Threat Report

2026-10-01 - 2026-10-31

RRCyber
SECURITY
24/7 DETECTION. RAPID RESPONSE. ENTERPRISE PROTECTION.

RRCYBER



Powered By:
HUNTRESS

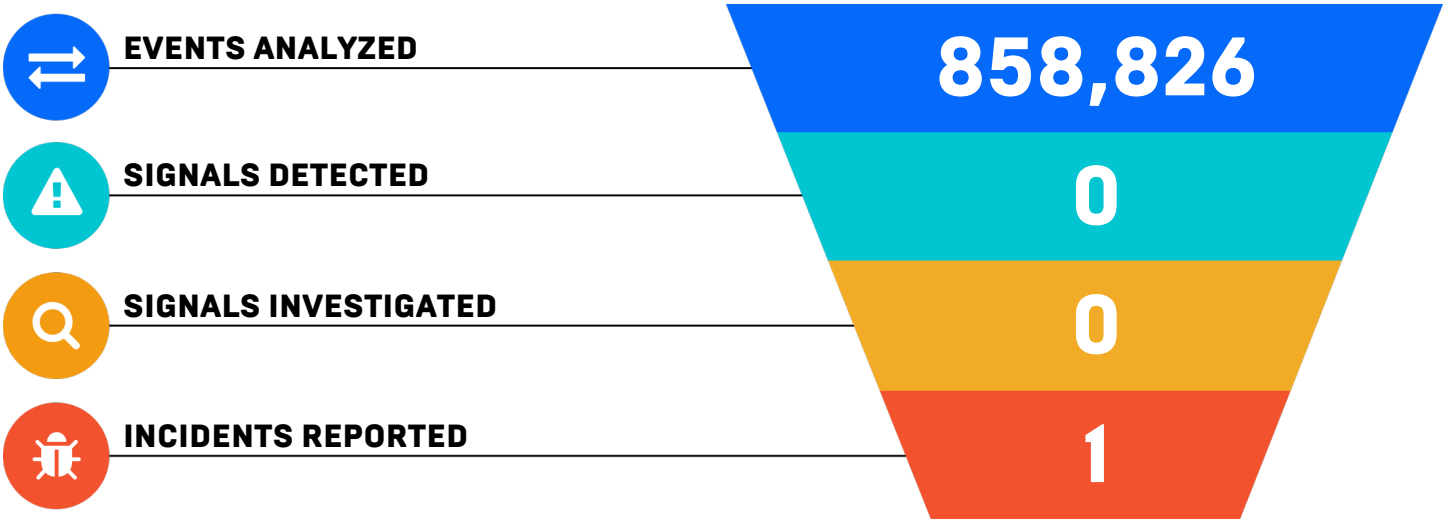
SUMMARY

During the time frame of this report, your cybersecurity platform **analyzed 858,826 events** from **2 entities** on your network.

Of those events, there were **0 signals detected**. Security analysts further reviewed the event data, resulting in **1 incident report**, which required remediation of compromised entities by your security team. This defense strategy continues to reduce your risk, which maximizes your security and minimizes cyberattack damage to your business.

ENTITIES PROTECTED

1 1



ANALYST NOTES



HERBIE ZIMMERMAN
MALWARE ANALYST

GLOBAL THREATS

- RMM
- MAV ALERTS

This month, trial-licensed remote monitoring and management (RMM) installs drove our alert volume. Attackers registered ScreenConnect services on endpoints, launched binaries staged in temp folders, and aimed service commands at relay domains outside any hosted instance. Antivirus flagged trojans being dropped on those same hosts. We'd suggest confirming which remote access tools are approved and alerting when new service installations occur.

PERSISTENT FOOTHOLDS

During this time frame, your cybersecurity platform **analyzed 1,110 autorun events** to discover persistent footholds that, if not remediated quickly, could become malicious threats to your business.

Of those events, there were **0 autorun signals detected**.

AUTORUN EVENT TRIAGE

1,110
Autorun Events Analyzed

0
Autorun Signals Detected

0
Autorun Signals Investigated

0
Foothold Incidents Reported

WHAT IS A PERSISTENT FOOTHOLD?

Persistent Footholds are mechanisms attackers use to gain long-term access to a network by exploiting common auto-starting applications (autoruns), such as Skype or Google Updater.

By abusing and masquerading as legitimate system components, attackers can slip by other security tools, remaining undetected while planning their next move.

RANSOMWARE CANARIES

During this time frame, your cybersecurity team monitored **15 canary files deployed** on Windows endpoints, which acted as early warning signals for ransomware on your network.

Like the old canary in the coal mine, Ransomware Canaries enable faster and earlier detection of potential ransomware incidents. When deployed, small lightweight files are placed on all protected endpoints—and if those files are modified or changed in any way, an investigation is conducted.

CANARIES IN YOUR MINE

3 Protected User Profiles

with **15** total canary files, deploying multiple canary files per user

0 Ransomware Incidents Reported

across **2** endpoints

RANSOMWARE IN THE NEWS

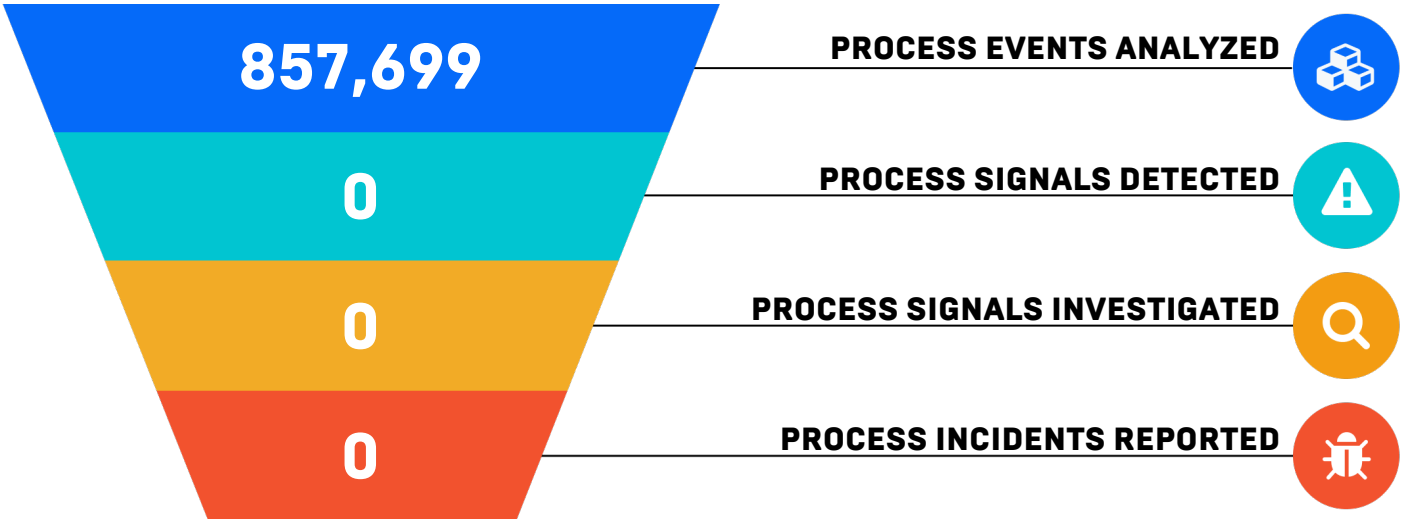
A new ransomware variant called Settra is being spotted in the wild. First reported in June 2026, Settra employs notable defense evasion techniques such as deleting Windows Event Logs and disabling the Windows Recovery Environment. Public reporting points to compromised VPNs and/or stolen credentials as potential initial access points. In two incidents Huntress investigated, the threat actor installed the MeshAgent RMM tool, and the later attack employed the Bring Your Own Vulnerable Driver (BYOVD) technique to disable certain security controls. Indicators of compromise include a ransom note named RESTORE_FILES.txt and an executable named after the victim's organization with _win64.exe appended.

PROCESS INSIGHTS

During this time frame, your cybersecurity platform **analyzed 857,699 process events** to identify suspicious processes that could lead to malware execution.

Of those events, there were **0 process signals detected**.

PROCESS INSIGHTS EVENT TRIAGE



WHAT IS PROCESS INSIGHTS?

Before causing disruption, malicious actors use covert processes to stalk the systems they plan to exploit. Process Insights enables your security team to detect these precursor actions.

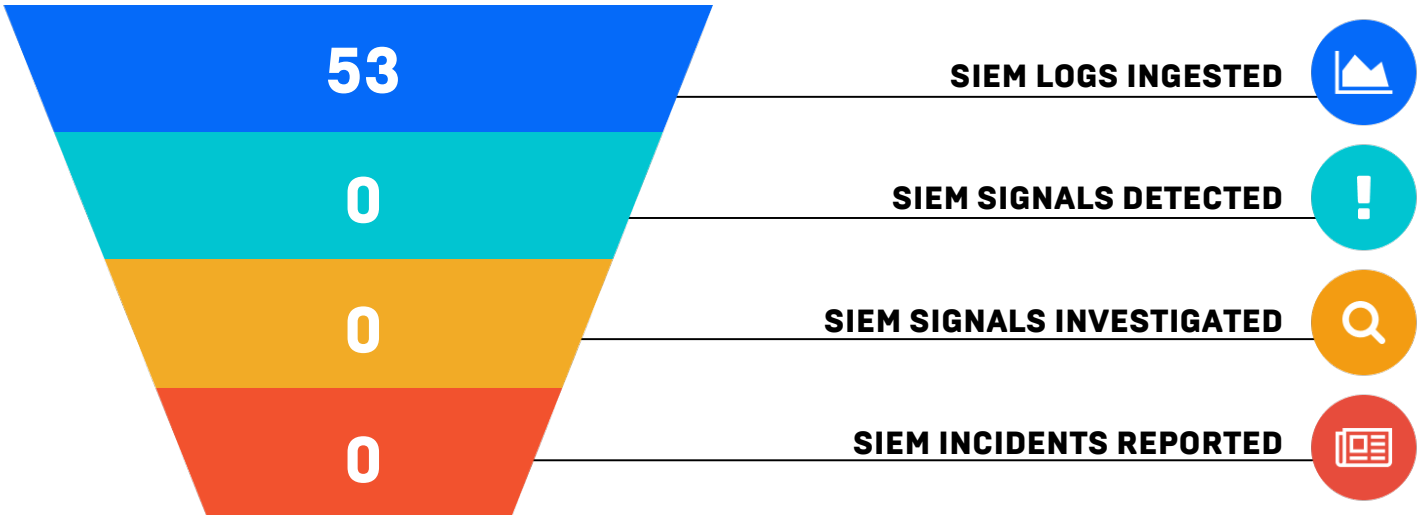
Once identified your cybersecurity platform is able to stop the maliciously running processes in their tracks, preventing further cyber attack spread.

MANAGED SIEM

During this time frame, your cybersecurity platform **ingested 53 logs** in order to identify any that could be potential threats to your organization.

From the ingested logs, there were **0 SIEM signals detected**.

SIEM EVENT TRIAGE



WHAT IS SIEM?

Security Information and Event Management (SIEM) aggregates and analyzes security data from various sources across an organization's IT infrastructure. It enables real-time monitoring, threat detection and response by identifying patterns, anomalies and alerts within the data.

Analysts use the consolidated information from SIEM to assess risks, correlate events and respond quickly to incidents.

INCIDENT SUMMARY

During this time frame, your security team responded to a total of **1 incident report** . This page provides summary metrics, broken down by incident severity, product, most common antivirus signals reported, and most targeted entities."

INCIDENT SEVERITY & SOURCE

1
Total

1 Critical
0 High
0 Low

1 EDR
0 ITDR
0 SIEM

MOST REPORTED AV SIGNALS

No AV Signals Reported!

MOST TARGETED DEVICES

Company X - PC

INCIDENT LOG

During this time frame, your security team resolved 1 out of the 1 incident reported. This log highlights the critical and high severity incidents.

2026-10-19 Critical

Closed - Company X - PC

----------SIMULATED INCIDENT---------- *** The Huntress Agent has been tasked to isolate this host from the rest of the network in order to prevent the incident from spreading to other hosts. *** ... (see more)

RRCyber