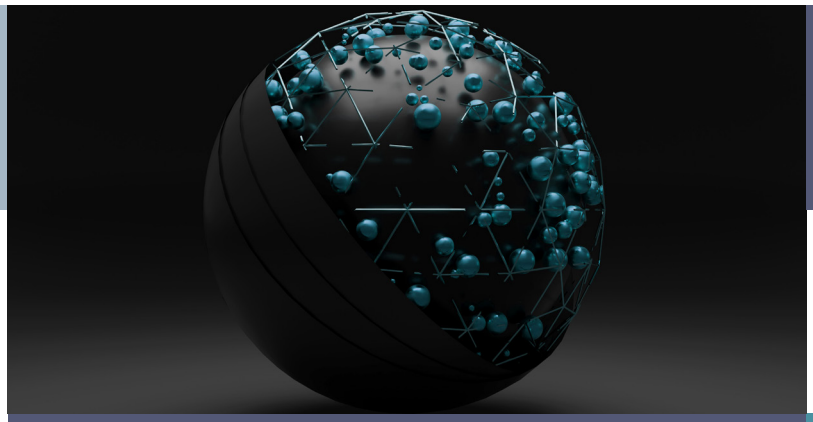
LOGPOINT



Logpoint Global Services

Emerging Threats Protection Report

This report is the outcome of Logpoint's Security Research team and Global Services, as part of our Emerging Threat Protection service to provide Logpoint's customers with up-to-date detection rules, Investigation and Response playbooks, and security best practices.

Emerging Threats Protection: Russia-Ukraine Cyber Operations

In this report, we have researched the detected new round of offensive and destructive cyberattacks directed against Ukraine's digital infrastructure and its alliances. The analysis includes the main two attack vectors detected, Phishing, and Wiper malware. Following the analysis, this report covers detection methods, investigation Playbooks, and recommended response and best practices.

All new detection rules are available as part of Logpoint's new release, as well as through Logpoint's download center. Customized Investigation and Response playbooks were pushed to Logpoint ETP customers.

The report below goes through the incident, potential threats, and how to detect any potential attacks and proactively defend using Logpoint's SIEM and SOAR capabilities.

What We Know So Far

Threat Actors

Primary

DEV-0665 (Deployed wiper in Jan 2022)

DEV-0586 (Deployed wiper in Feb 2022)

GhostWriter (Targeted phishing campaign)

Secondary

Threat Actor	Gamaredon
Aliases	ACTINIUM, BlueAlpha, Shuckworm, Primitive Bear
Target	Ukrainian government
Activity	From 2013 onwards

Timeline:

January 11, 2022: FBI, CISA, and the NSA warn critical infrastructures of a potential cyberattack from Russia as tension rises in West Europe.

February 18, 2022: Officials claim the United States has evidence of ongoing massive denial of service and SMS spam campaigns in Ukraine originating in Russia. *Source:* SC Media.

February 23, 2022: Wiper Malware: New wiper malware; named Hermetic Wiper, started targeting Ukrainian enterprises, according to ESET Research. Malware artifacts suggest that the attacks had been planned for several months. *Source:* SC Media.

February 24, 2022:

- The government of Ukraine started asking underground hacker groups to defend its IT systems and find vulnerabilities in the Russian systems. *Source:* Reuters.
- The websites of the Russian president, government, and State Duma lower house of parliament get targeted with DDoS attacks.
- A second destructive attack against a Ukrainian governmental network started, using a wiper named IsaacWiper.

A descriptive explanation of each event and malware is accessible through our friends at welivesecurity.

February 25, 2022:

- Phishing Attacks Allegedly Target Ukrainian Personnel. Hackers from Belarus have launched phishing emails against Ukrainian military personnel. *Source:* Ukraine Computer Emergency Response Team (CERT).

February 26, 2022:

- Kremlin Website Offline. The official website of the Kremlin, the office of Russian President Vladimir Putin, was down, following reports of denial of service (DDoS) attacks on various other Russian government and state media websites. *Source:* Reuters.
- Some Russian Banks Removed From SWIFT.
- CISA Alert: A CISA alert warned that threat actors have deployed malware such as WhisperGate and HermeticWiper was being used against organizations in Ukraine. *Source:* CISA.

March 1, 2022:

- Potential Cyberattacks vs. Russia Infrastructure: A Ukrainian cyber guerrilla warfare group plans to launch digital sabotage attacks against critical Russian infrastructure such as railways and the electricity grid. *Source:* Reuters.

Types of Attacks

1. Phishing Campaigns

On February 25, CERT-UA reported that the Minsk-based group UNC1151 (GhostWriter) was responsible for phishing attacks against Ukrainian soldiers. They are notorious for their past activities including promoting anti-NATO material via misinformation networks, website hijacking, spoofing, and targeting Belarusian media outlets and individuals ahead of the 2020 election. It has been suspected that the GhostWriter's members are officers of the Ministry of Defense of the Republic of Belarus. Since then many of the sites have been taken down, but several are still active and new ones keep popping up here and there.

For this, a comprehensive list has been created by Logpoint for detections.

Detection using Logpoint

We have added the following alert rule to the latest release, which is triggered whenever any Belarusian threat actor GhostWriter (UNC1151) IoC domains or IP Address match is found (T1566). IoC Reference: IoCs are latest up to Feb 2022.

```
(domain IN GHOSTWRITER_DOMAINS OR source_address IN GHOSTWRITER_IPS OR destination_
address IN GHOSTWRITER_IPS)
```

2. Wiper Malware

Disk wipers are one particular type of malware often used against Ukraine. The implementation and quality of those wipers vary and may suggest different hired developers. Though no link has been found between the two, it is believed that IssacWiper is targetting and affecting computers missed by HermeticWiper.

The day before the invasion of Ukraine by Russian forces on February 24, a new data wiper was found to be unleashed against several Ukrainian entities. This malware was given the name "HermeticWiper" based on a stolen digital certificate from a company called Hermetica Digital Ltd.

This wiper is remarkable for its ability to bypass Windows security features and gain write access to many low-level data structures on the disk. In addition, the attackers wanted to fragment files on a disk and overwrite them to make recovery impossible.

As we were analyzing this data wiper, other research has come out detailing additional components that were used in this campaign, including a worm and typical ransomware thankfully poorly implemented and decryptable.

In tracking this threat, early reports show that the malware has been deployed against a financial institution in Ukraine as well as two contractors in Latvia and Lithuania that provide services to the Ukrainian Government. Additionally, ESET researchers have warned that they found this malware installed across "hundreds of machines" in Ukraine.

However not as sophisticated as its predecessor, IssacWiper has a similar work pattern with a varying technique.

Detection using Logpoint

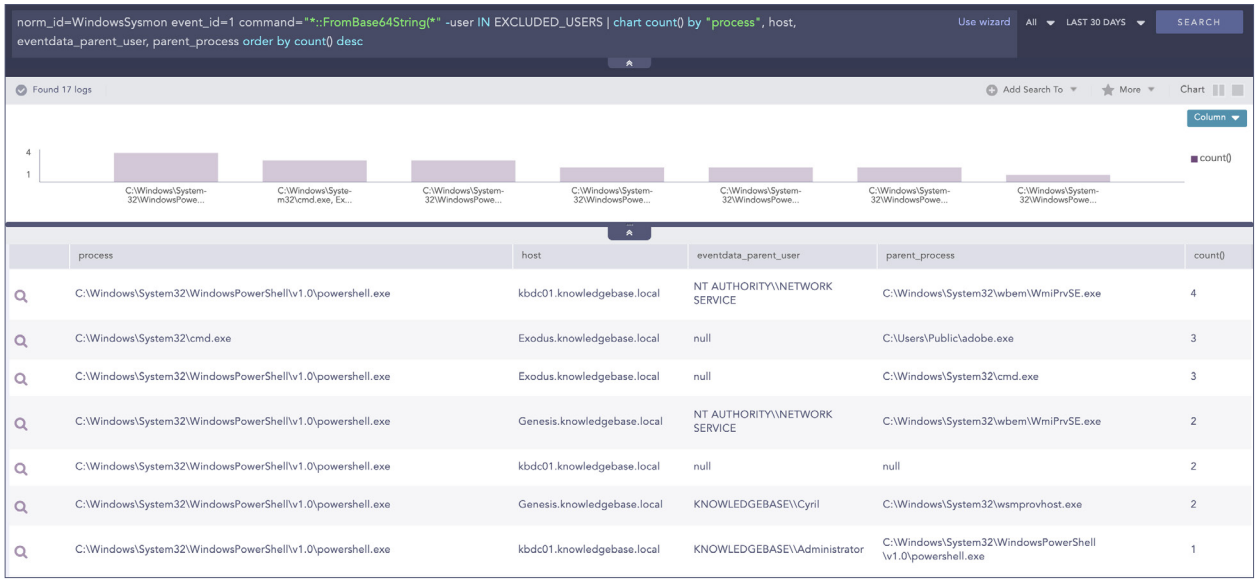
Upon execution, a process that runs administrative privileges in the background downloads the next-stage malware hosted on a Discord channel, with help of PowerShell and the download link hardcoded in the downloader.

An alert(T1059.001) has been created that can detect if PowerShell is being used as a download cradle which can be detected using process creation logs.

```
norm_id=WindowsSysmon event_id=1 image="*\powershell.exe" command IN ["*new-
object system.net.webclient).downloadstring(*", "*new-object system.net.webclient).
downloadfile(*", "*new-object net.webclient).downloadstring(*", "*new-object net.
webclient).downloadfile(*"] -user IN EXCLUDED_USERS
```

In the hermetic wiper malware, payloads are encoded using base64. The alert(T1059.001, T1059.003, T1140) below checks if any payload has been passed into PowerShell encoded as a base64 string.

```
norm_id=WindowsSysmon event_id=1 command="*::FromBase64String(*" -user IN EXCLUDED_
USERS
```



In one case, adversaries exploited a known vulnerability (CVE-2021-1636) in the Microsoft SQL server to gain access to the target organization. We can detect(T1590, T1059.001) these types of exploitation by looking for spawning of shell processes by the SQL server process.

```
norm_id=WinServer event_id=4688 parent_process="*\sqlservr.exe" "process" IN ["*\cmd.
exe", "*\powershell.exe", "*\bash.exe", "*\sh.exe", "*\bitsadmin.exe"]
```

In general, we can hunt for possible malicious PowerShell activity(T1059, T1059.001) by checking if its parent process belongs to a list of suspicious processes such as mshta.exe, winword.exe, etc.

```
norm_id=WinServer event_id=4688 parent_process IN ["*\mshta.exe", "*\rundll32.exe",
"*\regsvr32.exe", "*\services.exe", "*\winword.exe", "*\wmiprvse.exe", "*\powerpnt.
exe", "*\excel.exe", "*\msaccess.exe", "*\mspub.exe", "*\visio.exe", "*\outlook.exe",
"*\amigo.exe", "*\chrome.exe", "*\firefox.exe", "*\iexplore.exe", "*\microsoftedgecp.
exe", "*\microsoftedge.exe", "*\browser.exe", "*\vivaldi.exe", "*\safari.exe", "*\
sqlagent.exe", "*\sqlserver.exe", "*\sqlservr.exe", "*\w3wp.exe", "*\httpd.exe", "*\
nginx.exe", "*\php-cgi.exe", "*\jbosssvc.exe", "*MicrosoftEdgeSH.exe", "*tomcat*"]
(command IN ["*powershell*", "*pwsh*"] OR description="Windows PowerShell")
```

Next, administrators should lookout for credential dumping via comsvcs DLL(T1003).

```
norm_id=WindowsSysmon event_id=1 (image="*\rundll32.exe" OR file="RUNDLL32.EXE")
command IN ["*comsvcs*MiniDump*full*", "*comsvcs*MiniDumpW*full*"] -user IN EXCLUDED_
USERS
```

Adversaries can also call DLL's exported functions via ordinal(T1218, T1218.011) instead of specifying the function name.

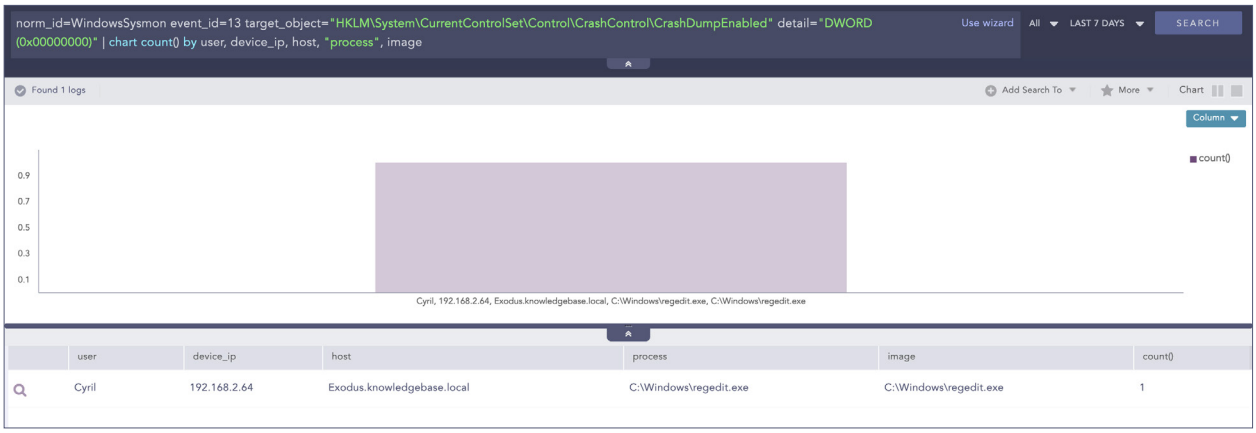
```
norm_id=WinServer event_id=4688 "process"="*\rundll32.exe" command IN ["*,#*", "*,
#*", "*.dll #*", "*.ocx #"] -command IN ["*EDGEHTML.DLL*", "*#141*"] -user IN
EXCLUDED_USERS
```

Impacket is a popular tool that adversaries use for lateral movement. Impacket leaves artifacts in process creation events which is trivial to detect(T1559, T1559.001, T1047, T1021, T1021.003).

```
norm_id=WindowsSysmon event_id=1 ((parent_image IN [“*\wmiprvse.exe”, “*\mmc.exe”, “*\explorer.exe”, “*\services.exe”] command IN [“*cmd.exe* /Q /c * \\127.0.0.1\*&1*”]) OR (parent_command IN [“*svchost.exe -k netsvcs”, “taskeng.exe*”] command IN [“cmd.exe /C *Windows\Temp\*&1”])) -user IN EXCLUDED_USERS
```

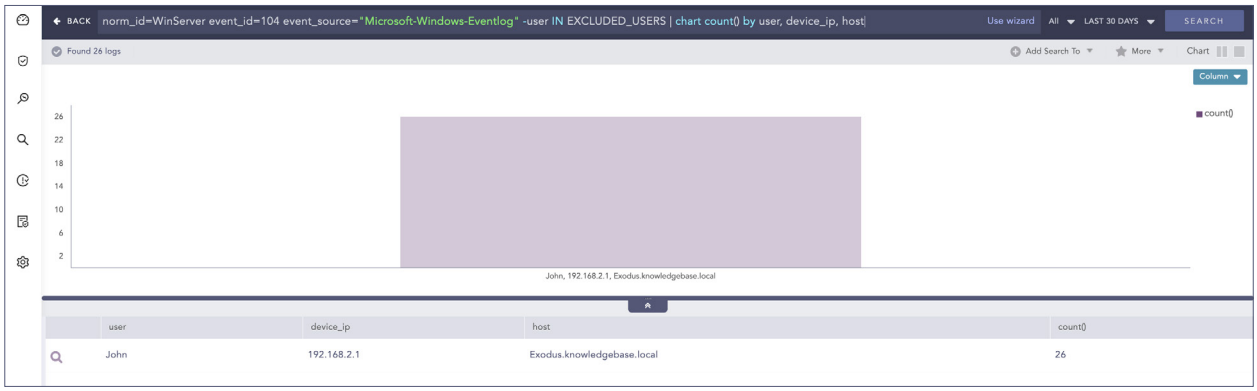
To make recovery difficult, HermeticWiper will disable Windows's crash dump feature which administrators can detect using Sysmon's registry events (T1112).

```
norm_id=WindowsSysmon event_id=13 target_object=”HKLM\System\CurrentControlSet\Control\CrashControl\CrashDumpEnabled” detail=”DWORD (0x00000000)”
```



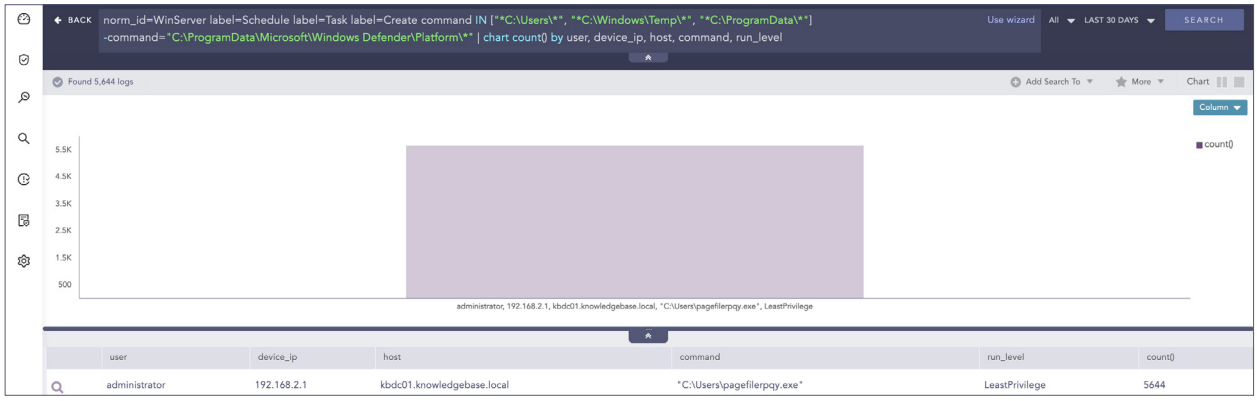
For clearing tracks, adversaries may clear event some log channels(T1070.001).

```
norm_id=WinServer event_id=104 event_source=”Microsoft-Windows-Eventlog” -user IN EXCLUDED_USERS
```



Threat actors targeting Ukraine commonly use scheduled tasks for persistence. Administrators should hunt for suspicious scheduled task creations and to keep in mind that they require proper whitelisting to reduce false positives (T1053.005).

```
norm_id=WinServer label=Schedule label=Task label=Create command IN [“*C:\Users\*”, “*C:\Windows\Temp\*”, “*C:\ProgramData\*”] -command=”C:\ProgramData\Microsoft\Windows Defender\Platform\*”
```



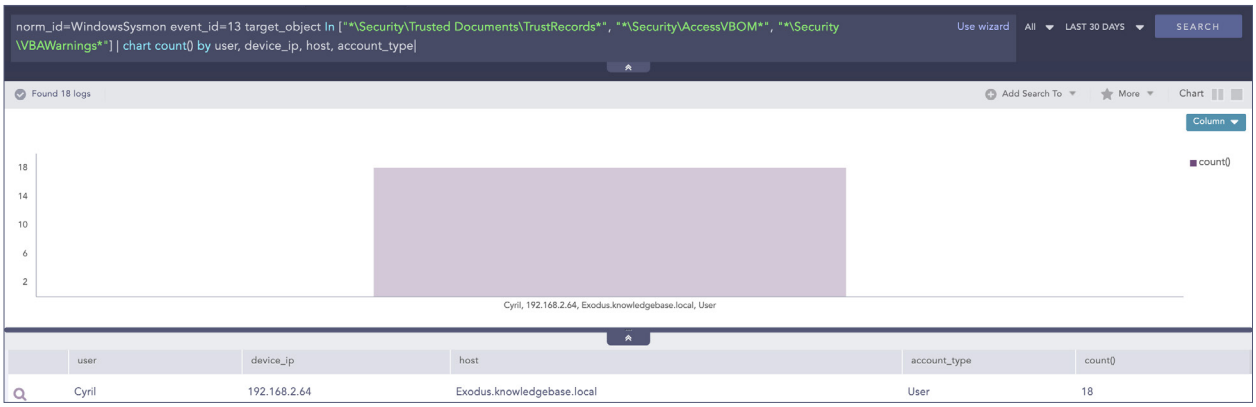
Gamaredon is known to use UltraVNC via command line for remote access to the victim network. Administrators should look out for the usage of remote access tools that have no business use in their environment(T1219).

```
norm_id=WinServer event_id=4688 command=”*-autoreconnect *” command=”*-connect *” command=”*-id:*”
```

Actinium is known to change Office’s macro and VBA execution security settings which administrators can detect using Sysmon’s registry events(T1112).

```
norm_id=WindowsSysmon event_id=13 target_object In [“*\Security\Trusted Documents\TrustRecords*”, “*\Security\AccessVBOM*”, “*\Security\VBAWarnings*”]
```

We released several IoC alerts in Alert Rules v5.3.6 for detecting malware such as HermeticWiper and threat actors such as Actinium.



HERMETIC_WIPER_HASHES list contains the IoC hashes of the Hermetic malware family compiled from security reports of Symantec, ESET, etc (T1588.001).

```
(hash IN HERMETIC_WIPER_HASHES OR hash_sha1 IN HERMETIC_WIPER_HASHES OR hash_sha256 IN HERMETIC_WIPER_HASHES)
```

Administrators can monitor for hashes of loaded drivers to detect matches on IoC hashes present on HERMETIC_WIPER_DRIVER_HASHES (T1588.001).

```
norm_id=WindowsSysmon event_id=6 (hash IN HERMETIC_WIPER_DRIVER_HASHES OR hash_sha1 IN HERMETIC_WIPER_DRIVER_HASHES OR hash_sha256 IN HERMETIC_WIPER_DRIVER_HASHES)
```

Similarly, the ISAAC_WIPER_HASHES list contains the IoC hashes of IsaacWiper (T1588.001).

```
(hash IN ISAAC_WIPER_HASHES OR hash_sha1 IN ISAAC_WIPER_HASHES OR hash_sha256 IN ISAAC_WIPER_HASHES)
```

ACTINIUM_HASHES and ACTINIUM_DOMAINS lists contain the IoC hashes and domains related to Actinium compiled from the MSTIC report (T1588.001).

```
(hash IN ACTINIUM_HASHES OR hash_sha1 IN ACTINIUM_HASHES OR hash_sha256 IN ACTINIUM_HASHES)
```

And for the domains (T1566)

```
domain IN ACTINIUM_
DOMAINS
```

WHISPERGATE_HASHES list contains the IoC hashes of WhisperGate malware (T1588.001).

```
(hash IN WHISPERGATE_HASHES OR hash_sha1 IN WHISPERGATE_HASHES OR hash_sha256 IN WHISPERGATE_HASHES)
```

The given alerts are available in the latest release and can be manually downloaded through the given link.

Alerts download.

Log source requirements

To make proper use of the detection techniques, Logpoint requires the following sources.

- Windows Sysmon
- Windows Native Auditing
- Firewall

Other than the two mentioned attack types that will be focused on prominently, the other types of attacks plaguing Ukraine include:

3. DDoS

While DDoS does not receive the same level of attention as some other forms of attack, it can still have significant impacts on business operations. Though the back and forth DDoS attacks between the two neighbors have been going on for ages, Russia launched a series of distributed denial of service (DDoS) attacks against Ukrainian websites early this February. The attacks focused on civilian impacting business and services including the Ukrainian banking and defense websites and were reportedly launched by the Russian military intelligence agency, GRU. The attacks came as tensions heightened between Ukraine and Russia. Ever since Ukraine requested the help of the cyber community, the attacks have been going back and forth.

Russia has continued to launch DDoS attacks intermittently, and, in the first week of March, Russian groups were found using DanaBot, a malware-as-a-service platform, to launch DDoS attacks against Ukrainian defense ministry websites. It is unclear who these groups are and whether they are connected to the Russian government.

4. Website defacement

Ukraine has also been experiencing website defacements, which provide attackers with an opportunity to spread messages. Website defacement is typically associated with hacktivist activity, but state-sponsored Russian actors could pose as hacktivists to disguise Russian state involvement and spread their strategic communication themes to international audiences by defacing Western websites. Since the hacktivist group, Anonymous, declared Russia as its target, Russian military sites have also been targets of defacement since then.

Incident Investigation using Logpoint SOAR

Post-compromise investigation

The necessary steps in investigating post-compromise activity include inspecting:

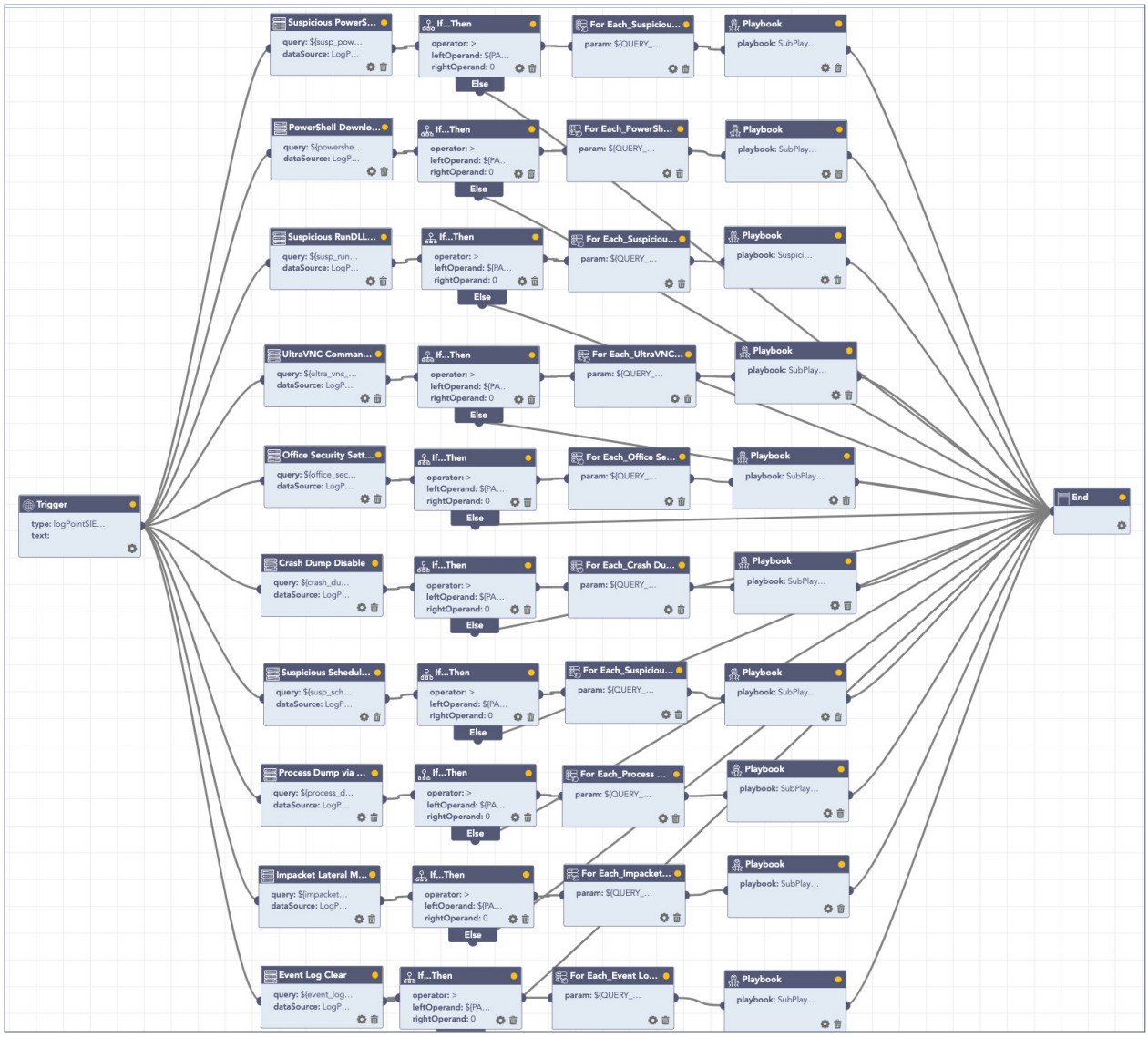
- If any accounts have been compromised, passwords are changed, or are receiving unusual logins, emails, or requests from any users.
- Any traffic has been found between the compromised domains.
- Unusual files that have been downloaded using PowerShell.
- Commands that have used generic evasion techniques like base64 encoding.
- Known vulnerabilities being exploited, including but not limited to, CVE-2021-1636.
- Processes being attributed to suspicious parent processes.
- Credential dumping attempts.
- Impacket use or attempts of use.
- Disabling of important features including but not limited to crash dump feature.
- Logs are being cleared.
- Suspicious scheduled tasks are being created.
- Unusual Remote Access Tools (RATs) making connections.
- Security settings are being changed rapidly.

In no way would monitoring for the listed activities eliminate the chance of being compromised, but would provide basic coverage of any attempt when added to existing company cybersecurity policies.

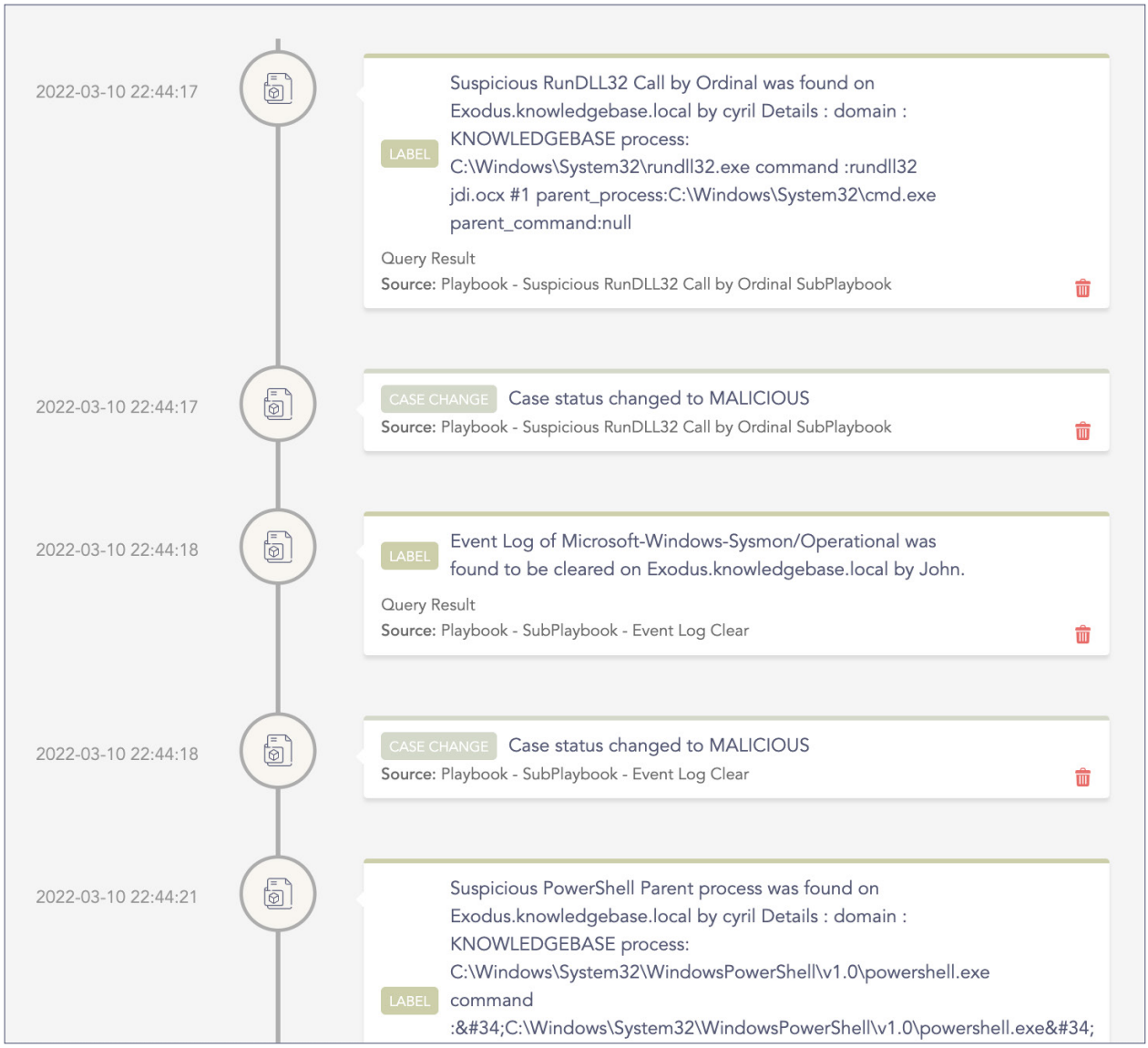
In lieu of the recent events, time is of the essence to make sure all the issues are prevented before any serious harm has occurred. We have created a few playbooks to automate the detection and response process.

These playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail each step for both incident and vulnerability detection.

The main playbook for investigation, with its multiple subplaybooks, goes deep into detection and investigation if an attack has taken place.



After executing the playbook in Logpoint SOAR, we can view the cases created by the playbook's components in the investigation timeline to get a high-level overview of the investigation's results.



The dependencies for this playbook include:

Sub-playbooks

- Suspicious RunDLL32 Call by Ordinal SubPlaybook
- SubPlaybook - Event Log Clear

Integrations

- Endpoint Detection and Response tools.
- Antivirus
- Threat Intelligence

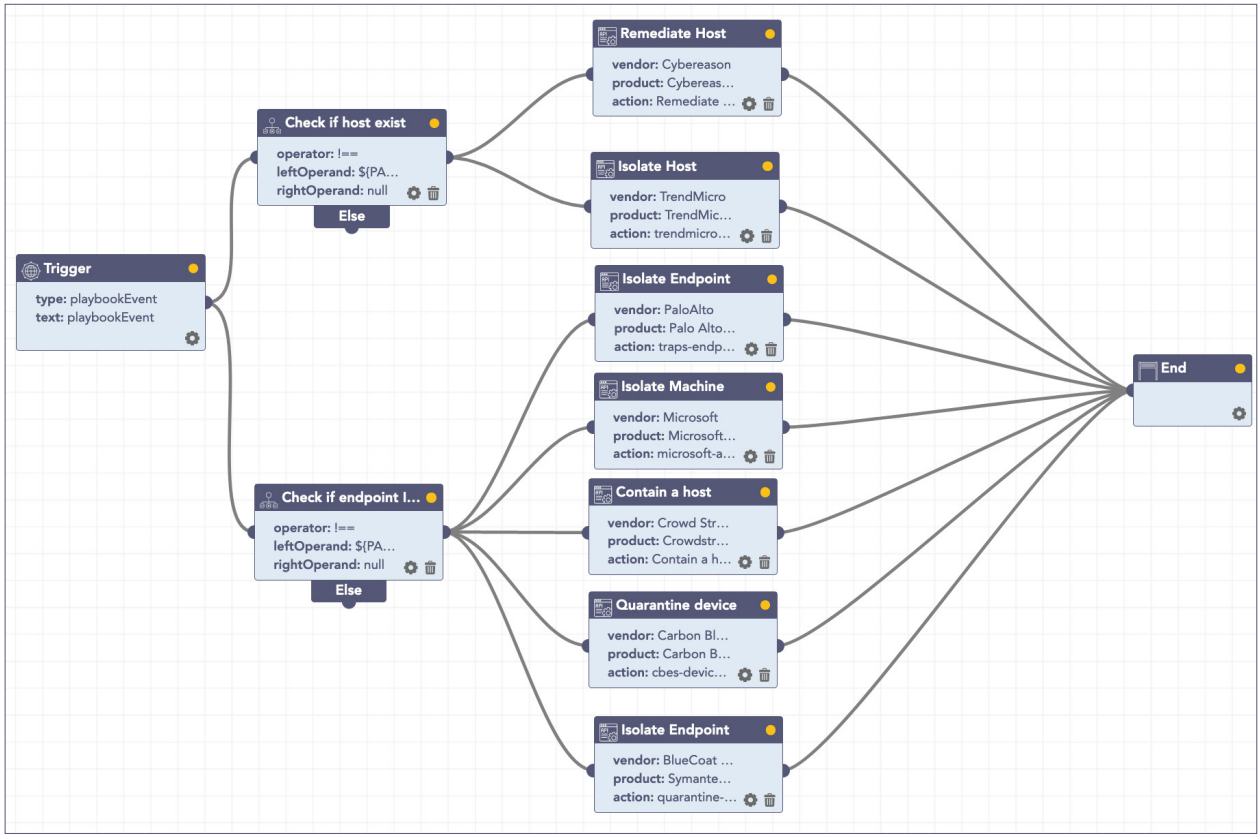
Incident Response

If and when an active attack has been detected, an organization should always follow the already set IT and Security guidelines. Plenty of resources is available to create and follow. Some notable ones are provided by CISA, FBI, and frameworks by NIST.

However, using Logpoint Technology, the following actions can be taken for immediate responses to the attacks.

These solutions come out of the box as playbooks that can be deployed with the latest release.

1. **Blocking IoCs:** We have updated our IoC lists with hashes, domains, and IPs, which can be turned on as alerts and used to block as soon as they are detected in the network.
2. **Isolate the endpoints:** When an attack is detected or a system is compromised, the immediate action should be to isolate the system, take proper logs, evaluate the situation and remediate.



A. Isolate Endpoint Mitigation – Generic

The playbook checks if a host has been infected. If the result is true, the playbook tries to isolate it using the EDR, contain and quarantine it before it spreads into other machines.

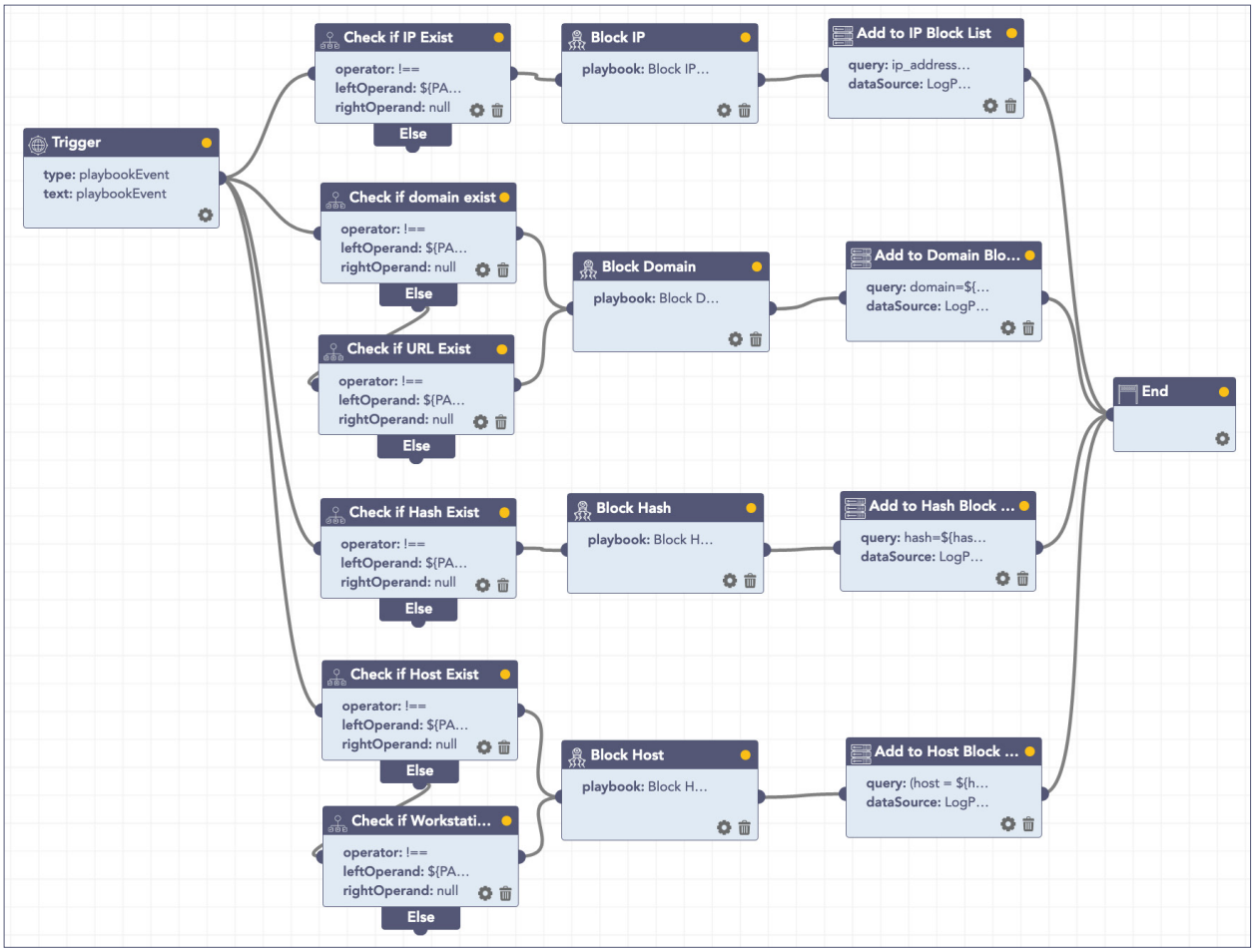
The dependencies for this playbook include:

Integrations

Endpoint Detection and Response tools.

Antivirus

Threat Intelligence



B. Block Indicators – Generic

This playbook is a do-all blocker. It checks if any IP, domain, URL, or host exists in a list of indicators of compromise, blocks them, and adds them to the blocked list.

The dependencies for this playbook include:

Integrations

Firewall / WAF

Endpoint Detection and Response tools.

Antivirus

Threat Intelligence

Along with the given playbooks, the organizations detecting potential APT activity in their IT or OT networks should:

1. Secure backups. Ensure your backup data is offline and secure. If possible, scan your backup data with an antivirus program to ensure it is free of malware.
2. Collect and review relevant logs, data, and artifacts.
3. Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.

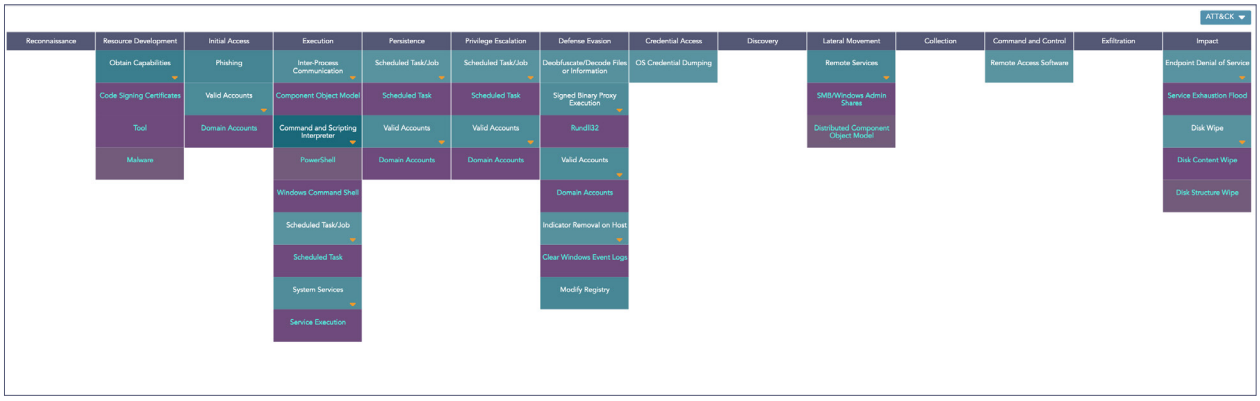
Note: It is crucial that for the OT assets, any organization should have a resilience plan that addresses how to operate if you lose access to – or control of – the IT and/or OT environment.

Security Best Practices

- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.
- Use Endpoint Detection (EDR) tools with proper restrictive policies to avoid leakage of data and MBR/VBR modifications.
- Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single-factor authentication, to confirm the authenticity and investigate any anomalous activity.
- Create active monitoring and incident response plans by using tools like Logpoint SIEM and SOAR.
- Enable multifactor authentication (MFA) to mitigate potentially compromised credentials and ensure that MFA is enforced for all remote connectivity. Use passwordless authenticator tools for an extra level of security.
- Make sure all the systems are actively patched and signatures are up to date for all endpoints, security products, and software products.

Summary

Of the two active attacks happening on the Ukrainian Cyberspace(Phishing and Wiper Malware), the MITRE mapping of the attacks in Logpoint ATT&CK is as follows.



MITRE ATT&CK techniques

This table was built using **version 10** of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1588.002	Obtain Capabilities: Tool	Attackers used RemCom and potentially Impacket as part of their campaign.
	T1588.003	Obtain Capabilities: Code Signing Certificates	Attackers acquired a code-signing certificate for their campaigns.
Initial Access	T1078.002	Valid Accounts: Domain Accounts	Attackers were able to deploy wiper malware through GPO.
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	Attackers used the command line during their attack (e.g., possible Impacket usage).
	T1106	Native API	Attackers used native APIs in their malware.
	T1569.002	System Services: Service Execution	HermeticWiper uses a driver, loaded as a service, to corrupt data.
	T1047	Windows Management Instrumentation	HermeticWizard attempts to spread to local computers using WMI.
Discovery	T1018	Remote System Discovery	HermeticWizard scans local IP ranges to find local machines.
Lateral Movement	T1021.002	Remote Services: SMB/ Windows Admin Shares	HermeticWizard attempts to spread to local computers using SMB.
	T1021.003	Remote Services: Distributed Component Object Model	HermeticWizard attempts to spread to local computers using WbemLocator to remotely start a new process via WMI.
Impact	T1561.002	Disk Wipe: Disk Structure Wipe	HermeticWiper corrupts data in the system's MBR and MFT.
	T1561.001	Disk Wipe: Disk Content Wipe	HermeticWiper corrupts files in Windows, Program Files, Program Files(x86), PerfLogs, Boot, System Volume Information, and AppData.
	T1485	Data Destruction	HermeticWiper corrupts user data found on the system.
	T1499.002	Endpoint Denial of Service: Service Exhaustion Flood	By using DDoS attacks, the attackers made several government websites unavailable.

About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats. Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more. Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company. For more information, visit www.logpoint.com

Contact Logpoint

If you have any questions or want to learn more about Logpoint and our next-gen SIEM solution, don't hesitate to contact us at www.logpoint.com/en/contact/

TRUSTED BY MORE THAN 1,000 ENTERPRISES

KONICA MINOLTA CAPTIVATE BOEING GoSecure RÉMY COINTREAU

AWARDS AND HONORS

Gartner peerinsights customers' choice 2021

Gartner Peer Insights

Gartner

Gartner Magic Quadrant

Software Reviews GOLD MEDAL 2021 SECURITY INCIDENT AND EVENT MANAGEMENT

SoftwareReviews Data Quadrant

For more information, visit logpoint.com
Email: sales@logpoint.com

LOGPOINT