DETECTION AS CODE INNOVATION REPORT 2020

THE POWER OF COMMUNITY

Edition #1

www.socprime.com

MESSAGE FROM THE CEO

ANDRII BEZVERKHYI

Founder and CEO at SOC Prime

A founding and acting CEO of SOC Prime with 14+ years of experience in cybersecurity. Andrii is also the architect of Uncoder.io, the common language for threat detection content.

At SOC Prime, we share the responsibility to secure the world by delivering Detection as Code operations to more than 5,000 organizations and the latest threat context to 13,800+ people around the globe. In strong collaboration with our Community, we provide Continuous Security Intelligence globally and help companies to rapidly enable Threat Detection and Response Capabilities using their existing SIEM and XDR stack.

During 2020, we have observed how cybersecurity became essential to remote work and how adversaries shifted the focus of their attacks as a result. Support of our community gives us the power to stand up defense armed with highly trusted, open source Detection as Code content, enabling behavior-based detection of the latest threats, exploits, attack tools, or techniques. This report is a result of the collaboration between the SOC Prime Team, our Threat Bounty Program members, and our worldwide community. By working hand in hand, we can deliver “an unfair advantage” against the attackers, being able to outpace and outsmart the adversaries. Thank you for defending the world together. It is genuinely an honor to work with all of you.

2020 MILESTONES IN NUMBERS

DETECTION RULES

96,363 ▲ 153%

Despite 2020 being a turbulent year, we've managed to follow our commitments and have been fortunate to expand our family with new partners and customers.

Instead of slowing down, we've pushed for new milestones.
Here is our growth in figures:

USERS

13,885 ▲ 93%

ORGANIZATIONS

5,028 ▲ 49%

PLATFORMS

16 ▲ 33%

THREAT BOUNTY CONTENT

33% Of All Content Used By Paid Subscribers

SECURITY TALKS

15 **1,155** People Per Event

EXPLOIT DETECTION

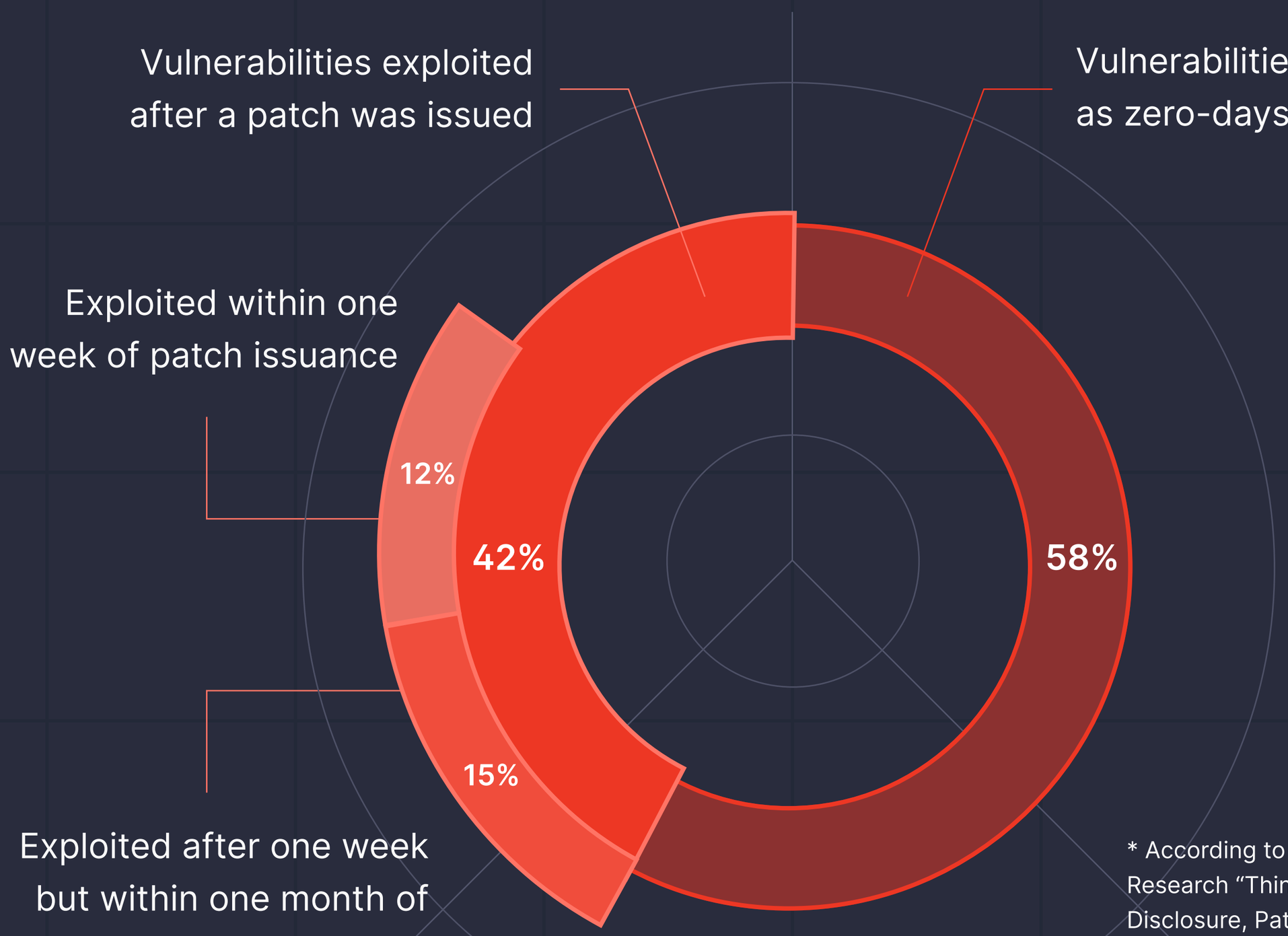
<48 Hours

48 HOURS — EXPLOITATION DETECTION

“FireEye Mandiant Threat Intelligence research into vulnerabilities exploited in 2018 and 2019 suggests that the majority of exploitation in the wild occurs before patch issuance or within a few days of a patch becoming available.” The majority of vulnerabilities are exploited as zero-days before the patch release while 42% are exploited after.

“For these non-zero-day vulnerabilities, there is a very small window (often only hours or a few days) between when the patch is released and the first observed instance of attacker exploitation.”

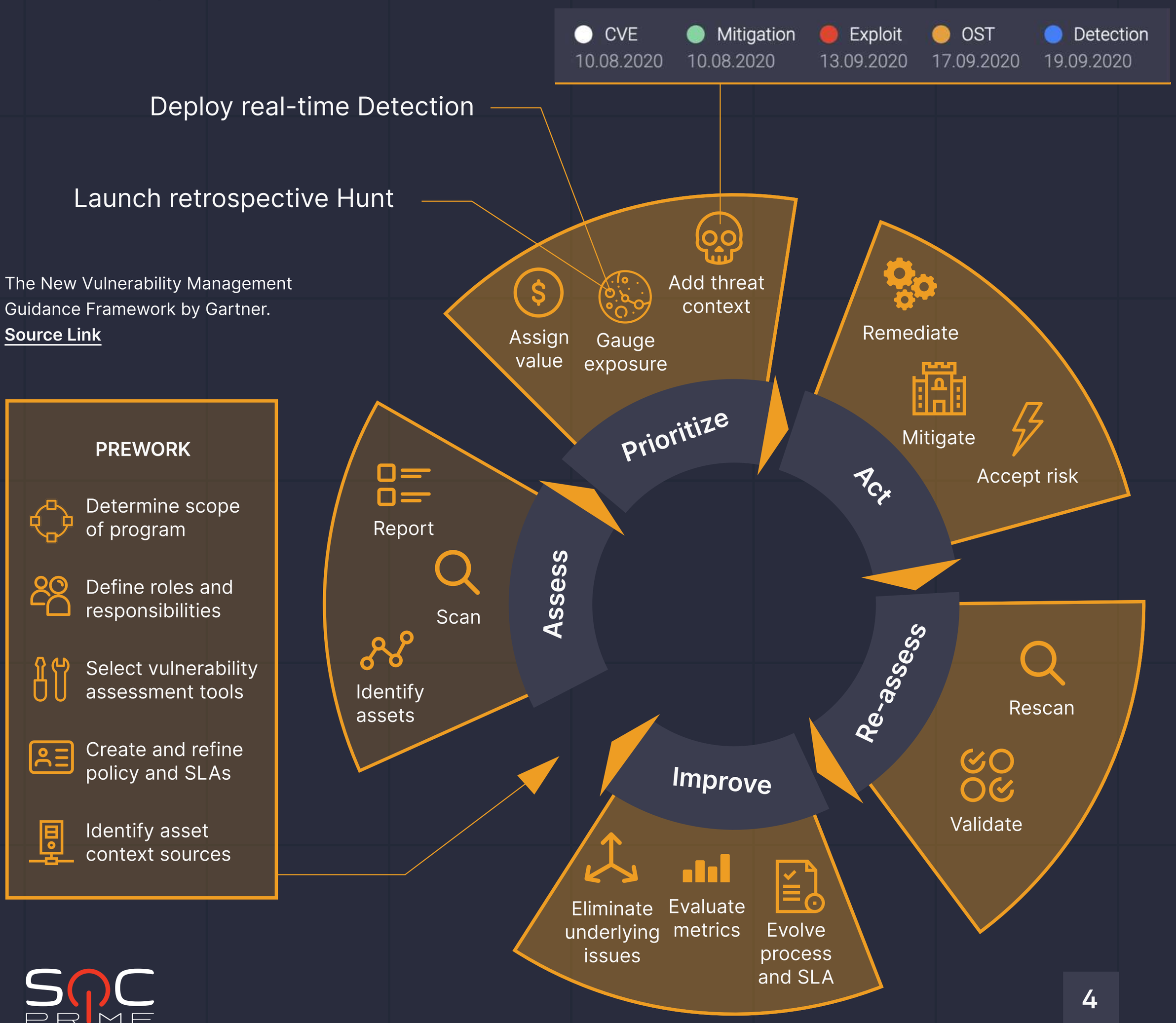
“Such a trend leaves up to 48 hours, in general, to proactively respond to the emerging threat before the avalanche of attacks breaks forth.” - SOC Prime Team



* According to FireEye Threat Research “Think Fast: Time Between Disclosure, Patch Release and Vulnerability Exploitation — Intelligence for Vulnerability Management” - **Source Link**

PROACTIVE VULNERABILITY DETECTION & MANAGEMENT

48 hours is the average time it takes SOC Prime to convert a critical CVE, a public proof-of-concept (PoC) exploit, or an Offensive Security Tool (OST) to Detection. We deliver our detections earlier than the patch release, or within a couple of days after patching, which checks with the “small window” before exploitation in the wild. SOC Prime helps to determine vulnerability priorities and detect the most critical activity. Apart from the detection content itself, we deliver complete threat context. This works well for real-time alerting and enables retrospective hunting. As a result, our customers are aware of the critical security threats and can detect attacks before being aware of the vulnerability.



The New Vulnerability Management Guidance Framework by Gartner.
Source Link

TOP 2020
EXPLOITS & THREATS

2020 saw many businesses increase their reliance on the internet to carry out their daily lives. This, in turn, provided hackers with more opportunities to take advantage of this lifestyle change using malicious activity.

Here are the most critical vulnerabilities of 2020 with public exploits available, followed by major incidents and trends that impacted the cybersecurity landscape last year. The overview is accompanied by SOC Prime's contribution to the proactive defense against these major threats.

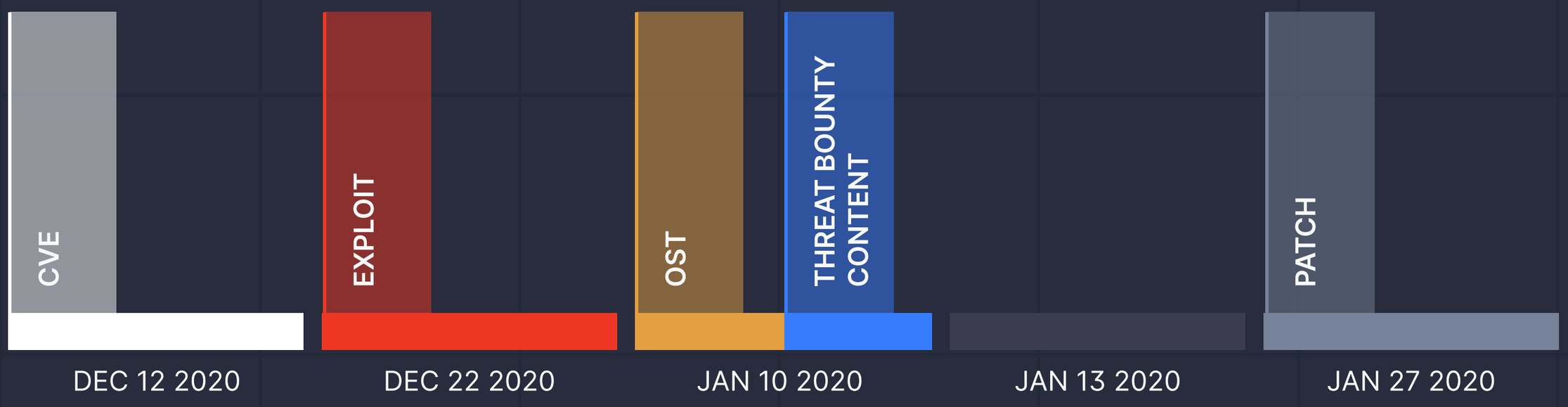
EXPLOITS

CITRIX NETSCALER ADC AND GATEWAY VULNERABILITY (CVE-2019-19781)

A vulnerability in Citrix Netscaler ADC and Gateway exposed an alarming number of networks to cyber-attacks:

- Allows unauthenticated attackers to perform arbitrary code execution on the targeted system
- Endangered lots of law enforcement, healthcare, military, and critical infrastructure institutions
- 80K+ businesses around the globe were found vulnerable

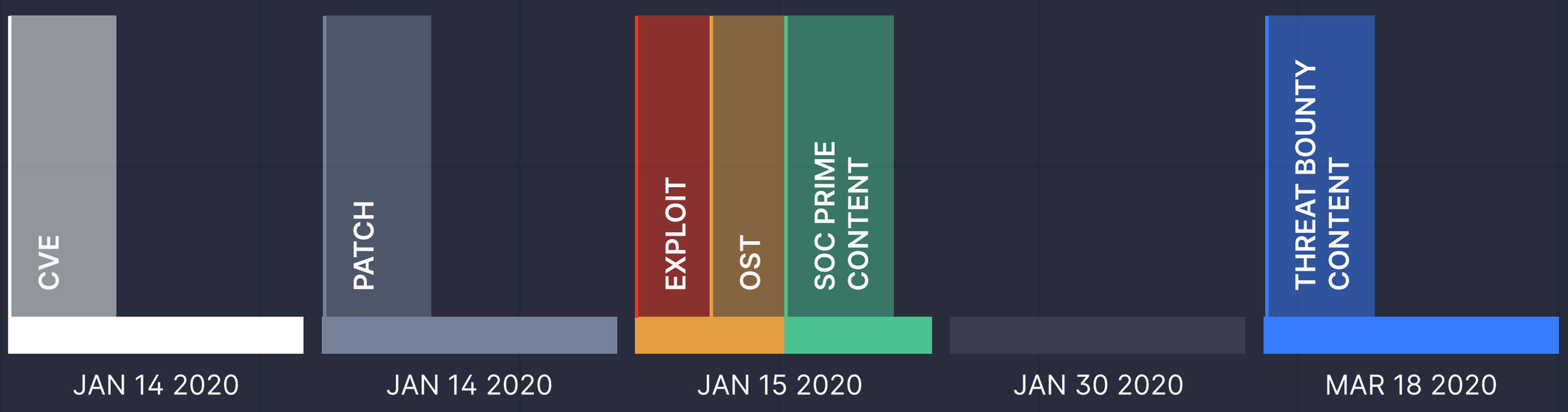
- Threat Bounty developers added detection rules for this CVE to Threat Detection Marketplace on January 10, 2020, which is the same day the OST was published



WINDOWS CRYPTOGRAPHIC VULNERABILITY (CVE-2020-0601)

Windows Crypt API (aka CurveBall) is an extremely dangerous flaw allowing hackers to covertly deliver malware to the targeted instances:

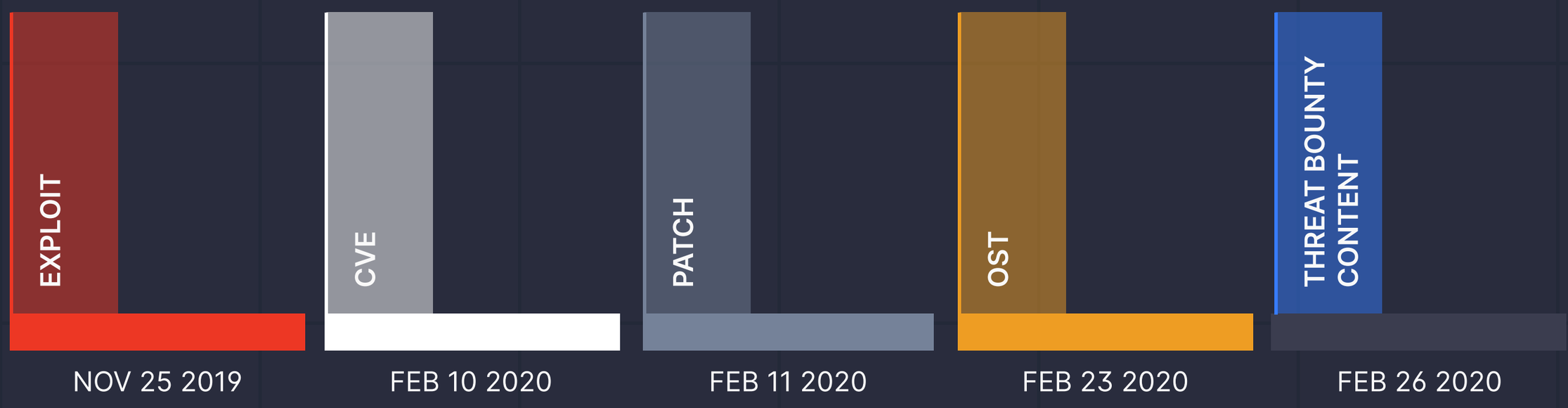
- Stems from the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (EEC) certificates
- Allows threat actors to fool security endpoint products into trusting falsely signed malicious executables
- SOC Prime Team released detections for this CVE on January 15, 2020, which is the day after the PoC exploit and the OST were published



MICROSOFT EXCHANGE SERVER RCE VULNERABILITY (CVE-2020-0688)

A remote code execution (RCE) vulnerability in Microsoft Exchange enables full system compromise:

- Occurs because Microsoft Exchange software fails to properly handle objects in memory
- Allows actors to turn any stolen Exchange user account into the compromise of Exchange environment and Active Directory
- 350K+ Exchange servers identified as vulnerable
- Threat Bounty developers added detection rules for this CVE to Threat Detection Marketplace on February 26, 2020, which is a couple of days after the OST was published



F5 BIG-IP VULNERABILITY (CVE-2020-5902)

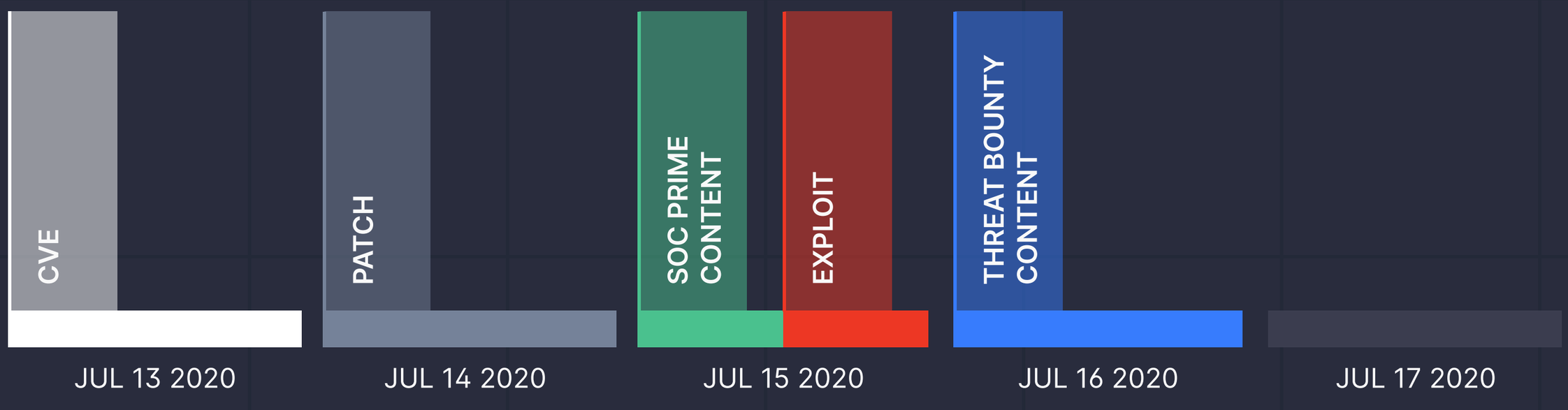
A critical remote code execution vulnerability in F5's BIG-IP networking devices has exposed thousands of businesses to the risk of attack:

- Allows adversaries to read files, execute code, and take complete control over a vulnerable host
- Many government agencies, financial institutions, and internet service providers found themselves exposed to cyber-attacks
- Massively exploited in the wild to install coin-miners, IoT malware, and dump admin credentials
- SOC Prime Team released detections for this CVE on July 4, 2020, which is the same day the PoC exploit and the OST were published

SIGRED VULNERABILITY (CVE-2020-1350)

SIGRed flaw in Microsoft's Domain Name System (DNS) implementation of Windows Server has endangered lots of vendors around the globe:

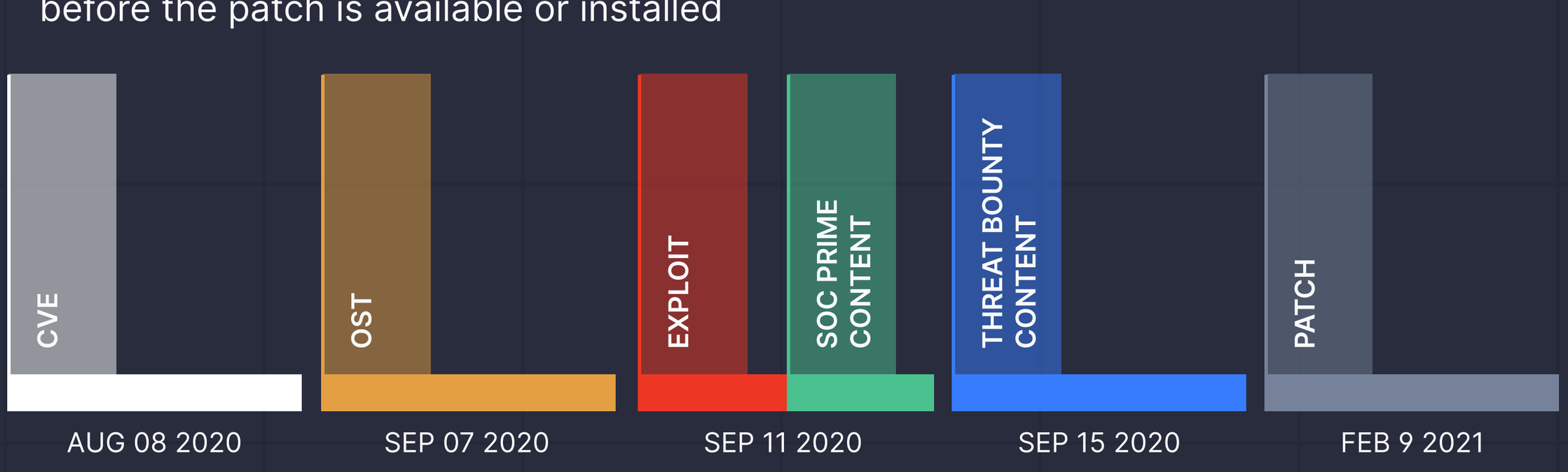
- Allows an unauthenticated attacker to perform remote code executions within the Windows DNS Server
- Tagged as "wormable", meaning that after exploitation the attacker could perform lateral and vertical movements across the targeted network
- Results in full system compromise
- SOC Prime Team released detections for this vulnerability on July 15, 2020, which is the same day the PoC exploit was published



ZEROLOGON VULNERABILITY (CVE-2020-1472)

Zerologon blasted loudly across the cybersecurity landscape in September 2020:

- Stems from a slight cryptographic issue within Windows Netlogon Remote Protocol (MS-NRPC) encryption routine
- Allows threat actors to utilize a zero-length password for gaining admin rights on the root domain controller
- State-sponsored hackers, including MuddyWater APT and APT10, exploited the bug to attack enterprises across the Middle East and Japan
- Fraudsters behind Clop and Ryuk ransomware strains adopted Zerologon vulnerability to increase infections
- Emotet and TrickBot developers utilized Zerologon to expand its malicious perspectives
- SOC Prime Team released detections for this CVE on September 11, 2020, which is the same day the PoC exploit was published
- 300+ organizations downloaded Zerologon detections 24 hours after the media release, while overall downloads show that almost 3,500 companies were interested in the related content. This ultimately indicates that Detection can be done nearly a month before the patch is available or installed



You can explore detection content for these critical vulnerabilities in Threat Detection Marketplace by searching for the CVE ID directly.

View Detections Here

INCIDENTS

COBALT STRIKE SOURCE CODE LEAK

In November 2020, a decompiled source code of the Cobalt Strike 4.0 post-exploitation toolkit was leaked online in a GitHub repository. This incident boosted a trend among cybercriminals in stealing Red Team and penetration testing tools to enhance their malicious capabilities.

- The code has all the dependencies fixed and the license check removed so anyone can compile and customize it on the fly
- The GitHub repository was forked for nearly 200 times, rapidly spreading the code on the web
- The leaked code might be continuously reused and rearranged by hacker groups to gain persistent remote access to the targeted network
- In 2020, the SOC Prime community released a total of 8 rules dedicated to the Cobalt Strike abuse, 7 of which crafted by the Threat Bounty developers

Dedicated Rules
in Threat Detection Marketplace

SOC Prime	Threat Bounty
1	7

View Detections for Cobalt Strike Here

INCIDENTS

SOLARWINDS SUPPLY-CHAIN ATTACK AGAINST FIREEYE AND US AGENCIES

SolarWinds epoch-making supply-chain attack impacted the world-leading security vendors, including FireEye, the US military, and government agencies, as well as 425+ of the US Fortune 500 businesses. In spring 2020, state-sponsored hackers compromised SolarWinds Inc. and trojanized updates to its Orion IT software to push SUNBURST backdoor:

- Dozens of Red Team tools were stolen to be used in malicious operations
- Stealing data on undisclosed exploits might be a new trend among APTs
- SOC Prime Team released 50+ detection rules (IoC-based) within 24 hours after the breach disclosure, with the Author credited to FireEye
- SOC Prime Team proceeds with developing a set of Behavior rules (not IoC-based) that summarize all findings regarding the breach. Major visibility can be gained by analyzing network data and using rules for Zeek/Corelight

Dedicated Rules
in Threat Detection Marketplace

SOC Prime
93

Threat Bounty
27

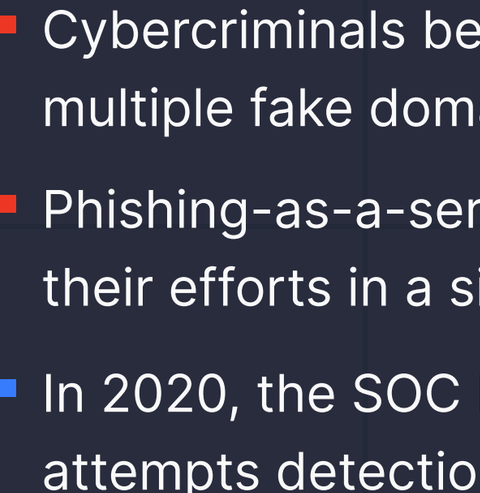
View Detections for FireEye Breach Here

TRENDS

PHISHING

The COVID-19 outbreak caused lots of cybercriminals to switch their lures in order to advance from the major topic of 2020. The trendy news and events surrounding the pandemic make up a core of the phishing messages:

- Threat actors profit from such topics as COVID-19 information, working from home, PPO Loans, stimulus checks, unemployment, Personal Protective Equipment & Medication
- Cybercriminals benefit from the video-conferencing apps “boom” by registering multiple fake domains to trick people into downloading malware
- Phishing-as-a-service (PaaS) is on the rise because hackers attempt to maximize their efforts in a situation of increased victims’ reliance on the Internet
- In 2020, the SOC Prime community released a total of 79 rules aimed at phishing attempts detection, 70 of which crafted by the Threat Bounty developers
- All these rules are either Behavior or generic, which makes attack detection much more effective by saving SIEM resources in comparison to the IoC-based approach



Dedicated Rules
in Threat Detection Marketplace

SOC Prime
9

Threat Bounty
70

View Detections for Phishing Attacks Here

TRENDS

RANSOMWARE

Throughout 2020, ransomware confidently took the leading positions among the threats challenging businesses of all sizes. The number of attacks is continuously growing to pose an even bigger menace in the upcoming years:

- The list of top ransomware samples in the cyber threat arena includes Sodinokibi, Maze, Ryuk, Phobos, and DoppelPaymer
- The top three most popular intrusion methods rely on unsecured RDP endpoints, email phishing, and the exploitation of corporate VPN appliances
- Alongside targeting the private businesses, ransomware actors turn their sights to the public sector with a significant uptick in attacks against healthcare organizations
- Ransomware operators set the new trend of stealing non-compliant victim's data and leaking these details unless the ransom is paid
- In 2020, the SOC Prime community released a total of 139 rules aimed at ransomware attack detection, 127 of which crafted by the Threat Bounty developers

Dedicated Rules
in Threat Detection Marketplace

SOC Prime	Threat Bounty
12	127

View Detections for Ransomware Attacks Here

INNOVATION OF 2020

CLOUDWARDS AND BEYOND

In 2020, we moved cloudwards expanding the detection capabilities with support for the cloud-native language format. Right now we can speak **Microsoft Azure Sentinel, Google Chronicle Security, Sumo Logic, Humio,** and **Elastic Cloud.**

30,000+ cross-platform on-the-fly translations are now available for these cloud-native environments.

In 2020, we expanded SOC Prime Threat Detection Marketplace integrations with the following SIEM, EDR, and NTDR solutions:

Detections tailored to these security solutions can now be seamlessly deployed with a couple of clicks.

Azure Sentinel · Chronicle · sumo logic · humio

kafka · corelight · CROWDSTRIKE · Sysmon

OPEN SOURCE SUPPORT

At SOC Prime, we embrace the values of our community and broaden the support of open source projects yearly.

CONTRIBUTOR RECOGNITION

Being part of the open source community means giving credit to all contributors. Open source Sigma detections that enrich our Detection as Code platform are mainly distributed under the Detection Rule License (DRL). Starting from July 2020, we release all open source detections with a link to the appropriate license to recognize each community content contributor.

ONE MORE HOME FOR SIGMA RULES

In 2020, we released the **Sigma rules repository mirror** powered by Threat Detection Marketplace. This library is in sync with the open source GitHub repository managed by Florian Roth. Now the latest behavior-based detections from the Sigma community are right at hand.

YARA-L: GENUINELY GENERIC

In 2020, we added support for the Google Chronicle Security solution enriching our SOC content library with YARA-L detections written in a new generic language format perfectly tailored to threat detection.

SOC 2 TYPE I

We value transparency when delivering Detection as Code operations to our worldwide community. Last year SOC Prime successfully completed the Service Organization Control (SOC) 2 Type I auditing procedure. SOC 2® compliance is essential for organizations looking for partnerships with SaaS and CaaS product vendors that are transparent in their business practices. Security performers can now feel even safer and more at home in our Threat Detection Marketplace.

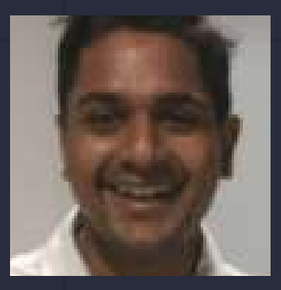
COMMUNITY AND KNOWLEDGE-SHARING

RESEARCHERS	DETECTION RULES	PAID IN BOUNTY
300+ ▲ 84%	1,165 ▲ 213%	$100K ▲ 481%

THREAT BOUNTY PROGRAM

Last year saw impressive growth of our Threat Bounty Program. The number of developers doubled, enriching the Threat Detection Marketplace community with trusted industry experts and experienced threat content developers. Their contribution delivered three times as much content compared to the previous year. To learn more about our developers and the Program itself, check out the interviews below and join our threat hunting community.

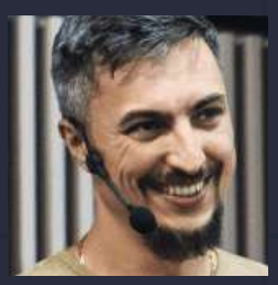
Ariel Millahuel



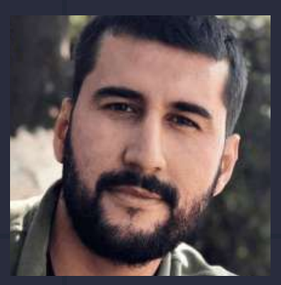
Sreeman Shanker

Osman Demir

Roman Ranskyi

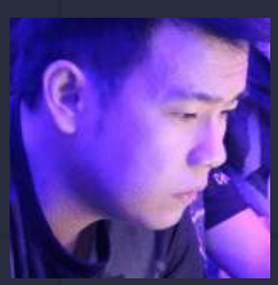


Den Iuzvyk



Emir Erdogan

Kyaw Pyiyt Htet



Sittikorn Sangrattanapitak

Join Threat Bounty Program

DEEP DIVE SECURITY TALKS

During 2020, we have organized a set of online security talks to discuss the latest trends in the cybersecurity arena to boost the exchange of ideas among security practitioners. Follow the links below to check out the top webinars from SOC Prime and our partners.

1

Security Talks with SOC Prime: Adventures in Mapping Things to MITRE ATT&CK ®

A live session devoted to the benefits behind mapping detections to MITRE ATT&CK® and the threats related to common pitfalls.

- Adam Swan, Senior Threat Hunting Engineer at SOC Prime
- Nate Guagenti, Solutions Architect at SOC Prime

2

Handle Zoom Bombings, Malware Spreading, COVID-19 Phishing & God Knows What Else

A dedicated session on Zoom hardening, logging and policy tips implemented by SOC Prime, and Pi-Hole deployment for securing your home DNS traffic from malware and ads.

- Andrii Bezverkhyi, CEO at SOC Prime
- Vladimir Garaschenko, CISO at SOC Prime

3

Using Sigma to Accelerate your SIEM Transformation to Azure Sentinel

A co-hosted session by Microsoft and SOC Prime where we talk about the optimization of security operations with an integrated, all-encompassing, and intelligent SIEM platform.

- Andrii Bezverkhyi, CEO at SOC Prime
- Ofer Shezaf, Principal Program Manager at Microsoft

4

Humio & SOC Prime Live Workshop: Identify Cybersecurity Threats in Real Time

A joint live workshop with Humio about SOC Prime's integration with Humio's live streaming and scalable log management platform. This innovation enables real-time visibility into distributed systems to provide fast and precise answers to critical security questions.

- Jordan Camba, Technical Account Manager at SOC Prime
- Richard Patrick, Solution Architect at Humio

CLOSER TO COMMUNITY

In 2020, we launched a dedicated Slack space to facilitate live discussions amongst our community of SOC Analysts, SIEM Administrators, DevOps, Threat Hunters, Detection Engineers, and any InfoSec practitioners involved.

We believe that chats for bug reporting and here-and-now talks will support security enthusiasts in their battle against existing challenges.

tdm-community.slack.com

Follow us on social media to keep up with the latest SOC Prime news, updates, and discussions:

/socprime | **/SOC_Prime** | **/company/soc-prime/**

Stay tuned to our **YouTube channel** to watch recordings of the insightful security talks and upskilling online events.

Read our **Blog** to keep abreast of the critical security incidents and find the latest detections.