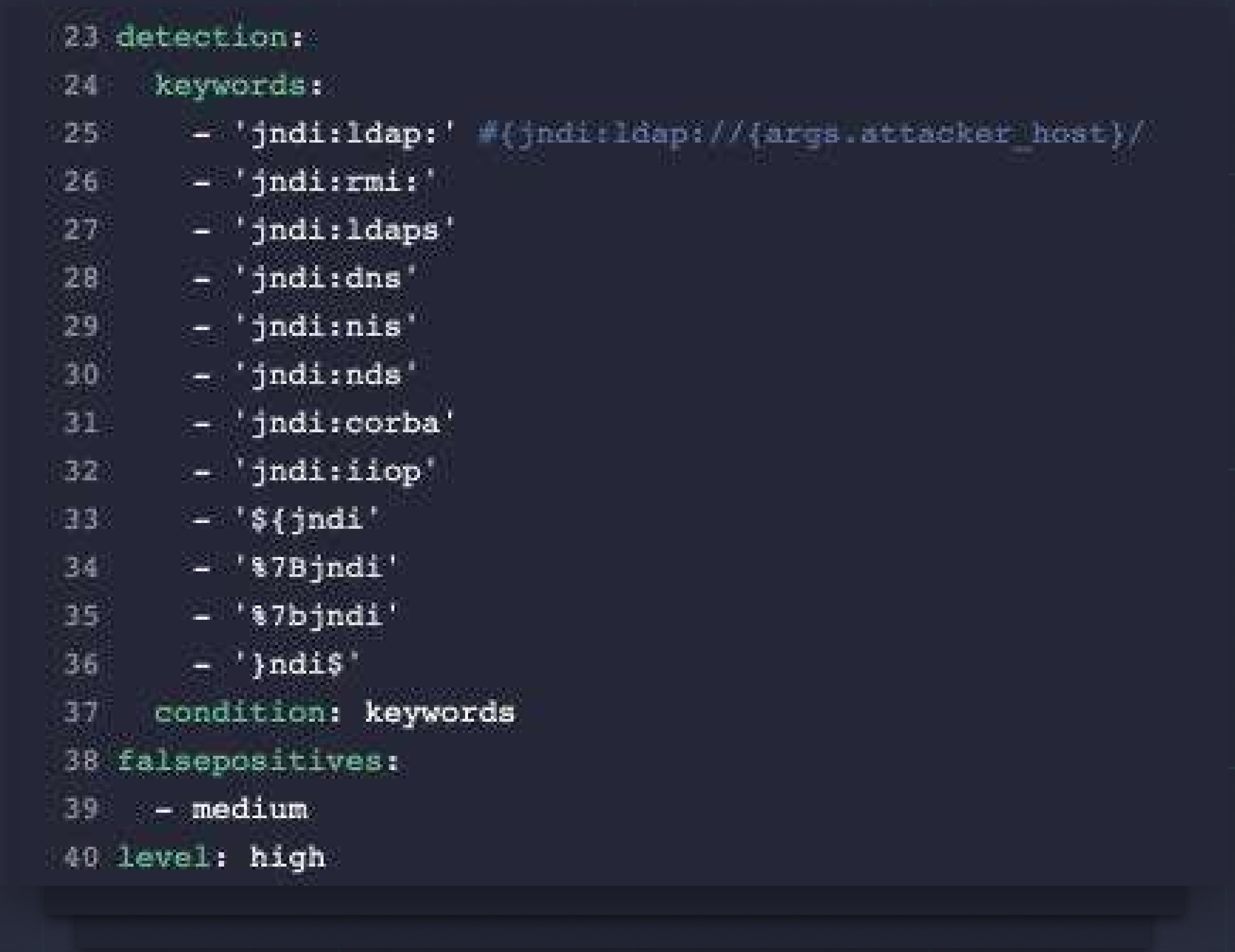
Proactive Detection of Vulnerability Exploitation remains one of the most common security use cases. At the end of 2021, the cybersecurity community was shaken by critical Log4j vulnerabilities (CVE-2021-44228, CVE-2021-45046) affecting the Apache Log4j Java logging library. Given that Log4j is open-source software used across all major operating systems and thousands of products, the critical easy-to-exploit vulnerability became a threat of a global scale. Adding to the enormous scope on affected systems, the Log4j exploits were hard to detect, with their notoriety and impact evolving hour by hour. While the defense vendors started to produce detections for known exploits and announced working protections, attacks swiftly evolved within the first 24 hours, morphing stock exploits into obfuscated ones.

Seeing Log4j vulnerabilities as an extremely critical threat to the global community, SOC Prime worked expeditiously to outspeed the attackers. Starting from stock exploits detection produced within hours after public revelations, our experts tracked the Log4j threat evolution to coordinate the collaborative cyber defense. Sigma rules developed to detect simple Log4j exploits without obfuscations were contionuously updated keeping up with the pace of attackers that applied obfuscations and bypass techniques to evade detection.



```
detection:
  keywords:
    #- 'jndi:ldap:' #{jndi:ldap://{args.attacker_host}/
    #- 'jndi:rmi:'
    #- 'jndi:ldaps'
    #- 'jndi:dns'
    #- 'jndi:nis'
    #- 'jndi:nds'
    #- 'jndi:corba'
    #- 'jndi:iiop'
    - '${jndi'
    - '%7Bjndi'
    - '%7bjndi'
    - '}ndi$'
    - 'Reference Class Name:'
    - 'env:BARFOO:-j'
    - '${upper' #https://github.com/woodpecker-appstore/log4j-payload-generator/raw/master/docs/log4j-payload-generator.png
    - '${lower' #https://github.com/woodpecker-appstore/log4j-payload-generator/raw/master/docs/log4j-payload-generator.png
    - '${::'
    - '${base64::'
    - ':-j}$' # https://github.com/woodpecker-appstore/log4j-payload-generator/raw/master/docs/log4j-payload-generator.png
  condition: keywords
falsepositives:
  - medium
level: high
```

Basic Sigma rule code sample with keywords to detect Log4j vulnerabilities produced within hours after threat discovery



```
detection:
  keywords:
    - 'jndi:ldap:' #{jndi:ldap://{args.attacker_host}/
    - 'jndi:rmi:'
    - 'jndi:ldaps'
    - 'jndi:dns'
    - 'jndi:nis'
    - 'jndi:nds'
    - 'jndi:corba'
    - 'jndi:iiop'
    - '${jndi'
    - '%7Bjndi'
    - '%7bjndi'
    - '}ndi$'
  condition: keywords
falsepositives:
  - medium
level: high
```

Modified Sigma rule for detecting obfuscations that try to bypass the original detection method

While obfuscated exploits are hard to detect due to the Sigma language limitations, the SOC Prime Team overcame the challenge with the help of queries in native SIEM languages leveraging regular expressions to enhance the translation quality across multiple SIEM & XDR solutions.

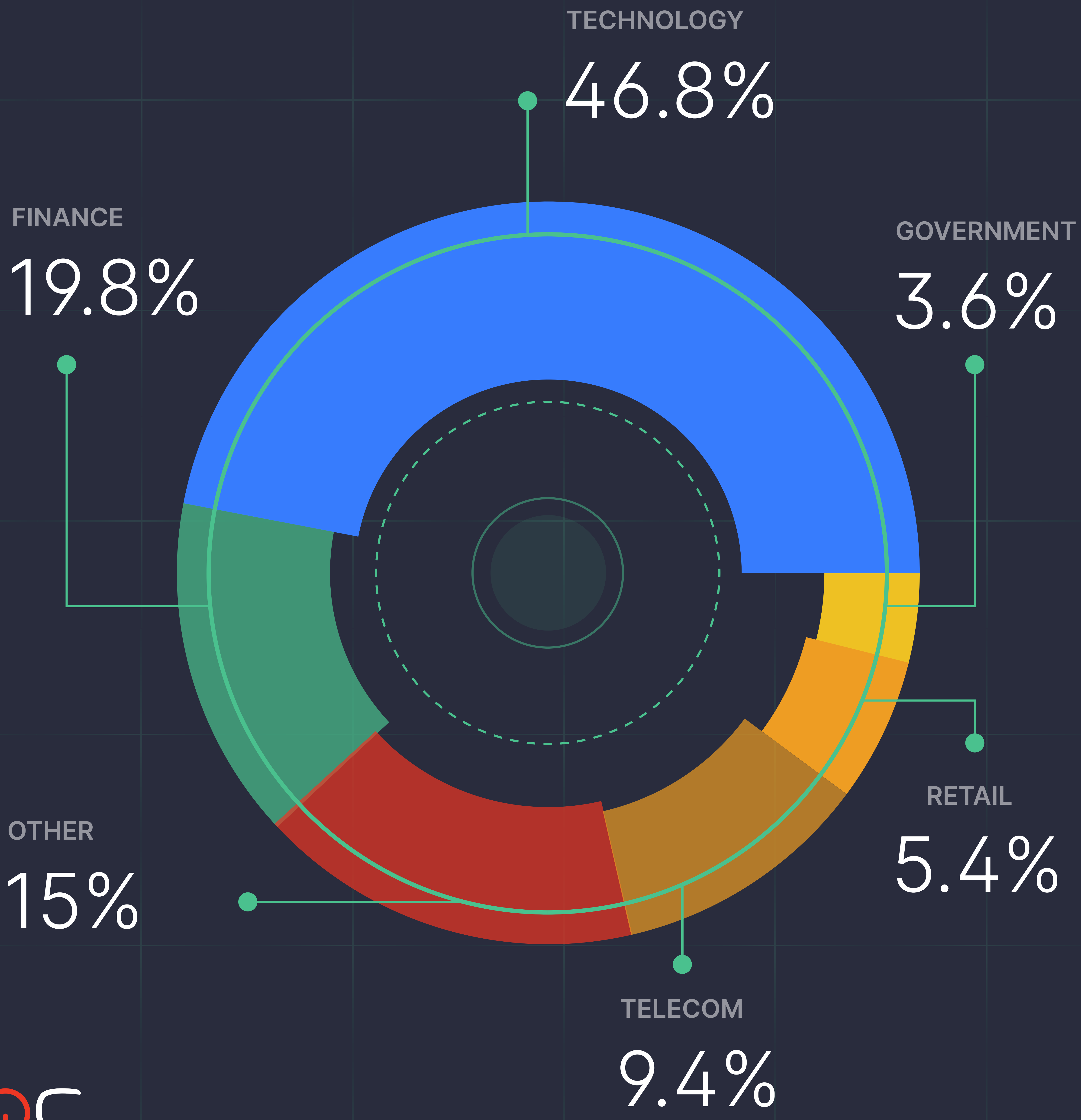
To accelerate threat detection efforts, SOC Prime relied on the Detection as Code approach. While the SOC Prime Team dug into threats within our Lab across all the SIEMs and produced native SIEM language queries alongside the universal Sigma rules, the Threat Bounty content contributors checked cloud attack vectors and researched the broader scope. Within 3 days, SOC Prime released 26 curated Sigma rules, which along with all available translations into native SIEM, EDR, and XDR formats, ended up in 600+ detection algorithms.

As evidence of the growing utilization and effectiveness of collaborative cyber defense, consider the stats below, which draw a comparison between the detection coverage and content consumption to address Log4j vulnerabilities of 2021 and the notorious Zerologon vulnerability (CVE-2020-1472) of 2020:

	ZEROLOGON	LOG4J
SIGMA RULES	17	26 ▲ 52%
ALL DETECTIONS	402	602 ▲ 50%
CONTENT DOWNLOADS	3,894	13,442 ▲ 345%

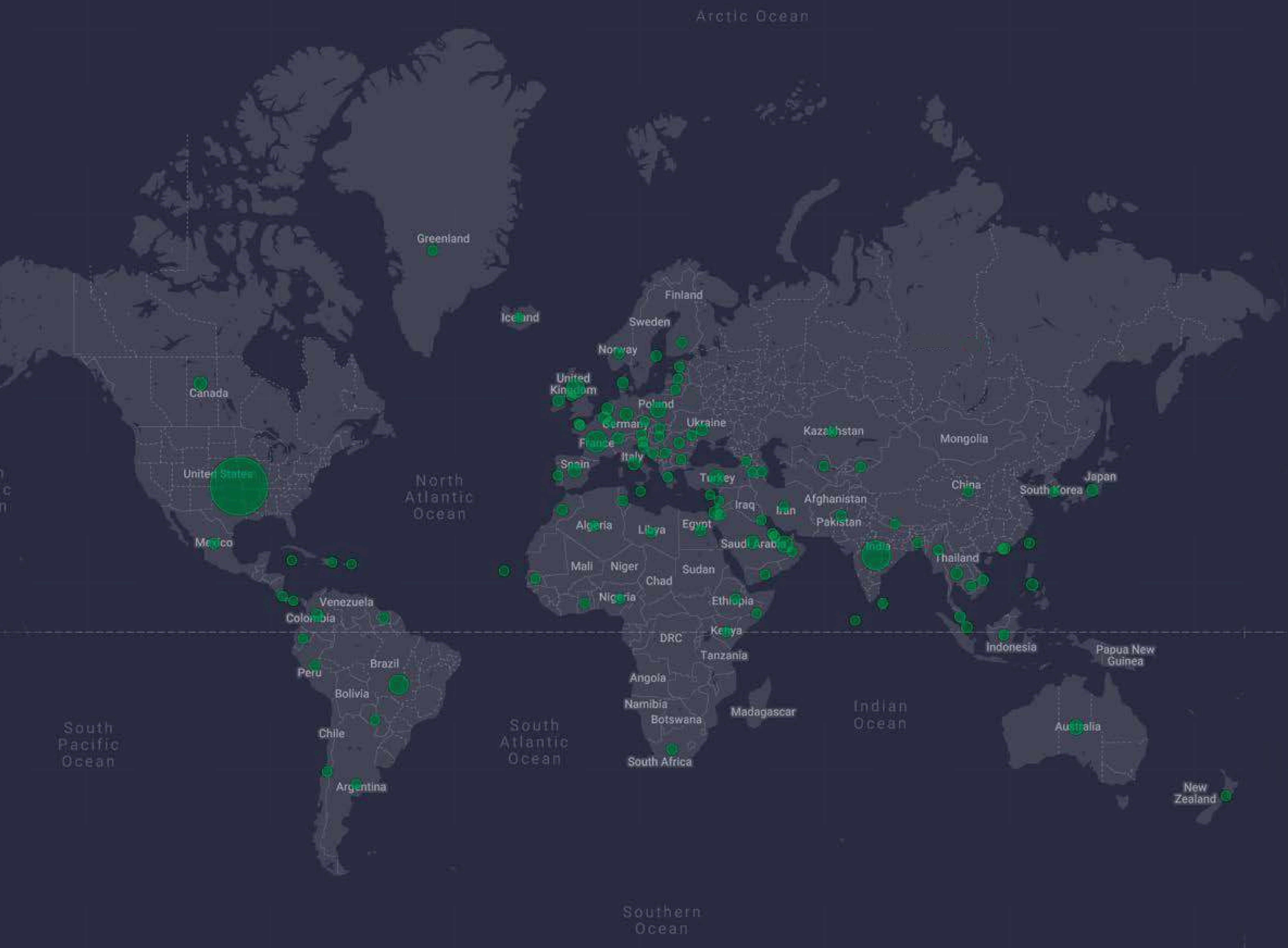
INDUSTRY TRENDS IN CONTENT CONSUMPTION

SOC Prime's research also highlighted that a few industries dominated the utilization of collaborative threat detection content to power their SOC operations as illustrated below. Based on the content download telemetry of 2020-2021, the top industries that consume Detection-as-Code content are **Tech, Finance, Telecom, Retail**, and **Government** covering 85% of all industry sectors with the **Technology** sector holding a leading position since 2020 and comprising almost a half of all detection content downloads (46.8%). Among other top industries covering 15% of content consumption for the second year in a row remain organizations in **Healthcare**, **Capital Goods**, and **Diversified Consumer Services**.



GEOGRAPHIC HEATMAP OF CONTENT DOWNLOADS

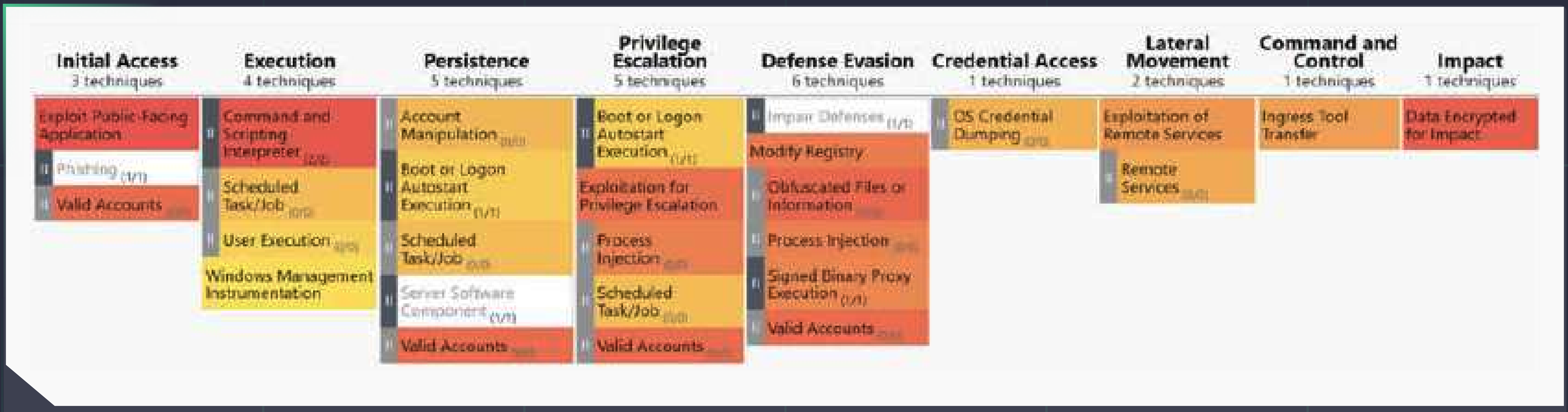
The year 2021 shows the expanding geography of cybersecurity professionals interested in collaborative cyber defense to increase the effectiveness of threat detection operations. SOC Prime's research shows that U.S., France, Germany, UK, Australia, and India are among top Detection-as-Code content consumers, with a growing trend observed within South America and Europe.



MITRE ATT&CK® TRENDS

Detection-as-Code content in the SOC Prime's platform is mapped to corresponding MITRE ATT&CK techniques whenever possible, which enables aligning the behaviors identified by detection rules with the industry standard for classifying adversary activity. This report provides insights into the most common MITRE ATT&CK techniques covered by the Detection-as-Code content in 2021. The heatmap based on the MITRE ATT&CK Navigator layer provided below illustrates the distribution of the top 25 techniques.

The MITRE ATT&CK coverage trends illustrate that Defense Evasion, Privilege Escalation, and Persistence tactics are the most common ones for which Sigma rules were created in 2021. Less covered with Sigma detections were Credential Access, Lateral Movement, Command and Control, and Impact tactics, which helps identify potential gaps when building a future-proof roadmap for improving visibilty.



Initial Access 3 techniques	Execution 4 techniques	Persistence 5 techniques	Privilege Escalation 5 techniques	Defense Evasion 6 techniques	Credential Access 1 techniques	Lateral Movement 2 techniques	Command and Control 1 techniques	Impact 1 techniques
Exploit Public-Facing Application	Command and Scripting Interpreter	Account Manipulation	Boot or Logon Autostart Execution (1/1)	Impair Defenses (1/1)	OS Credential Dumping	Exploitation of Remote Services	Ingress Tool Transfer	Data Encrypted for Impact
Phishing (1/1)	Scheduled Task/Job	Boot or Logon Autostart Execution (1/1)	Exploitation for Privilege Escalation	Modify Registry		Remote Services		
Valid Accounts	User Execution	Scheduled Task/Job	Process Injection	Obfuscated Files or Information				
	Windows Management Instrumentation	Server Software Component (1/1)	Scheduled Task/Job	Process Injection				
		Valid Accounts	Valid Accounts	Signed Binary Proxy Execution (1/1)				
				Valid Accounts				

MITRE ATT&CK Navigator layer displaying the 25 top ATT&CK techniques of 2021 based on SOC Prime's research

TOP TEN ATT&CK TECHNIQUE TRENDS

- In 2021, the **Exploit Public-Facing Application (T1190)** technique climbed to the #1 position as compared with 2020 based on the volume of detection content created. This trend is shaped by an avalanche of critical vulnerabilities affecting open-source projects and popular software products. For instance, global-scale threats posed by Log4j exploits and a zero-day in Zoho ManageEngine Desktop Central (CVE-2021-44515) showcase a growing demand for detection content to combat an emerging volume of attacks.

- The **Signed Binary Proxy Execution (T1218)** technique is still among the top 3 leaders since it's continuously leveraged by attackers allowing them to use the Living-off-the-Land binaries to evade security controls.

- **Command and Scripting Interpreter (T1218)** continues to rank highly on the list of trends since a wide range of command-line interfaces and scripting capabilities are actively abused by attackers as a means of executing arbitrary commands, thus playing a significant role in a great number of the threats our Detection-as-Code content addresses.

- **Phishing (T1566)** also ranked in the top 5 techniques as a response to a rapid surge in phishing campaigns across the globe pushing organizations to create a demand for detection content addressing the related cyber threats.

TOP TEN MITRE ATT&CK TECHNIQUES TRENDS 2020 VS 2021

#1	▲ +2	T1190 Exploit Public-Facing Application
#2	▼ -1	T1059 Command and Scripting Interpreter Services
#3	▲ +1	T1218 System Binary Proxy Execution Application
#4	NEW	T1078 Valid Accounts Execution
#5	▲ +2	T1566 Phishing
#6	▲ 0	T1547 Boot or Logon Autostart Execution
#7	NEW	T1486 Data Encrypted for Impact
#8	NEW	T1027 Obfuscated Files or Information
#9	NEW	T1021 Remote Services
#10	▼ -1	T1003 OS Credential Dumping Escalation

TOP 2021 EXPLOITS & THREATS

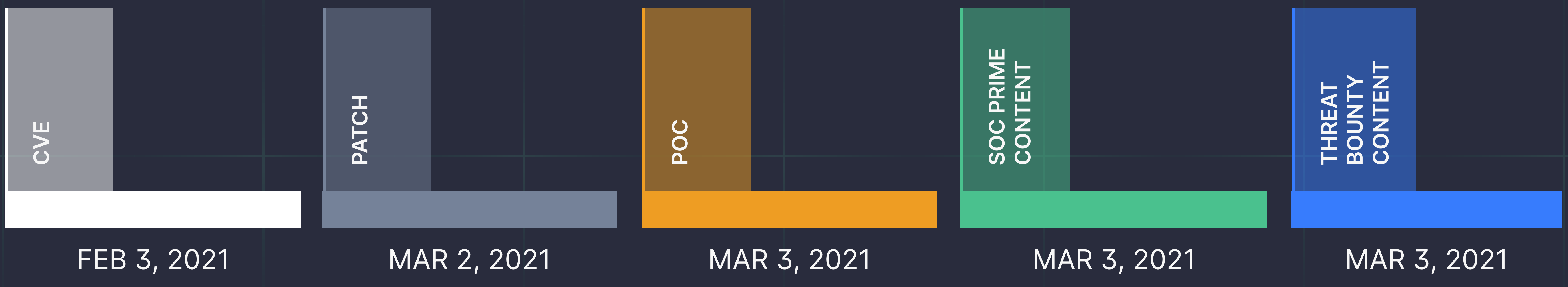
Trends that were established in 2020 continued throughout 2021. The attack surface was enhanced by the global pandemic, which led to increased reliance on remote workforces and new vulnerabilities created by ever-growing supply chains with their enhanced risks in terms of potentially devastating cascading effects. These factors contribute to establishing an attractive and growing threat landscape for adversaries to intensify the scale and scope of attacks.

The analysis below outlines the most impactful and newsworthy vulnerabilities of 2021, including public exploits, major incidents, and trends that impacted the cybersecurity domain last year.

Microsoft Exchange ProxyLogon Attack (CVE-2021-26857, CVE-2021-26855, CVE-2021-26858, CVE-2021-27065)

Microsoft Exchange is one of the most common email solutions in the world that is integral to daily operations and secure connection for many global enterprises. In 2021, a series of vulnerabilities collectively known as ProxyLogon emerged claiming to be the most severe and impactful in the Exchange history:

- Enabled a threat actor to bypass the authentication requirements and obtain admin privileges on unpatched Microsoft Exchange servers.
- Actively used to upload the initial web shell to the server for future malicious access and actions.
- Leveraged by multiple threat actors, including APT groups, to target government institutions, large enterprises, as well as local small businesses.
- The SOC Prime Team together with crowdsourced Threat Bounty researchers and content developers released detections for ProxyLogon on March 3, 2021. The very same day the proof-of-concept (PoC) exploit was published.

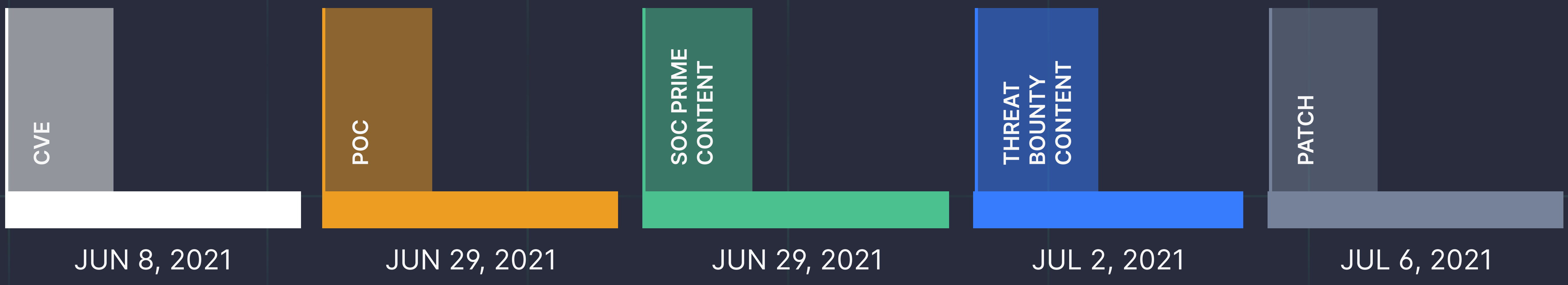


TOP 2021 EXPLOITS

PrintNightmare Vulnerabilities (CVE-2021-1675/CVE-2021-34527)

In 2021, a critical remote code execution (RCE) bug found in Windows Print Spooler allowed attackers to compromise the entire infrastructure of a targeted organization. Some further details and impact of the vulnerability are as follows:

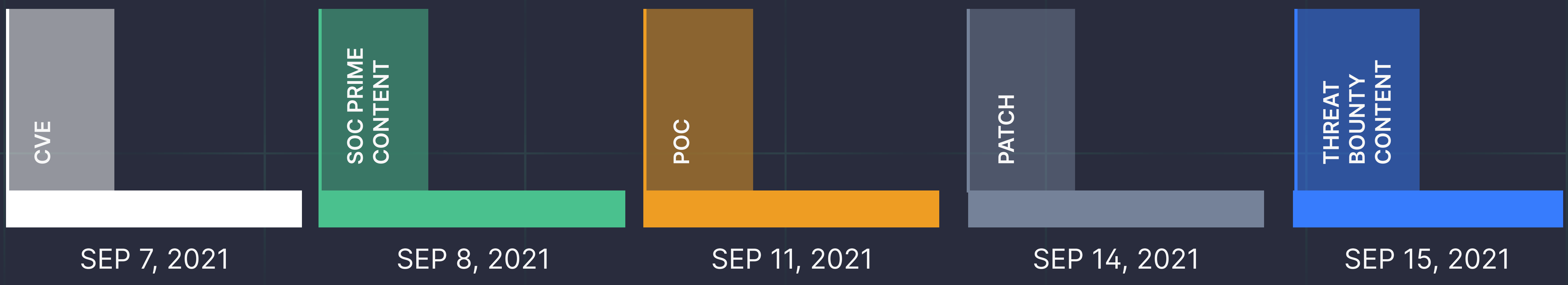
- Resulted from the improper privileged file operations performed by the Windows Print Spooler service.
- Allowed attackers with a regular, unprivileged user account to gain admin rights and remotely run arbitrary code with the SYSTEM privileges.
- Multiple PoC exploits for PrintNightmare were publicly released and adopted by threat actors to proceed with ransomware attacks and other malicious campaigns.
- SOC Prime Team released detections for this vulnerability on June 29, 2021, which is the very same day the PoC exploit was published.



Microsoft MSHTML Vulnerability (CVE-2021-40444)

MSHTML is Microsoft's browser engine for the Microsoft Windows version of Internet Explorer. In 2021, Microsoft Threat Intelligence Center (MSTIC) identified an alarming vulnerability in MSHTML that resulted in remote code execution allowing attackers to distantly run malicious code on targeted Windows systems. Below are further details of the vulnerability exploitation attempts:

- Actively exploited in the wild with the help of weaponized Microsoft Office documents aimed at malicious scripts delivery.
- Organizations within energy, industrial, banking, medical technology, telecommunications, and IT sectors have fallen victims to the targeted attacks.
- SOC Prime Team released detections for this vulnerability on September 8, 2021, which is three days earlier than the PoC exploit was published.

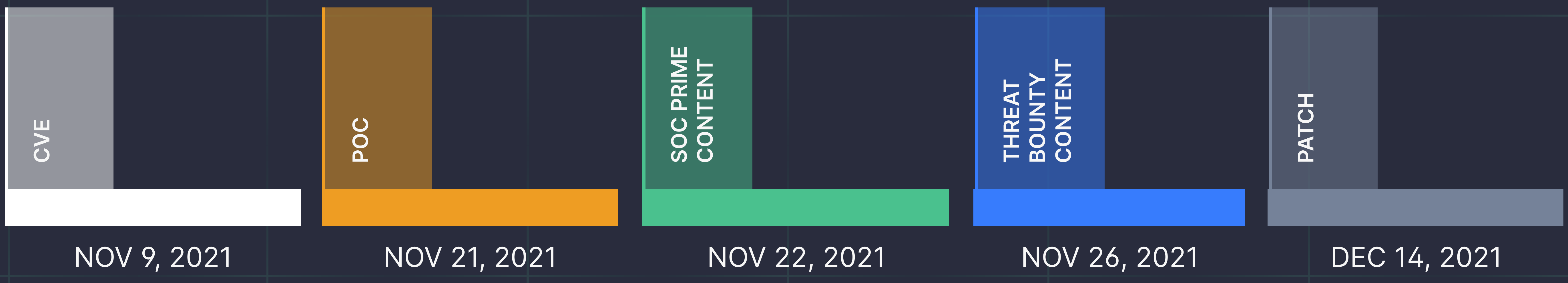


TOP 2021 EXPLOITS

Windows Installer Elevation of Privilege Vulnerability (CVE-2021-41379/CVE-2021-41379)

In November 2021, the security researcher Abdelhamid Naceri detected an elevation of privileges vulnerability affecting Windows Installer. This critical vulnerability enabled an unprivileged user to run the command prompt as SYSTEM. Further details indicate:

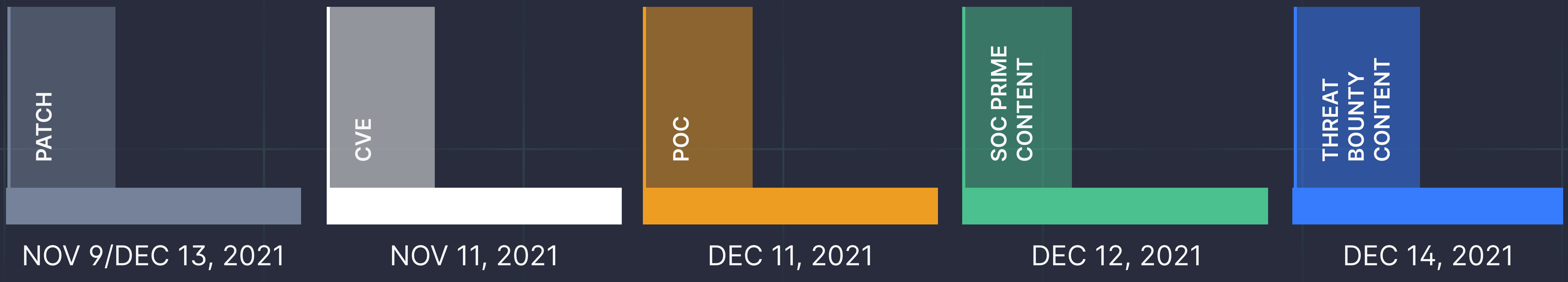
- The InstallerFileTakeover PoC for this flaw allowed hackers to bypass the patch released by Microsoft, reach admin privileges when logged into Windows, and run any malicious code on the vulnerable instance.
- Affected all supported Windows versions, including Windows 11 and Server 2022.
- SOC Prime Team released detections for this vulnerability on November 22, 2021, which is the next day after the PoC exploit was published.



Active Directory Domain Service Privilege Escalation Vulnerabilities (CVE-2021-42287, CVE-2021-42278)

Active Directory is Microsoft's proprietary directory service for Windows domain networks that is designed to enable administrators to manage access permission to network resources. In 2021, Domain Controller Impersonation (CVE-2021–42287) and sAMAccountName Spoofing (CVE-2021–42278) vulnerabilities were discovered that, if chained, allowed a regular domain user to easily take over a domain controller. More details are as follows:

- The PoC tool exploited in the wild allowed hackers to escalate privileges from standard Active Directory user to a Domain Admin in default configurations.
- Enabled threat actors to easily deploy additional malware to the targeted infrastructure, including various ransomware samples, after gaining domain access.
- SOC Prime Team released detections for this CVE on December 12, 2021, which is the next day after the PoC exploit was published.



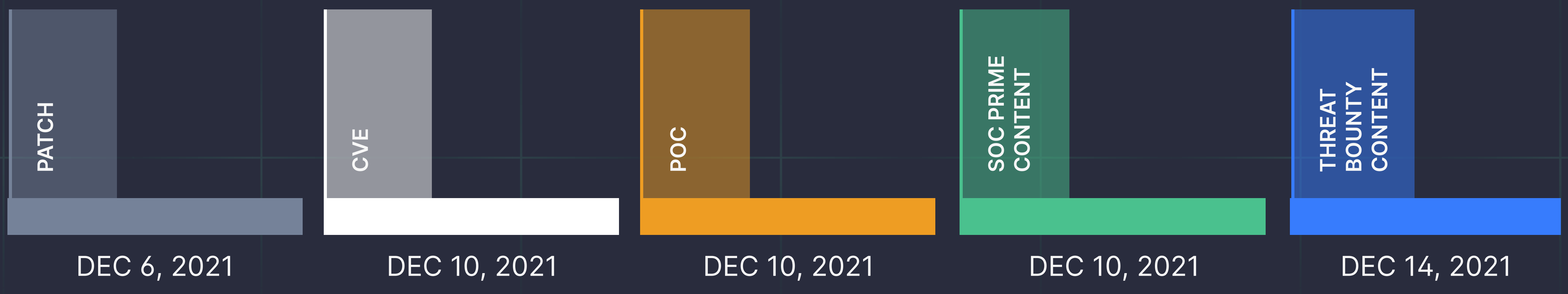
TOP 2021 EXPLOITS

Critical Vulnerabilities in Log4j Java Library (CVE-2021-44228, CVE-2021-45046)

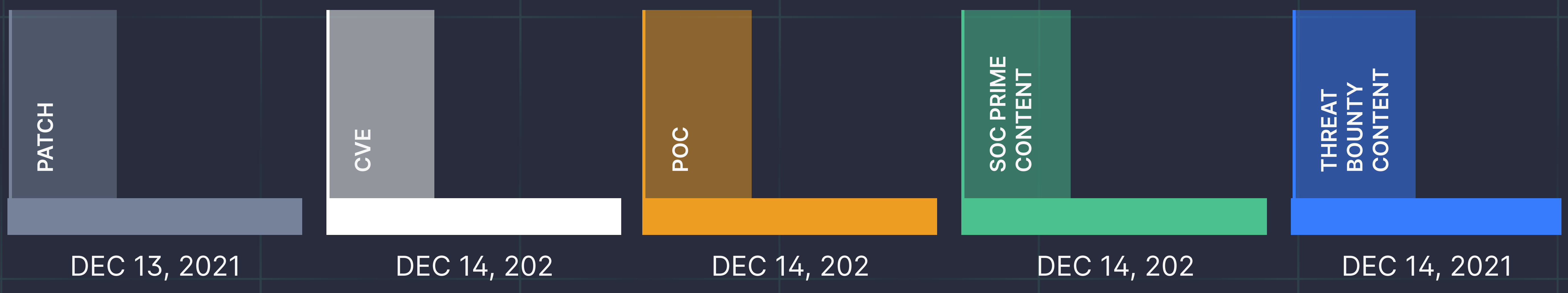
Apache Log4j Java logging library is used in most Java applications. At the end of 2021, critical vulnerabilities aka Log4Shell affected many versions of the Apache Log4j apps that enabled hackers to perform remote code execution and take full control over affected instances. Below are further details:

- Hundreds of millions of devices around the globe were found vulnerable as Log4j is one of the most popular logging libraries used online.
- Such world-leading companies as Atlassian, Amazon, Apple, IBM, Oracle, Cisco, and Google found their software affected.
- Researchers winessed over 1,8 million in-the-wild attacks using at least 70 distinct malware families during first weeks after public PoCs release.
- The vulnerability is still actively exploited in the wild by multiple threat actors, including the state-sponsored APT35 group and various financially-motivated adversaries.
- SOC Prime Team released detections for CVE-2021-44228 on December 10, 2021 and for CVE-2021-45046 on December 14, 2021, which is the very same day the public PoC exploits were published.

CVE-2021-44228



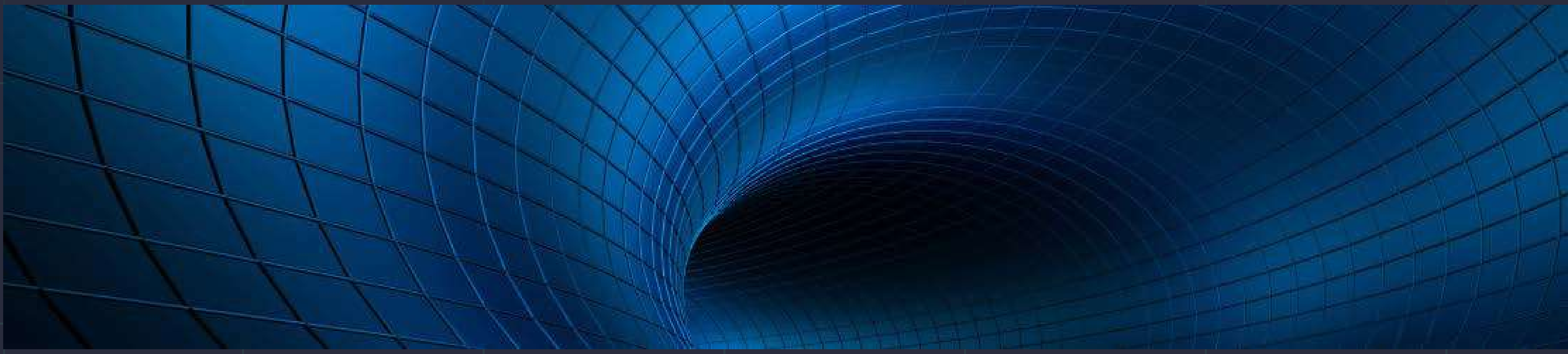
CVE-2021-45046



You can explore detection content for these critical vulnerabilities in SOC Prime's platform by directly searching for the CVE ID.

View Detections Here

TOP 2021 INCIDENTS

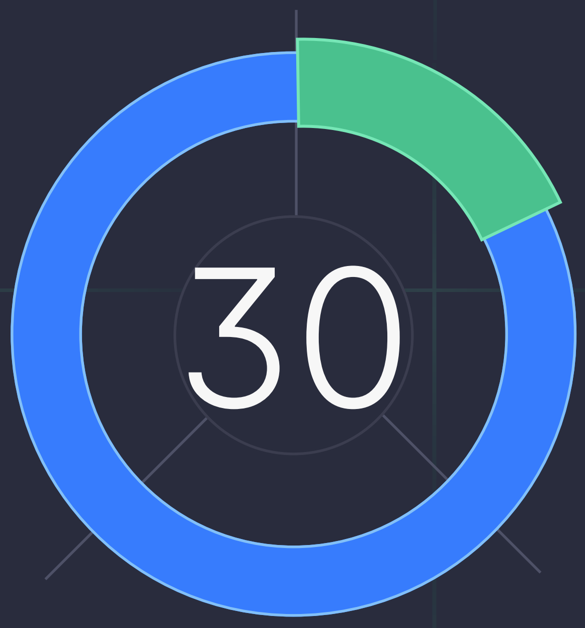


Colonial Pipeline Hack

Colonial Pipeline is an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States. On May 7, 2021, the DarkSide hacking collective launched a massive ransomware attack against Colonial Pipeline IT infrastructure. This incident is claimed to be the largest publicly disclosed cyber-attack against the U.S. critical infrastructure to date.

- Threat actors got access to the Colonial Pipeline network through an exposed password for a VPN account.
- Nearly 100 gigabytes of data was stolen within a two-hour window, which was followed by a ransomware infection.
- Colonial Pipeline's CEO ultimately authorized a $4.4 million ransom payment to restore the systems.
- The incident resulted in partial fuel pipeline shutdown, temporary gasoline outages across the U.S. East Coast, as well as jet fuel shortage for many carriers.

- In 2021, SOC Prime community released a total of 30 rules to detect DarkSide attacks, 25 of which were contributed by the Threat Bounty Program members.

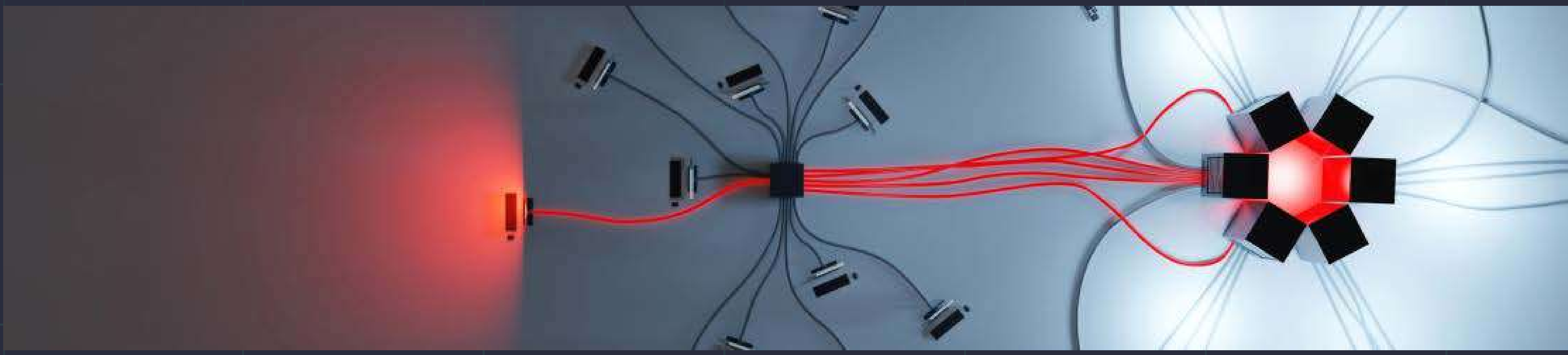


Dedicated Rules
in Threat Detection Marketplace

🟩 SOC Prime	🟦 Threat Bounty
5	25

View Detections for DarkSide Hacking Collective

TOP 2021 INCIDENTS

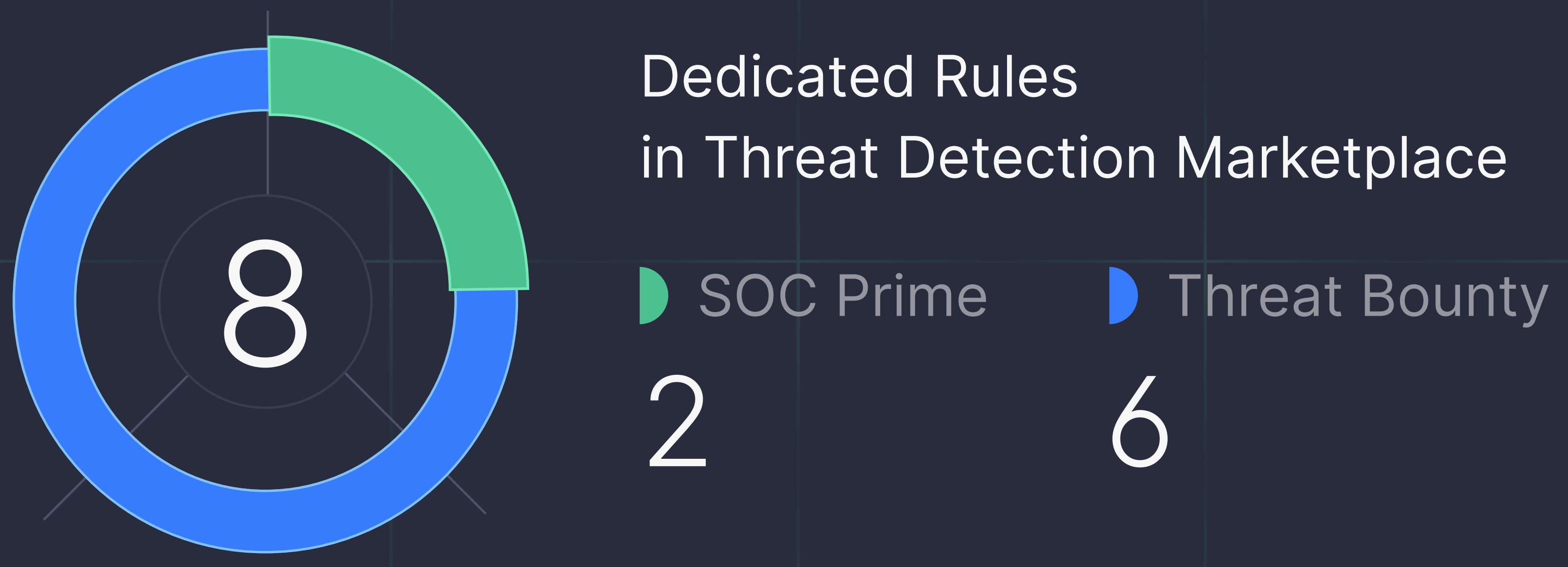


Kaseya Supply Chain Attack

Kaseya VSA remote monitoring and management (RMM) software helps managed service providers (MSPs) and IT teams to manage digital assets, service decks, and more. On July 4, 2021, REvil ransomware gang leveraged a zero-day vulnerability in Kaseya's VSA software to launch a devastating supply chain attack. As a result, dozens of major MSPs and multiple customers worldwide found their assets infected with ransomware. Further details of the attack are as follows:

- A zero-day vulnerability in Kaseya's VSA servers was exploited to bypass authentication on the web panel and execute SQL commands on the appliance to deploy REvil payload to all connected clients.
- Kaseya supply chain attack resulted in more than a million individual devices being encrypted and frozen out of operation.
- Over 30 MSPs and over 1,000 businesses in the U.S., AUS, EU, and LATAM were impacted in the course of the attack.

- SOC Prime community released a total of 8 rules dedicated to the Kaseya supply chain attack detection, 6 of which were crafted by the Threat Bounty Program members.



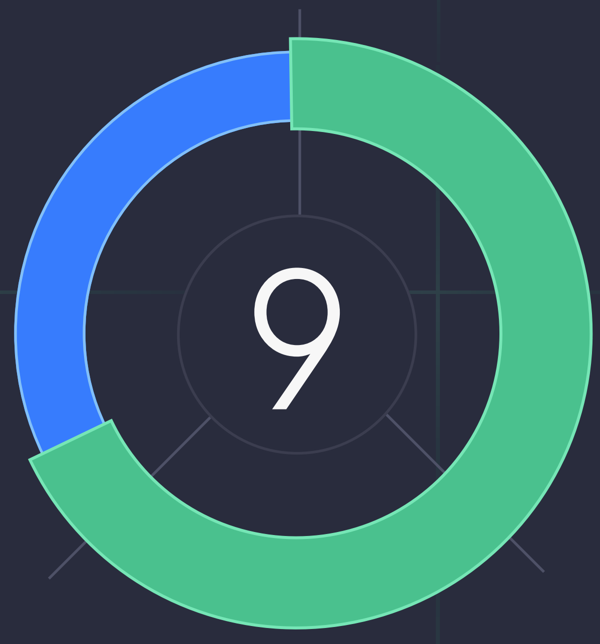
View Detections for Kaseya Supply Chain Attack

WhisperGate Attack Against Ukrainian Government

On January 13, 2022, a massive data-wiping WhisperGate attack hit Ukraine, taking down the online assets of the country's government, including the Cabinet, seven ministries, the Treasury, the National Emergency Service, and the state services. Moreover, multiple non-profit organizations and major Ukrainian IT firms have fallen victim to the attack.

- Up to 70 websites experienced temporary performance issues due to the intrusion, including Ukrainian government systems, prominent non-profit organizations, and major IT firms.
- The Computer Emergency Response Team of Ukraine (CERT-UA) assumes that most likely threat actors leveraged the vulnerability in the October content management system (CMS) to proceed with the intrusion.
- The analysis of the TTPs leveraged in the course of the attack shows they are similar to those used in BlackEnergy and NotPetya campaigns against the Ukrainian government during 2015-2018.
- Security experts, with the high level of confidence, point that the Russian state-sponsored APT group is responsible for the WhisperGate attack, which was carried out as part of cyber war against Ukraine.
- SOC Prime released detections to identify possible malicious activity associated with WhisperGate on January 17, 2022, which is the very same day the samples were uploaded to VirusTotal.

- SOC Prime community released a total of 9 rules dedicated to the WhisperGate attack detection, 3 of which were crafted by the Threat Bounty Program members.

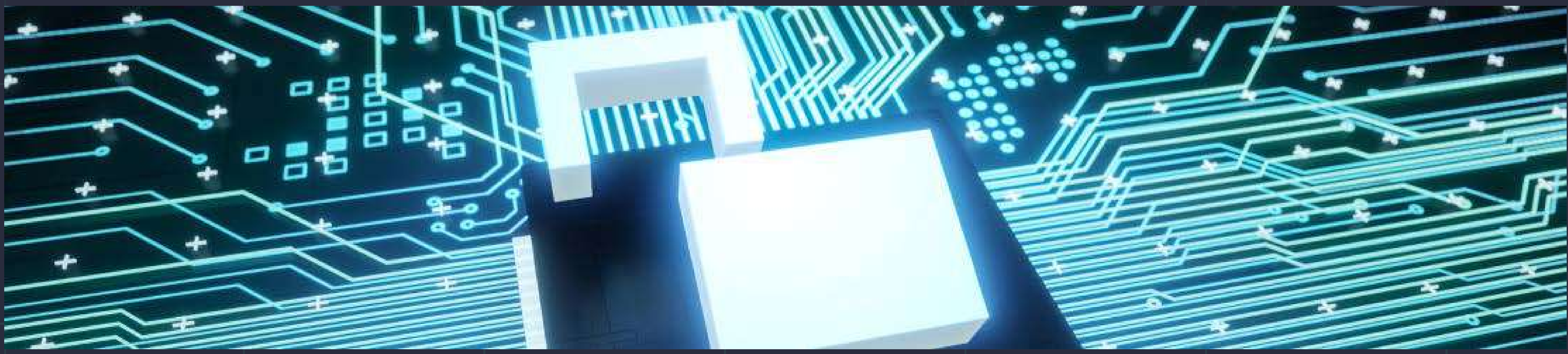


Dedicated Rules
in Threat Detection Marketplace

◗ SOC Prime	◗ Threat Bounty
6	3

View Detections for WhisperGate

TOP 2021 TRENDS

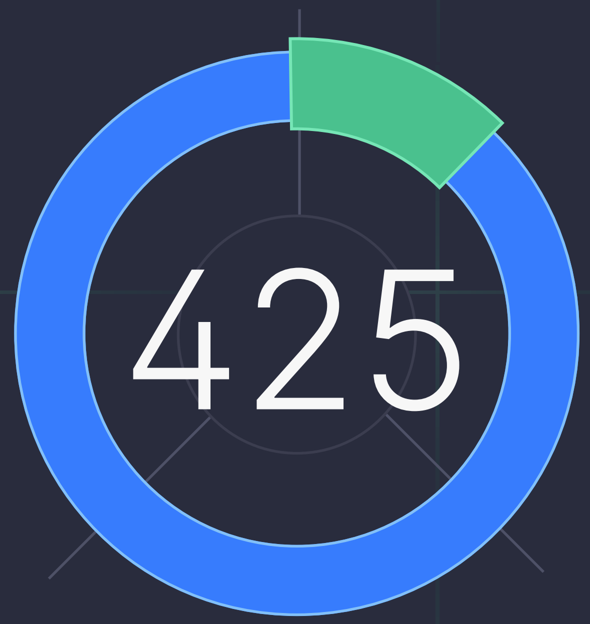


Ransomware

The cybersecurity community is facing a major challenge caused by the escalating threat of high-profile ransomware attacks. Advancing the trend of 2020, ransomware continued to be the number one problem in 2021, with the increasing sophistication of intrusions and a constantly growing number of malicious affiliates.

- The Ransomware-as-a-Service (RaaS) model is gaining a monopoly on the malicious arena, with the majority of ransomware affiliates engaged in various RaaS programs.
- Double Extortion practice is gaining momentum, with NetWalker, RagnarLocker, REvil, and DarkSide heading the list of samples that leverage the approach to gain sky-high profits.
- Ransomware actors increasingly rely on commodity malware to gain initial access to the targeted networks, with Trickbot, Qakbot, Dridex, IcedID, and Zloader being among the most frequently used samples.
- APT groups joined the ransomware domain, with Lazarus and APT27 being increasingly spotted to use their malicious infrastructure for ransomware attacks, thus, enriching the ransomware landscape with sophisticated TTPs borrowed from state-sponsored collectives.

- In 2021, the SOC Prime community released a total of 425 rules aimed at ransomware attack detection, 383 of which were crafted by the Threat Bounty developers.



Dedicated Rules
in Threat Detection Marketplace

SOC Prime	Threat Bounty
42	383

View Detections for Ransomware Attacks

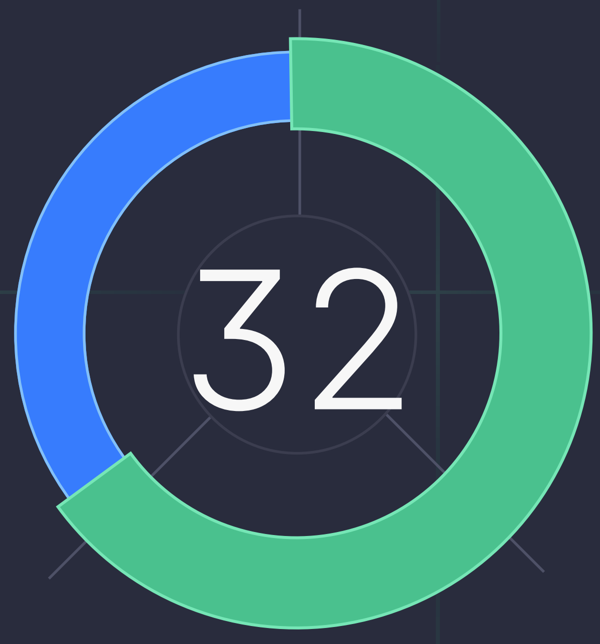
TOP 2021 TRENDS

Supply Chain Attacks

Supply chain attacks have been taken to a new level of sophistication during 2021, with the continuously growing volume of attacks to pose an even bigger menace in the upcoming years:

- Supply chains were increasingly targeted by both cybercriminal gangs and nation-state actors, with SolarWinds, Kaseya, and Codecov incidents.
- Software was a primary supply chain target throughout 2021, with open-source software (OSS) providers as main victims.
- Main supply chain attack vectors include vulnerabilities in open-source applications, compromised pipeline tools, and code integrity

- In 2021, the SOC Prime community released a total of 32 rules aimed at ransomware attack detection, 11 of which were crafted by the Threat Bounty developers.

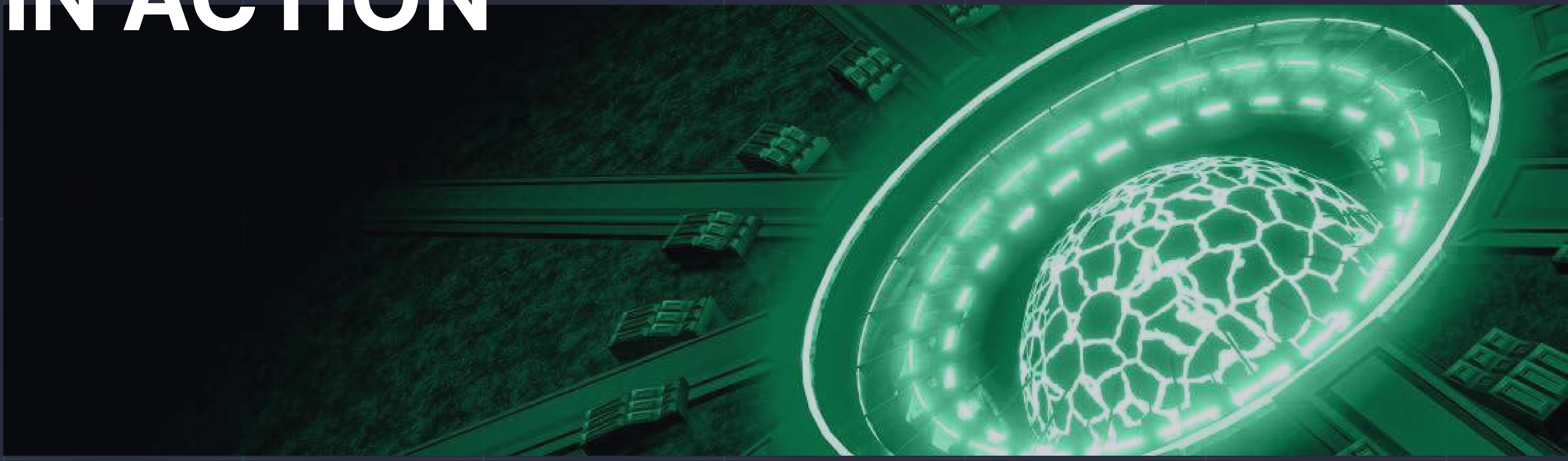


Dedicated Rules
in Threat Detection Marketplace

◗ SOC Prime	◗ Threat Bounty
21	11

View Detections for Supply Chain Attacks

DETECTION AS CODE IN ACTION



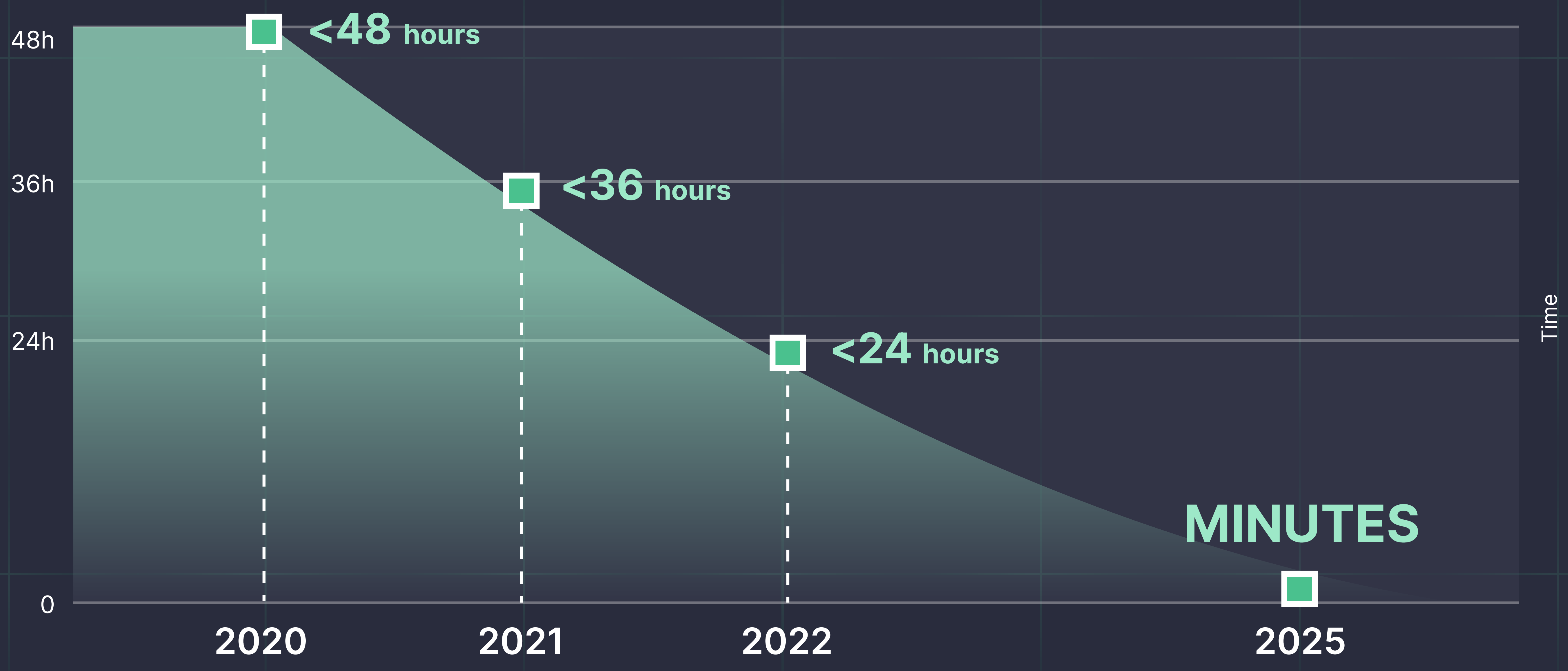
Ever-growing reliance on shared digital assets significantly expands the attack surface and shapes cyber threat trends of 2021-2022. Industry-wide collaboration and streamlined data exchange are vital to proactively withstand the emerging challenges. Thus, the revolutionary Detection as Code approach is gaining momentum. Throughout 2021, SOC Prime has evolved the velocity of detection delivery to confront the current spectrum of cyber risks and keep pace with the rapid evolution of attack sophistication and volume by leveraging collective cybersecurity expertise.

24 HOURS

FOR CONTENT AVAILABILITY

In 2021, SOC Prime delivered Sigma rules to detect critical CVE, a public PoC exploit, or an Offensive Security Tool (OST) within 36 hours after threat discovery, which is 25% faster than in 2020. Backed by the contribution of our growing Threat Bounty community and SOC Prime's Threat Hunting Team, at the turn of 2022, we displayed progression from 36 hours to the current 24 hours with an ultimate goal to deliver critical detections in less than 1 minute assisted by automated capabilities of the Detection as Code platform.

DETECTION CONTENT AVAILABILITY DYNAMICS



2021 EXPERTISE IN NUMBERS

USERS

22,921 ▲ 73%

ORGANIZATIONS

6,933 ▲ 37%

CROWDSOURCED CONTENT CONTRIBUTORS

450+

DETECTION RULES

155,165 ▲ 60%

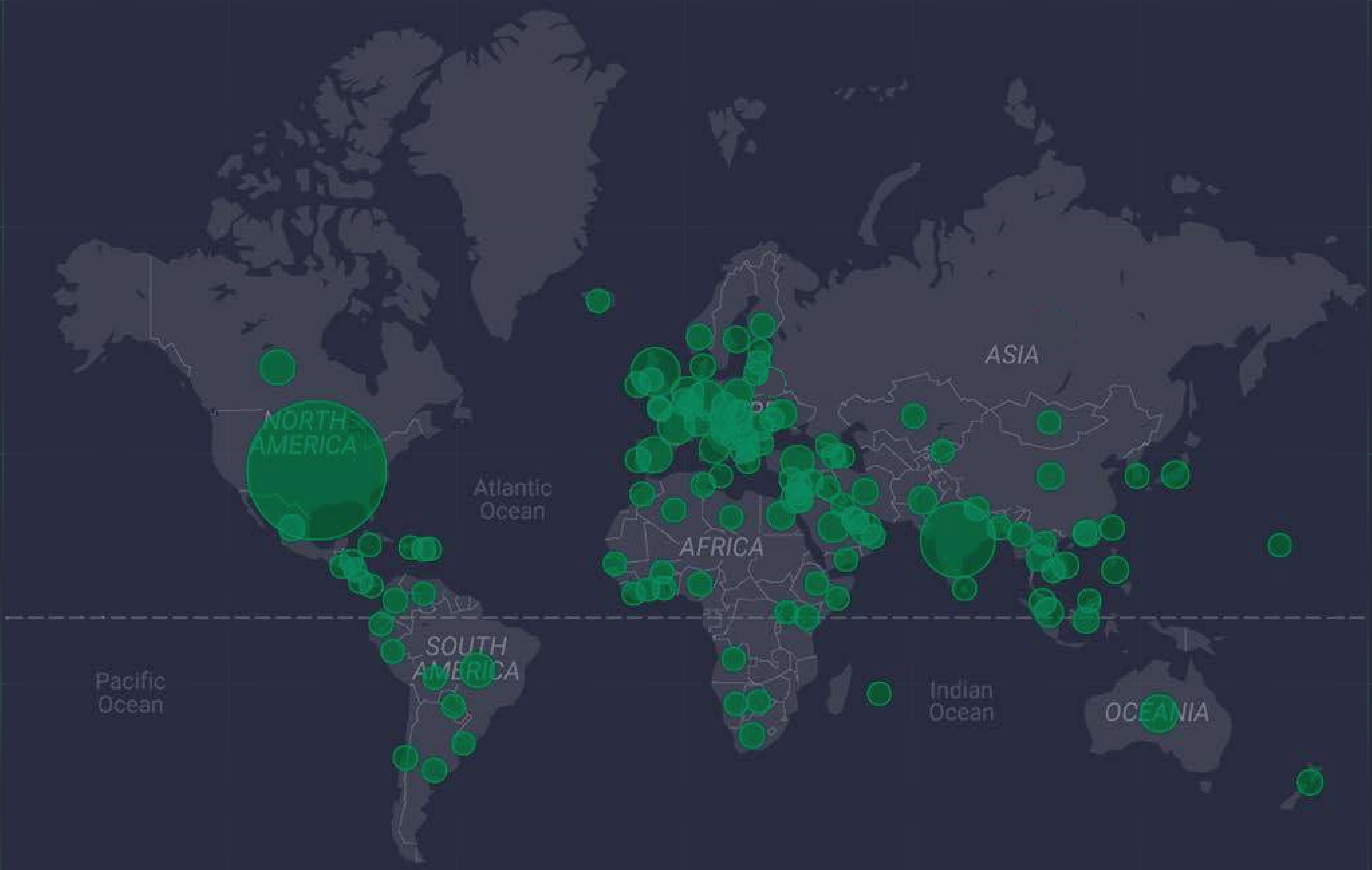
SUPPORTED PLATFORMS

25 ▲ 56%

COLLECTIVE EXPERTISE-AS-A-SERVICE

SOC Prime supports continuous content quality improvement backed by feedback from nearly 7,000 companies and 23,000 users along with 450+ crowdsourced Threat Bounty Program content contributors, which yields the collective cybersecurity expertise growing exponentially. In 2021, this dynamic pool of knowledge saw a 73% increase in the number of InfoSec practitioners leveraging the Detection as Code platform with 37% more organizations protected against critical threats.

The illustration provided below illustrates how cybersecurity professionals leveraging the Detection as Code platform worldwide are geographically distributed based on the 2021 stats. Over the past year, the cybersecurity community has been vastly enriched with InfoSec practitioners from U.S. comprising over one-quarter of all its global audience (25.74%), as well as with Detection-as-Code users from India, UK, France, Australia, Spain, and Germany whose contribution, industry collaboration, and feedback shapes up collective expertise able to outweigh the offensive capabilities.



Heatmap showing the distribution of the global cybersecurity community in 2021

SUPPORT FOR NEXT-GEN CLOUD TECHNOLOGIES

SOC Prime is driven to transform cybersecurity by turning collaboration into security innovation. We continuously broaden support for security analytics tools & technologies and enrich the detection capabilities for next-generation cloud-native SIEM, EDR and XDR platforms, including FireEye, LimaCharlie, FireEye Helix, and Securonix.

With nearly 7,000 global organizations leveraging SOC Prime's platform, we're constantly striving to deliver custom content needs and expand the list of supported language formats. In 2021, we added support for OpenIOC — FireEye, AWS OpenSearch (former name — Open Distro), and Splunk Alerts to ensure we expand integration support and unlock more detection opportunities for the Security Operations Center.

SECURONIX™
FIREEYE™
limacharlie.io
OpenSearch
25+
platforms

SIGMA: VENDOR-NEUTRAL AND FUTURE-PROOF

SOC Prime is the largest commercial contributor to the Sigma standard with 70% of the SIEM and EDR backends built by the SOC Prime Team. Sigma is a common language that enables organizations to unveil the power of global collaboration and community-driven crowdsourcing. Throughout 2021, we continued to develop the efficiency of Sigma-based detections and establish Sigma as the de-facto standard for expressing threat hunting queries.

Here's how Sigma transforms cybersecurity on a global scale:

- Open-source General Public License (GPL) project developed with privacy in mind
- Promotes individual authors via Detection Rules License (DRL)
- Easy-to-learn, fast-to-write and share
- Can be used across multiple security analytics tools
- No Traffic Light Protocol (TLP) limitations, making the use of Sigma faster than CTI

QUALITY

To ensure content quality and the validity of detections SOC Prime operates, we run a true Continuous Integration / Continuous Delivery (CI/CD) lab for all supported technologies to enable continuous testing of content, validate detections with VirusTotal datasets, and deliver a series of quality control checks.

During 2021, we improved Sigma detection content quantity and quality. Our results are reflected below:

ADDED IN 2021	UPDATED	REJECTED FOR QUALITY
2,563 ▲ 49%	86%	66%

INNOVATION

In 2021, SOC Prime introduced filtering of Sigma-based detections by Alerts and Queries, to streamline content search. This innovation significantly reduced analyst workload by allowing security professionals to deploy fully-tested Alerts that are unlikely to generate false positives, or choose Queries better suited for investigations, lookups, and threat hunting operations.

SIGMA RULES	QUERIES	ALERTS
5,188	4,296 (83%)	892 (17%)

PRIVACY AND SECURITY COMMITMENTS

Trust, transparency, and privacy are inherent values SOC Prime delivers throughout all security operations, processes, and procedures to their customers. As a security-conscious organization dedicated to data protection and privacy, SOC Prime collects and processes all user data within the scope of the GDPR driven by a single purpose to improve the customer experience with the Detection as Code platform. All the projects are run by the in-house SOC Prime Team, which ensures privacy protection and no access for third parties to the platform functionality.

SOC 2 TYPE II COMPLIANCE

In 2021, SOC Prime successfully completed the **Service Organization Control (SOC) 2 Type II** audit, demonstrating the company's commitment to customer data security. The audit conducted by I.S. Partners, LLC in line with attestation standards established by the American Institute of Certified Public Accountants (AICPA), validates that SOC Prime has effective controls in place for its cybersecurity solutions, business operations procedures, and technical infrastructure.

THREAT BOUNTY PROGRAM

RESEARCHERS

450+ ▲ 33%

PAID IN BOUNTY

$125,400 ▲ 25%

SIGMA AND YARA RULES

1,550 ▲ 33%

PUBLISHED DETECTIONS

45,767 ▲ 18%

CONTENT USED BY CUSTOMERS (%)

42%

VIEWED CONTENT YOY (%)

67.7%

DOWNLOADED CONTENT YOY (%)

57%

2021 ushered in significant growth in contributor and content volume to the SOC Prime Threat Bounty Program. The number of content authors increased significantly, reflected by a 33% percent growth in Sigma-based detections and YARA rules submitted by Threat Bounty contributors. However, quality remains a primary driver as among over 500 detections submitted to the platform each month, only one-third pass verification and become accessible in the SOC Prime's platform.

Improving content quality remains a top priority. In fact, 86% of previously published detection content was enhanced to accomodate the threat landscape evolution, indicated by the viewed content YoY growth to nearly 68% and the downloaded content YoY growth reaching 57%.

The increasing content quality directly affected the Bounty reward payments, which grew by 25% in 2021. Also, beginning November 2021, we doubled the Bounty rewards for active content contributors.

STAYING IN THE KNOW

In 2021, we invested a great deal of effort and resource into collaboration-enabling tools to promote SOC Prime's crowdsourcing initiative and enhance communication among Threat Bounty members.

- SOC Prime created a dedicated Slack channel for knowledge-sharing, Information exchange, and platform updates. Here also, Threat Bounty Program authors can find out what content is in growing demand to make sure their contribution is highly relevant and tailored to the customers' needs.
- SOC Prime started publishing Monthly Digests covering the results and achievements of the previous month, including the number of detections that passed reviews, insights into top authors, Bounty rewards, and top content.

On December 2, 2021, SOC Prime hosted a dedicated webinar "Threat Bounty Program: Crowdsourcing Detection Engineering" sharing insights into collaborative cyber defense and the latest detections, as well as overviewing the world's largest and most advanced Threat Bounty Program for cyber defenders to contribute detection content.

To delve into more detail about the last year’s Threat Bounty Program achievements, check out our 2021 Monthly Digests below or read the interviews with developers for a closer look at the world's largest and most diverse threat hunting community.

Threat Bounty is a great place to constantly expand your horizons

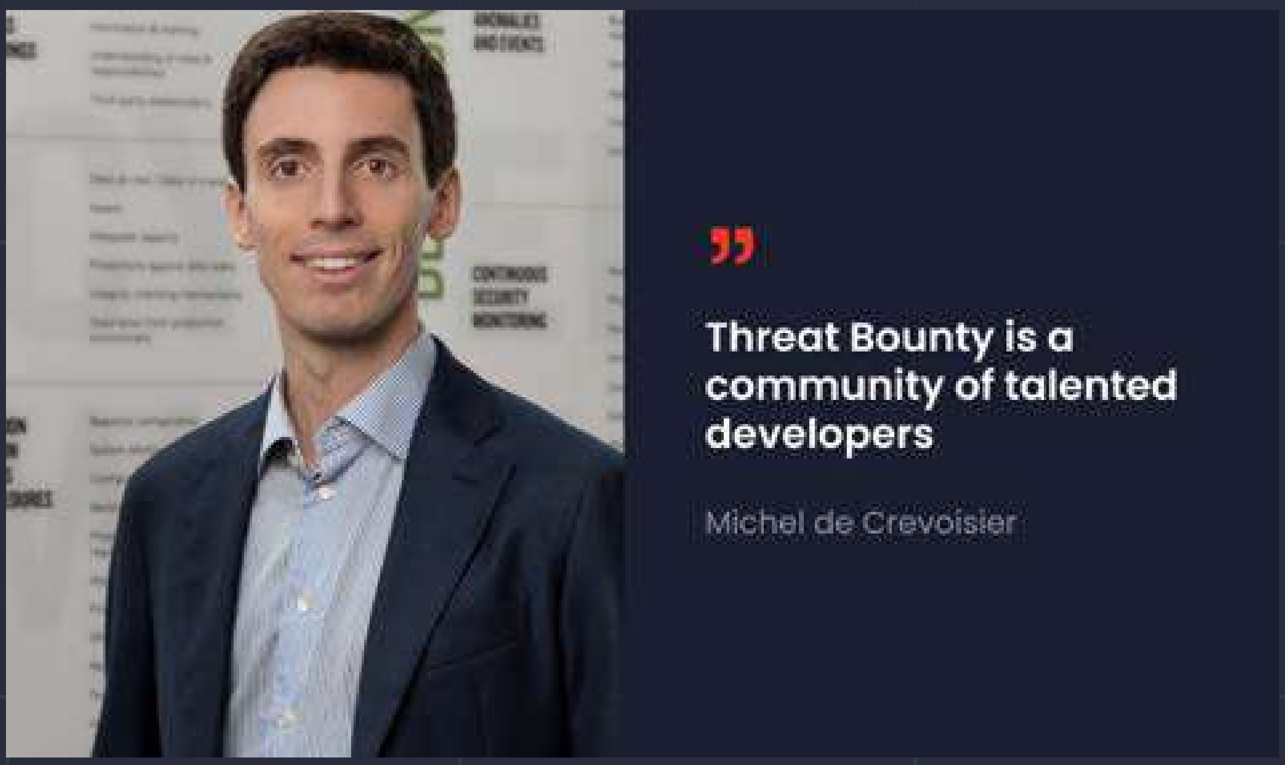
Kyaw Pyiyt Htet

Kyaw Pyiyt Htet

Developers can choose the rules they want to create, and get rewarded

Shelly Raban

Shelly Raban



Threat Bounty is a community of talented developers

Michel de Crevoisier

Michel de Crevoisier

With Threat Bounty, I can improve myself and contribute to the community

Onur Atali

Onur Atali

SOC PRIME THREAT BOUNTY

September 2021 Results

October 2021 Results

November 2021 Results

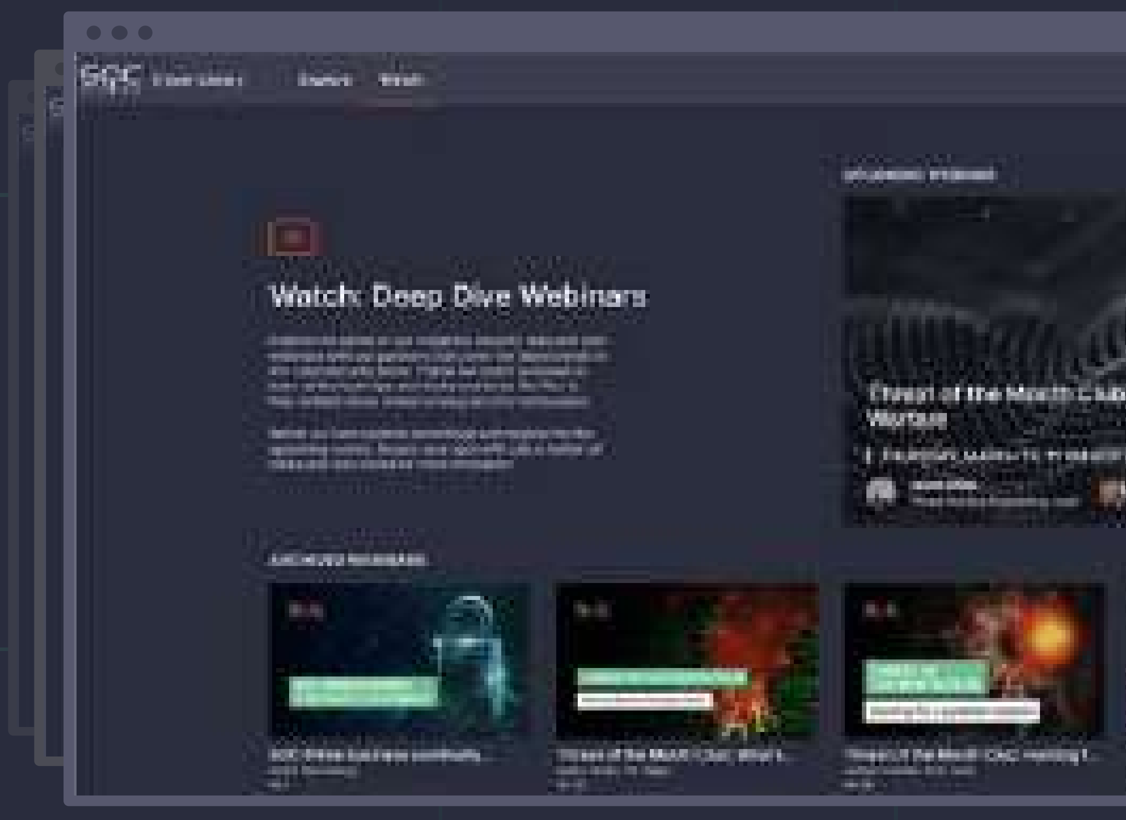
December 2021 Results

KNOWLEDGE SHARING

CYBER LIBRARY

In March 2021, we created a Cyber Library for security enthusiasts designed to simplify threat hunting and threat detection. The library is a rich learning resource for security practitioners to directly access "how-to" guides for SIEM & EDR platforms and view webinar recordings. Registration has been simplified and does not require populating cumbersome sign-up forms.

In 2021, SOC Prime hosted 11 online events, including a series of Security Talks, all of which are now available to watch for Cyber Library users.



Explore Cyber Library

CYBER THREATS SEARCH ENGINE

SOC Prime's Detection as Code platform provides comprehensive threat context, including relevant CTI, MITRE ATT&CK® references, CVE descriptions, autolinks to open exploits, patches, and more metadata.

Browse Cyber Threats Search Engine

Follow us on social media to keep up with the latest SOC Prime news and updates or join our Slack Community to stay always connected with your industry peers:

/socprime

/SOC_Prime

/company/soc-prime/

Join Slack Community via SOC Prime's Platform

Read our Blog to keep abreast of the critical security incidents and defend against the latest threats easier, faster, and more efficiently than ever.

FUTURE OF THREAT DETECTION: COLLABORATIVE CYBER DEFENSE

This may seem obvious, but new and emerging threats succeed because they are undetected. Unfortunately, even equipped with abundant in-house expertise, individual organizations cannot keep pace with the security challenge of matching the speed and scale of cyber attackers. Significant resource investments are required to build, deploy, hunt, and manage threat detection operations. Attack volumes are continuous and accelerating, while lack of visibility into coverage gaps amongst most organizations is extensive. The true cost of effective cyber defense is exceptionally high and growing. What's for certain is that attack volumes will not slow and that most organizations will remain under-resourced.

SOC Prime's Detection as Code platform based on the Sigma standard offers a compelling path forward that immediately raises effectiveness levels of any organization endeavoring to confront cyber attacks by operating a SOC (Security Operations Center). Enabling collective cyber expertise offers a promising path forward for effective and immediate cyber defense. SOC Prime operates the world's largest and most advanced collaborative cyber defense platform and makes it accessible to any security practitioner around the globe. Our capability has given us some unique insights and allows us to make some predictions for the future.

Collaboration

Collaborative cyber defense that produces behavior-based detections enables ultra-fast threat detection and is key to outpacing capable adversaries. Comprehensive CTI and collaborative expertise results in 77% better detection and response capabilities.

Automation

Automating threat hunting tools is critical to success as the pace of attacks requires machine speeds to keep up. This is an important part of a successful future for cyber defense.

Capabilities Becoming Attributes

Threat hunting and detection engineering must become a mainstream capability for organizations to successfully confront an increasingly active cyber adversary. As an example, SOC Prime's Quick Hunt simplifies threat hunting queries and operations.

Tactical Awareness with MITRE ATT&CK®

SOC Prime contributes playbooks and toolkits while continuously tagging detections with the MITRE ATT&CK framework, which simplifies cybersecurity operations. Additionally, the growing community of cybersecurity researchers continuously adds SOC content enabled with ATT&CK tagging to the vast detection library.

Talent Shortages Alleviation

With all of the vast tools and resources enabled by standards like Sigma, organizations can close talent gaps in defensive cybersecurity engineering that historically were only available to those capable of making large resource investments.

Threat Detection Acceleration

Detection data originated by organizations operating cloud-based SIEM, EDR, and XDR solutions will become freely shared across the global cybersecurity community, available 24/7, highly searchable, and updated in real time.

Threat Detection Evolution

Harnessing the collective expertise of a collaborative and highly capable cybersecurity community allows threat detection operations to keep pace with continuous attack volume. Response to emerging threats will become lightning-fast and super-efficient.