THREAT REPORT

2025-09-01 - 2025-09-30

PC Solutions

PC SOLUTIONS

Powered By:

HUNTRESS

THREAT REPORT 2025-09-01 to 2025-09-30
PC SOLUTIONS

SUMMARY

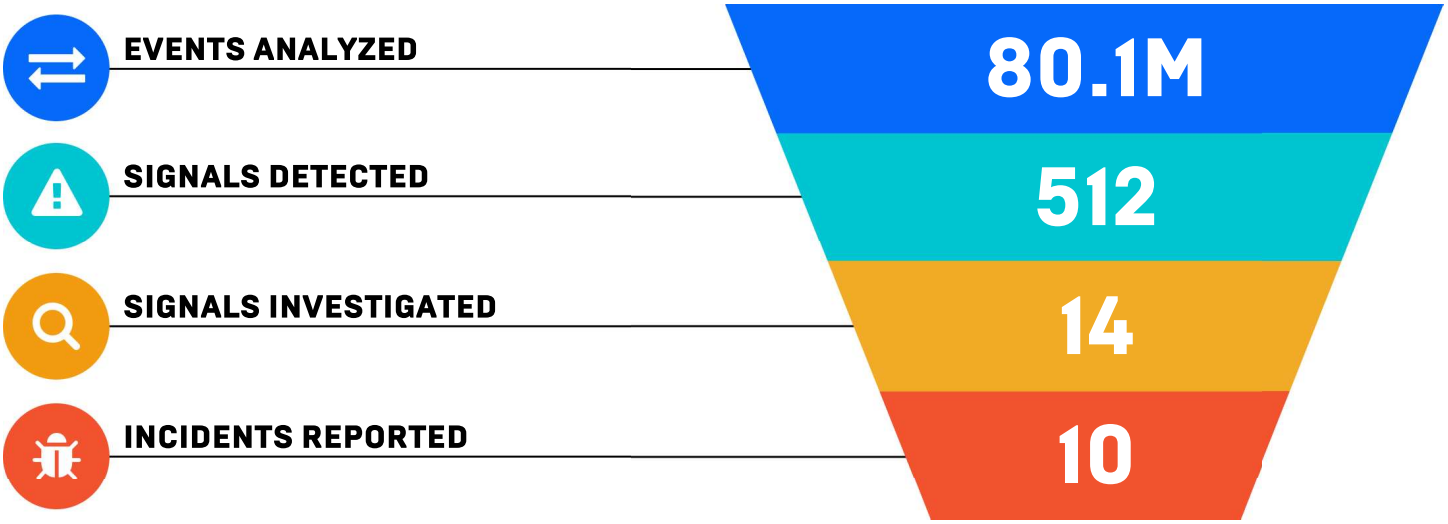
During the time frame of this report, your cybersecurity platform **analyzed** 80,092,563 **events** from 372 **entities** on your network.

Of those events, there were 512 **signals detected** through automated and human analysis. Security analysts manually **investigated** 14 **signals** that were suspicious in nature. Those investigations led to 10 **incident reports**, 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

365 32

7



ANALYST NOTES

HERBIE ZIMMERMAN
MALWARE ANALYST

GLOBAL THREATS

- ATO
- SOCIAL ENGINEERING

This month, we're seeing attacks against cloud identity accounts, mainly from ISPs with malicious ASN ratings. By launching attacks from ISPs with these overly lenient policies, threat actors are using time-tested techniques, like sending Business Email Compromise (BEC) emails or manipulating a user's inbox with rules to redirect or hide messages. Adding security "speed bumps" like MFA and providing awareness training are great ways to slow down threat actors and help protect user identities.

PERSISTENT FOOTHOLDS

During this time frame, your cybersecurity platform **analyzed 178,265 autorun events** to discover persistent footholds that, if not remediated quickly, could become malicious threats to your business.

Of those events, there were **14 autorun signals detected** through automated and human analysis. Security analysts manually **investigated 1 signal** that was suspicious in nature. That investigation led to **1 foothold incident report**, which required remediation of compromised endpoints by your security team.

AUTORUN EVENT TRIAGE

178,265
Autorun Events Analyzed

14
Autorun Signals Detected

1
Autorun Signals Investigated

1
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 **5,388** **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

949 Protected User Profiles

with **5,388** total canary files, deploying multiple canary files per user

0 Ransomware Incidents Reported

across **365** endpoints

RANSOMWARE IN THE NEWS

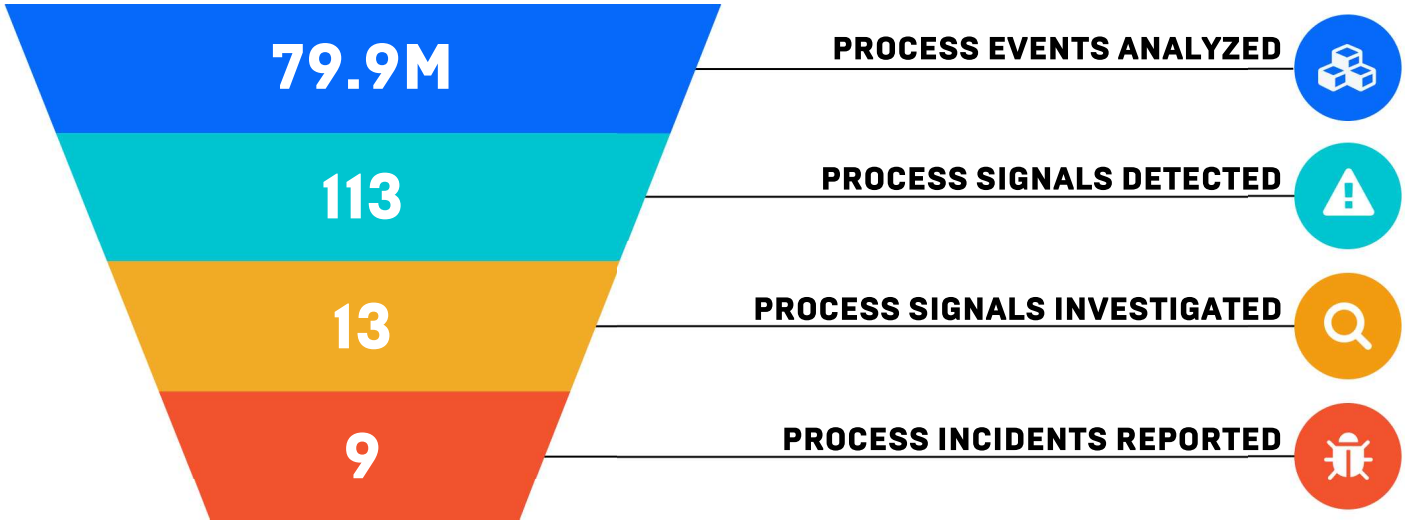
In the last year alone, the number of ransomware groups has exploded, with 41 new groups emerging. This change was due to efforts to shut down major players like LockBit and Conti. These smaller, agile groups are targeting supply chains and cloud vulnerabilities. Key newcomers include Obscura, Cephalus, and PromptLock, joining notable groups like RansomHub, Qilin, and Akira. PromptLock uses generative AI to build real-time malicious scripts, attracting less-skilled attackers. At the same time, the seemingly unstoppable DragonForce is trying to form a "cartel" with LockBit and Qilin, suggesting brutal joint attacks soon. This quarter, attacks focused on automotive, airline, healthcare, retail, and manufacturing facilities, often through third-party integrations like technical support services and apps. Attackers are getting better at disabling EDR services and wiping system logs to erase their digital footprints, making it much harder for cybersecurity defenders to keep up.

PROCESS INSIGHTS

During this time frame, your cybersecurity platform **analyzed** 79,908,090 **process events** to identify suspicious processes that could lead to malware execution.

Of those events, there were 113 **process signals detected** through automated and human analysis. Security analysts manually **investigated** 13 **signals** that were suspicious in nature. Those investigations led to 9 **process incident reports**, which required remediation of compromised endpoints by your security team.

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.

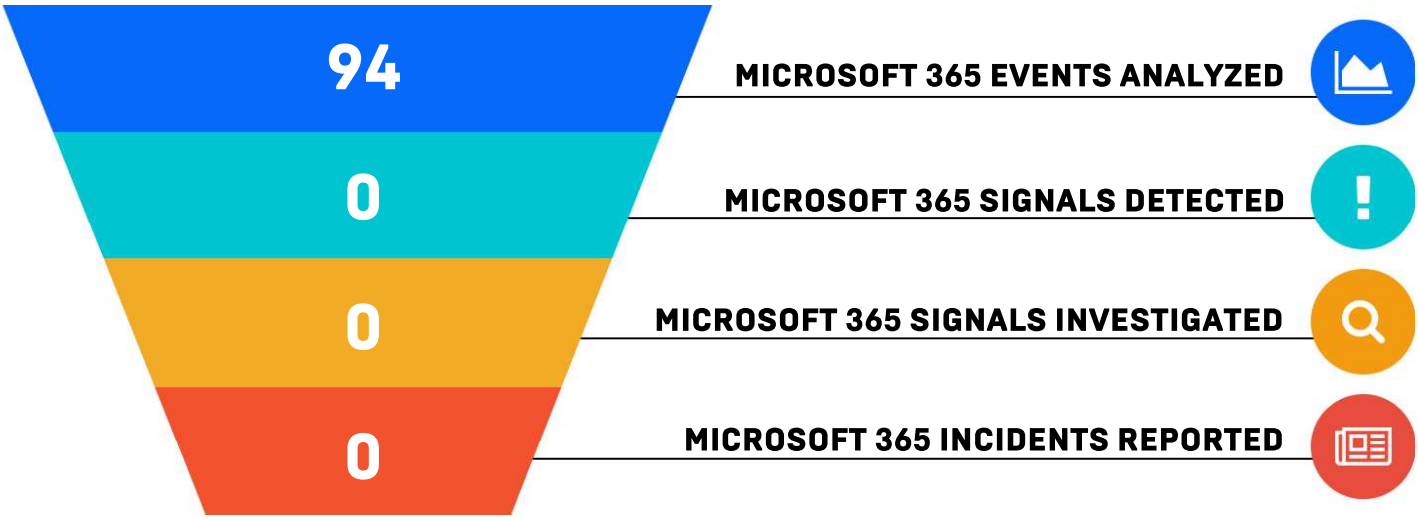
Once identified your cybersecurity platform is able to stop the maliciously running processes in their tracks, preventing further cyber attack spread.

MANAGED ITDR

During this time frame, your cybersecurity platform **analyzed 94 Microsoft 365 events** to identify any that could be potential threats to your Microsoft 365 users or environment.

Of those events, there were **0 Microsoft 365 signals detected.**

MICROSOFT 365 EVENT TRIAGE



WHAT IS MANAGED ITDR?

As an integral and widespread productivity suite, Microsoft 365 is a high-profile target for threat actors. Managed ITDR can detect anomalous logins, suspicious email rules, and other hacker tradecraft within Microsoft 365.

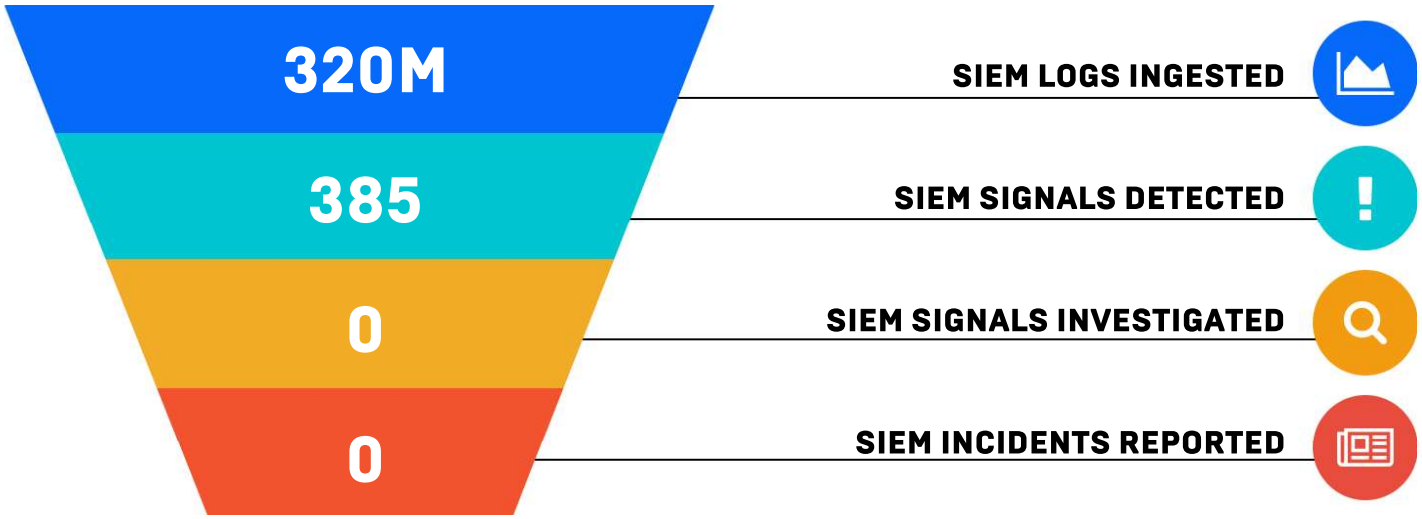
When a potential attack is detected, a security analyst reviews the activity, and an incident report with remediation steps is actioned by your security team.

MANAGED SIEM

During this time frame, your cybersecurity platform **ingested 320,370,954 logs** using Smart Filtering to reduce noise **from originally 2,609,664,624 logs** in order to identify any that could be potential threats to your organization.

From the ingested logs, there were **385 SIEM signals detected** through automated and human analysis. None of the detected signals were suspicious in nature, thus no further investigation was warranted by your security team.

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 **10** **incident reports**. This page provides summary metrics, broken down by incident severity, product, most common antivirus signals reported, and most targeted entities."

INCIDENT SEVERITY & SOURCE

10
Total

- **0** Critical
- **0** High
- **10** Low

- **10** EDR
- **0** ITDR

MOST REPORTED AV SIGNALS

No AV Signals Reported!

MOST TARGETED DEVICES

devices
identities
removed
by RR

INCIDENT SAVINGS

Save your organization thousands, if not millions, of dollars by identifying and remediating cyber incidents in a timely manner. The costs increase dramatically depending on the size of your organization and the value of your data. Use our downtime calculator to see what an incident could potentially cost your organization.