OPSWAT.

# OPSWAT Monthly Executive Report

## OPSWAT SOC Services for {Customer Name}

Prepared by: OPSWAT Inc.

| | |
|---|---|
| Client Name | {Company Name} |
| Client Technical Contact(s) | {Contact Name} |
| Client Managerial Contact(s) | {Contact Email Address} |
| Project Name | Monthly Executive Report |
| Document Date | 2024/05/01 |
| Document Version | 1.0.0 |

OPSWAT.

# Contents

OPSWAT.

# 1. Executive Summary

## 1.1 Key Points

This monthly SOC report delivers a comprehensive overview of security posture, providing an in-depth analysis of alerts/incidents and critical metrics for {Month – Year}.

The OPSWAT Security Team is continuing to learn and understand the environment's behavior to improve the accuracy of the alerts.

Here are the highlights for {Month – Year}:

| Description | Metric |
|---|---|
| Events Received | 98,765,432 |
| Alerts/Investigation | 24/24 |
| True Positive Alerts | 19 |
| False Positive Alerts | 5 |
| Security Incidents | 0 |
| Alerts not reviewed within 8 hours | 0 |
| Data out of the network (GB) | 1905 |
| Data leaks exposing customer account information | 0 |
| Unique Data Source Types providing SIEM data (https://attack.mitre.org/datasources/) | 11/41 |
| Time to finish IOC Sweep of the site (seconds) | 10 |

OPSWAT.

# 2. Monitoring Summary

**Objective:** Report and detect anomalous traffic in the environment. Continuously monitor the environment and communication between critical assets.

## 2.1 Summary

In {Month - Year} OPSWAT monitored no anomalous monthly traffic volume. There was no anomalous authentication or authorization from external IP addresses to internal IP addresses. There was a decrease in bytes out of the network.

## 2.2 Details

### 2.2.1 Event Trend

In {Month - Year}, 98,765,432 events were forwarded to MetaSIEM. Firewall traffic logging is the primary source of forwarded information and events.


*Figure 1: April Event Trend*

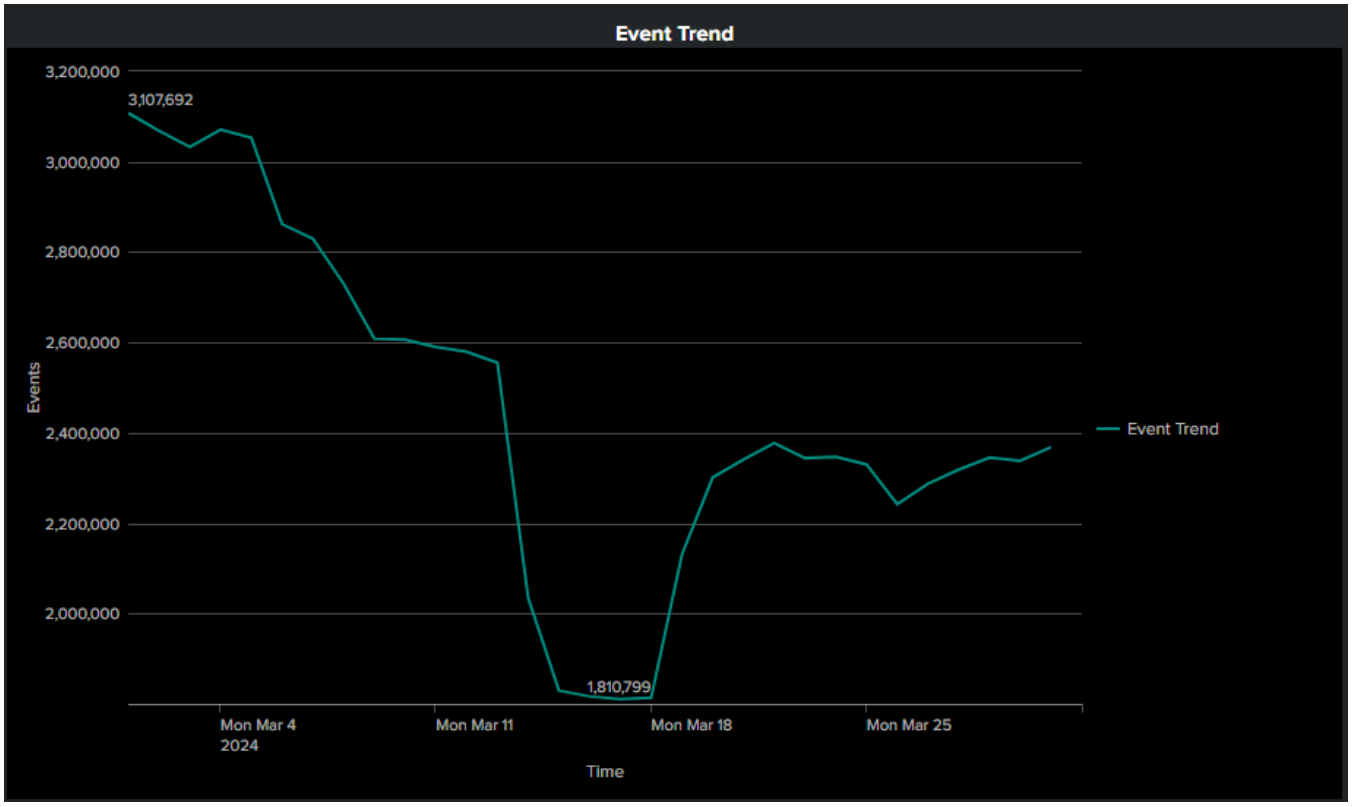



*Figure 2: March Event Trend*

### 2.2.2 Egress Bytes

In April 2024, 4766.44 GB of data went outbound from the network (internal IP addresses communicating to external IP addresses), a 260.5% increase from the previous month.

| Month | 2024 April | 2024 March | 2024 February |
|---|---|---|---|
| Data out of the network (GB) | 1905.24 | 1200.16 | 2674.22 |

Last two months egress bytes over time comparison charts

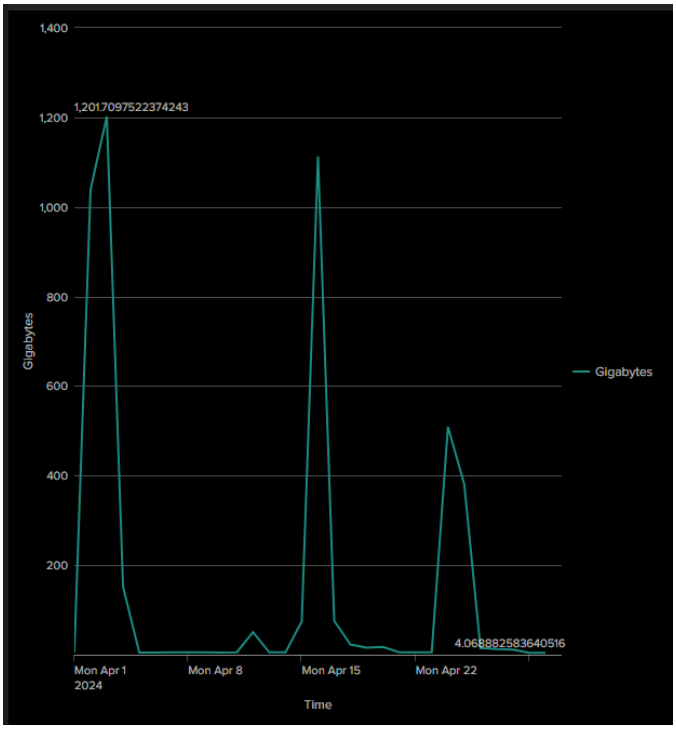



*Figure 3: April Egress Bytes Over Time*

On April 2, egress bytes reached the highest level of the month.

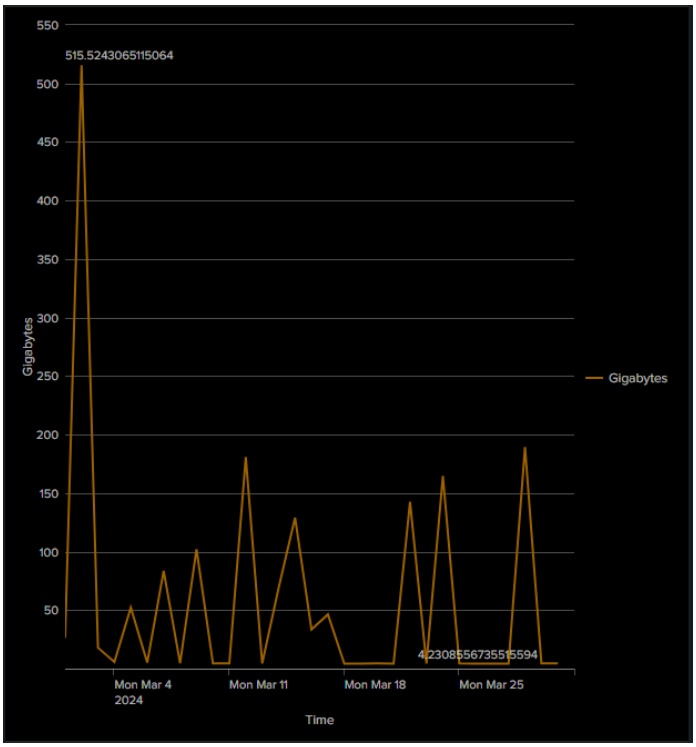


*Figure 4: March Egress Bytes Over Time*

**Sending data out of the network by hosts:**

| Source IP | Gigabytes Out | Distinct Destination IP |
|---|---|---|
| Source IP 1 | 1000 | 500 |
| Source IP 2 | 900 | 400 |
| Source IP 3 | 800 | 300 |
| Source IP 4 | 700 | 200 |

*Figure 5: 19 Hosts Sending Data Out of the Network*

### 2.2.3 Number of Authentication/User Monitors

**Windows Event Logs Logon Event**

| | 2024 April (count) | 2024 March (count) |
|---|---|---|
| Successful Authentication | 4 | 4 |
| Failed Authentication | 11 | 0 |
| Lockout Account | 0 | 0 |
| Rare User Authentication | 0 | 0 |

In April, OPSWAT did not record unusual authentication from machines sending logs to OPSWAT MetaSIEM.

*Figure 6: Successful Logons*

### 2.2.4 External to Internal Connection

No RDP, SSH, FTP, or SMB connections were observed from external to internal zones.

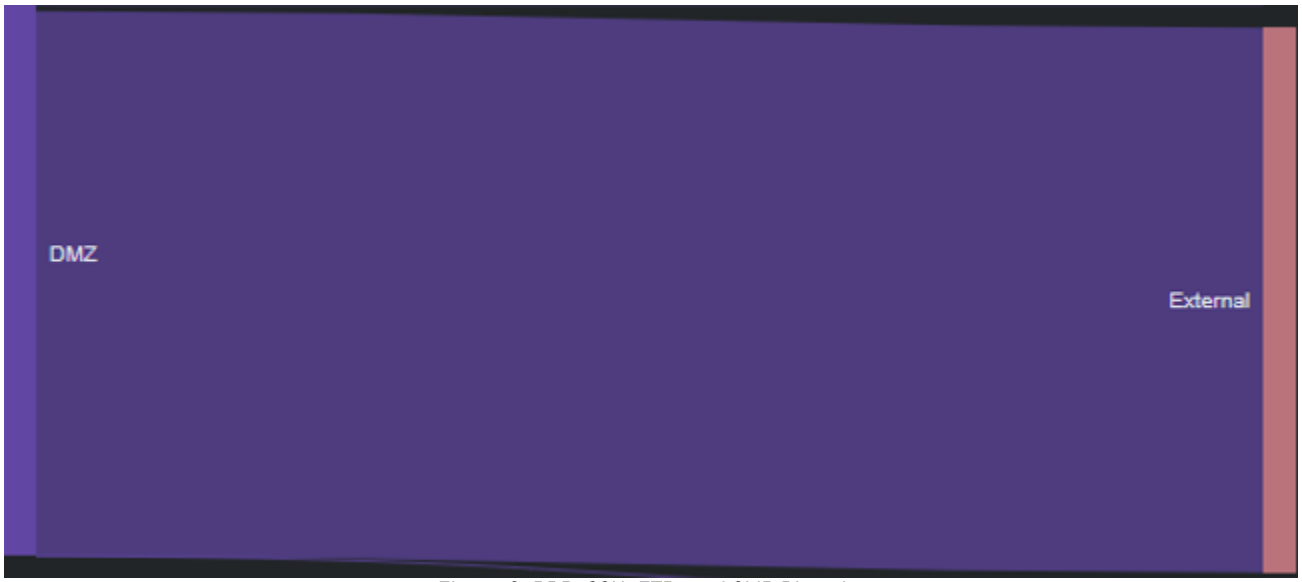



*Figure 8: RDP, SSH, FTP, and SMB Direction*

### 2.2.5 Workstations, OT Assets, and Server Monitors

MetaSIEM receives logs from eight (8) servers and workstations, encompassing servers, workstations, and firewalls:

**Customer Name**

| Host | IP Address |
|---|---|
| DEVICE #1 | 0.0.0.0 |
| DEVICE #2 | 0.0.0.0 |
| DEVICE #3 | 0.0.0.0 |
| DEVICE #4 | 0.0.0.0 |

### 2.2.6 Detection coverage (MITRE TTP Coverage)

OPSWAT MetaSIEM currently collects data from 11 data sources, which covers 87.8% of the tactics, techniques, and procedures (TTPs) from the MITRE ATT&CK Framework. This data is used to generate 55 alerts that detect each phase in the cyber kill chain.

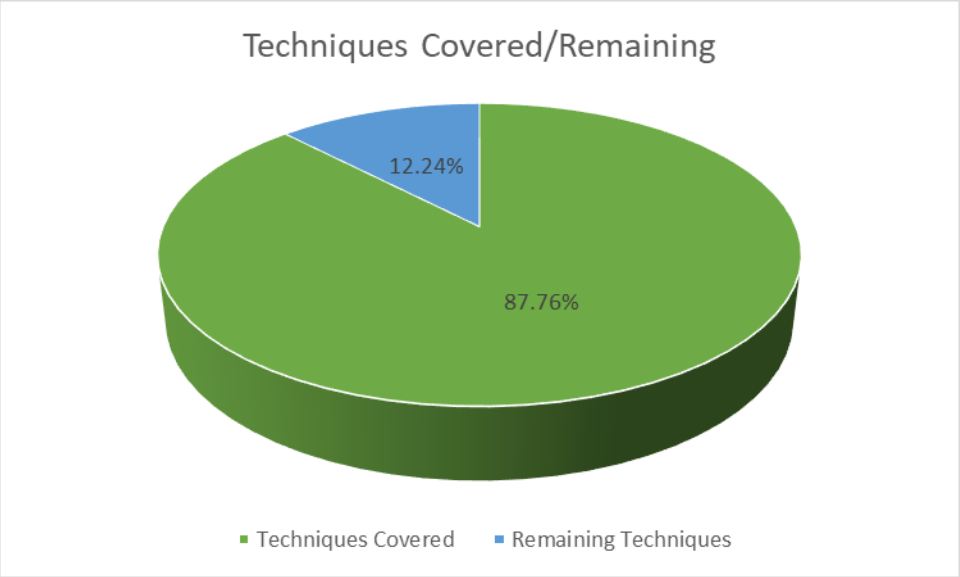


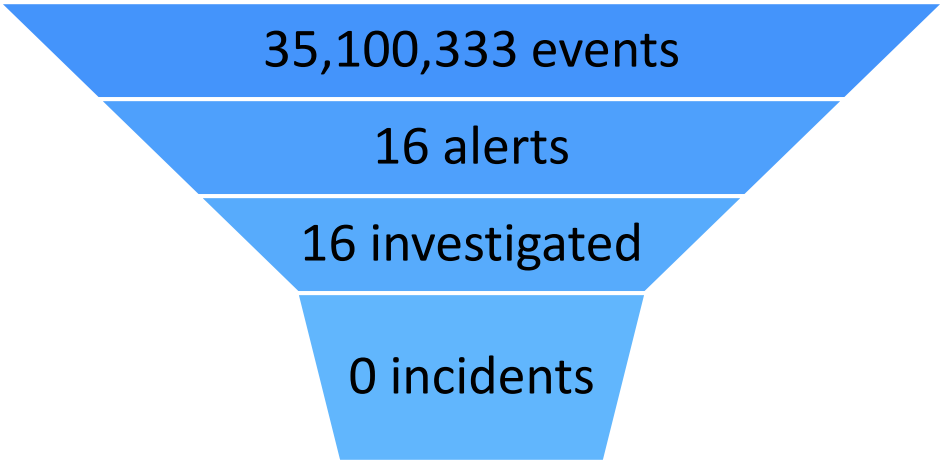

*Figure 7: Detection Coverage*

## 3. Security Event and Incident Summary

**Objective:** Review security events, investigate and resolve any incidents that might occur, and provide statistics on the security operation center's performance and health.

### 3.1 Summary

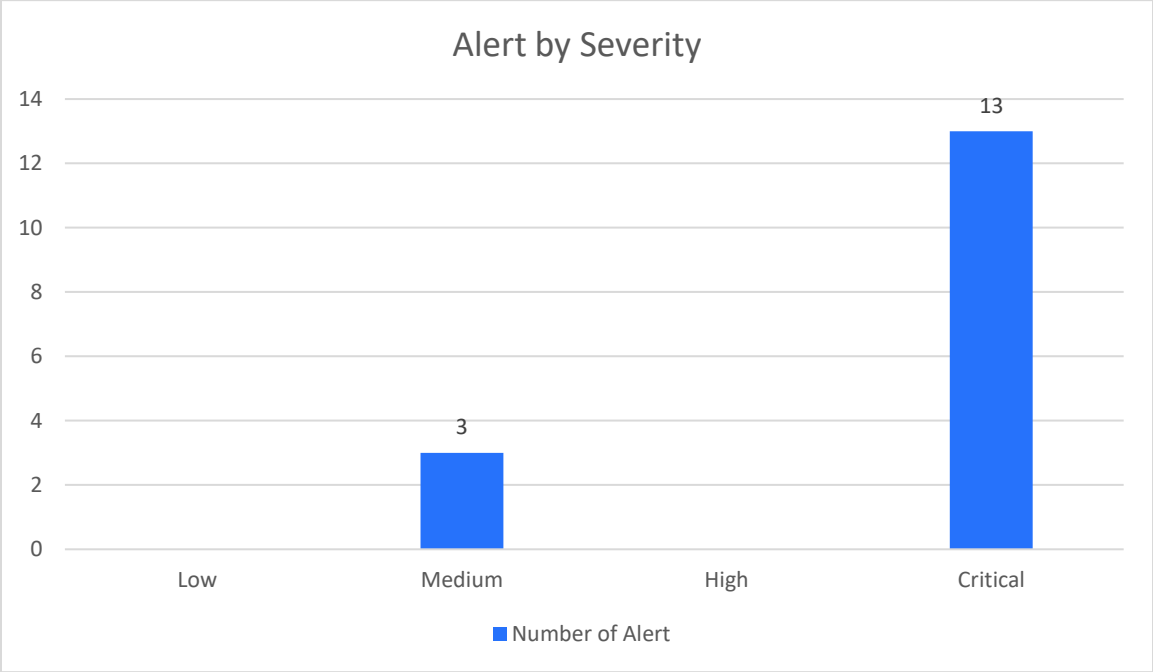
In April 2024, OPSWAT collected **35,100,333 events** and conducted 16 investigations from 16 triggered alerts. We have leveraged various tooling and statistical methods to triage. No security incident was detected.



## 3.2 Details

### 3.2.1 Alerts by Severity

For April 2024, OPSWAT has received a total of 16 alerts.




In Details:

| Host | Alert Name | Severity | Count | True Positive / False Positive |
|---|---|---|---|---|
| Device #1 | {Alert Name} | Critical | 13 | 13/0 |
| Device #1 | {Alert Name} | Medium | 3 | 0/3 |

OPSWAT detected thirteen [13] alerts as True Positives. Further examination determined that the firewall successfully blocked all these alerts without impacting the operational environment.

### 3.2.2 Most and Least Triggered Alerts

**Most triggered alerts by host**

| Host | Count | Severity | Type of Alerts |
|---|---|---|---|
| Device #1 | 13 | Critical | {Alert Name} |

Least triggered alerts by host

| Host | Count | Severity | Type of Alerts |
|---|---|---|---|
| Device #2 | 3 | Medium | {Alert Name} |

### 3.2.3 Security Monitoring

OPSWAT does not just react to alerts. We also keep a dashboard for real-time analysis and statistics on the logs we collect.

| | |
|---|---|
| Number of anomaly command line execution | 0 |
| Number of users authenticate outside of work hours | 0 |
| Number of new users access the OPSWAT-monitored devices | 0 |
| Number of anomaly network communication | 0 |

OPSWAT monitored and observed that no anomalous activities were occurring.

** These report fields are based on the firewall log and the devices sending logs to MetaSIEM using Splunk UF.*

# 4. Threat Summary

**Objective:** Proactive seeking for threats and assessing customer environment.

## 4.1 Summary

Leveraging open-source intelligence (OSINT) methods, OPSWAT conducted a comprehensive internet search to collect publicly available customer business email addresses. These email addresses were then scrutinized using OSINT Scanner and IOC Sweeper to uncover any compromise in data breaches. This valuable information can be utilized to identify and mitigate potential attack vectors.

## 4.2 Details

### 4.2.1 Threat Intelligence

In April, OPSWAT ingested 306 indicators of compromise from 15 threat feeds [1].

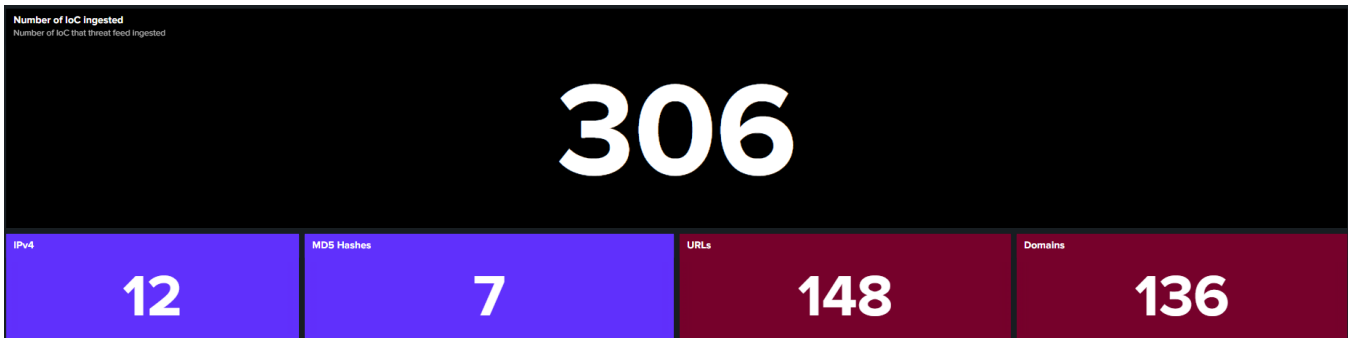



*Figure 8: Threat Intelligence Dashboard*

The IOC sweeper did not identify any matches during April, indicating the absence of indicators of compromise (IOCs) within the environment. This positive outcome suggests that the environment remains uncompromised.

The gap:

- OPSWAT only has information about endpoints that installed Splunk UF or Sysmon; hosts that are not installed by OPSWAT can only use network traffic to scan and correlate.

To fully address potential vulnerabilities, OPSWAT is actively working on expanding its endpoint coverage and implementing network traffic analysis capabilities.

[1] OTX Threat Feed – Ransomware, C2 Tracker, Energy Sector Related IoC, Blocklist tracker, Botnet Exposer

We track company email public on the Internet; this could pose a risk to the site and monitor these email addresses:

| Email | Public on the Internet | Public Data Breached Found | Impact on the System |
|---|---|---|---|
| {user1.mail.address} | X | | Low |
| {user2.mail.address} | X | | Low |
| {user3.mail.address} | X | | Medium |
| {user4.mail.address} | X | | Medium |

**Impact on the system is based on the amount of system access and the latest date when the mail was found in a public data breach.*

No indications of data breaches have been identified on forums or messaging platforms commonly used to trade stolen data, implying the absence of stealer infections on compromised machines.

### 4.2.2 ICS/OT CVE Tracking

There were no CVEs that affected the {Customer Name} site this month.

OPSWAT.

# 5.Conclusion(s) and Recommendation(s)

## 5.1 Conclusion(s)

{Customer Name} maintains a strong security posture, as evidenced by the absence of security incidents in April 2024. All alerts were thoroughly investigated and successfully mitigated. The current security posture effectively shielded the network from high and critical severity threats from external entities.

## 5.2 Recommendation(s)

OPSWAT recommends that:

- Recommendations about device security
- Recommendations about security enhancements
- Recommendations about the alerts

OPSWAT is a global leader in IT, OT, and ICS critical infrastructure cybersecurity, and for the last 20 years has continuously evolved an end-to-end solutions platform that empowers public and private sector organizations with the critical advantage needed to protect their complex networks and ensure compliance. OPSWAT solves customers' cybersecurity challenges around the world with zero-trust solutions and patented technologies across every level of their infrastructure, securing their networks, data, and devices, and preventing known and unknown threats, zero-day attacks, and malware.

## OPSWAT Professional Services

www.opswat.com/services/professional-services

For more information
Visit www.opswat.com

OPSWAT.
Protecting the World's Critical Infrastructure