THREAT REPORT

11/01/21 - 11/30/21

DUNDLER MIFFLIN

Powered by:

HUNTRESS

THREAT REPORT 11/01/21 - 11/30/21
DUNDLER MIFFLIN

SUMMARY

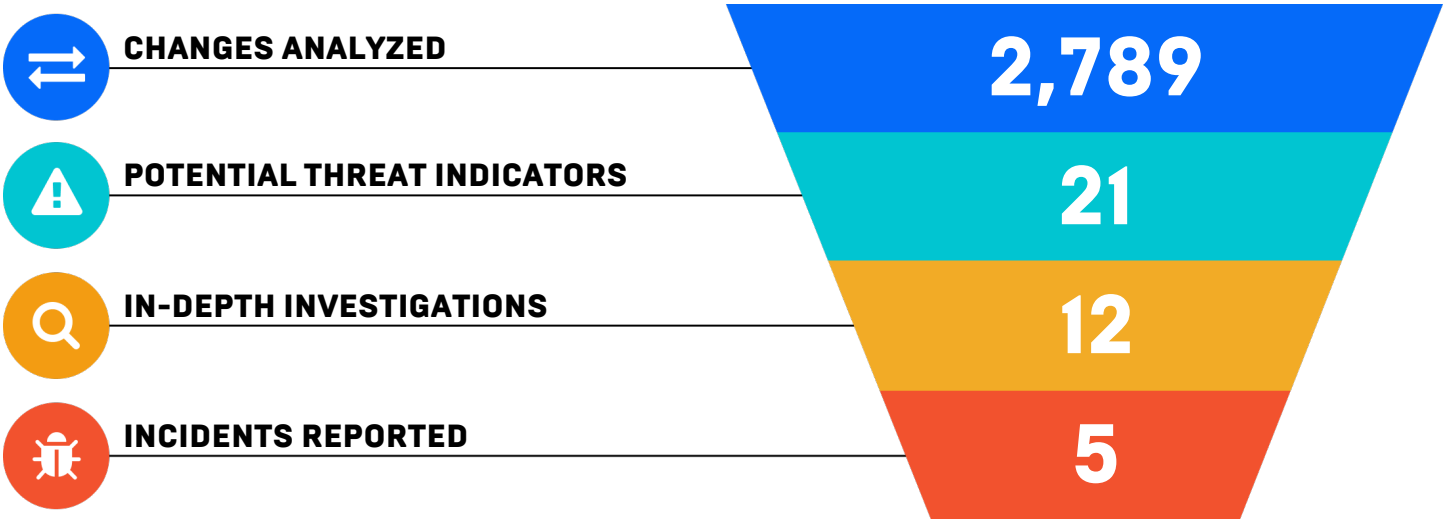
During this report's timeframe, your cybersecurity platform analyzed **2,789** **changes** to the computer systems on your network in order to detect malicious activity.

Cyber Threat Hunters reviewed **21** **potential threat indicators** that were previously unknown or suspicious. **In-depth investigations** were conducted as needed and **5** **cyber incident reports** were created and responded to by your security team. This defense strategy continues to reduce your cyberattack risk, maximize your security, and minimize downtime and damage to your business.

SYSTEMS PROTECTED

3 COMPUTERS

1 SERVERS



ANALYST NOTES

JOHN FERRELL
TECHNICAL DIRECTOR, THREATOPS

GLOBAL THREATS

- LEMON DUCK
- JUPYTER
- QAKBOT

We've seen a rise in internet facing services being compromised. Take time to audit any externally accessible services including web applications, VPNs, remote desktop, etc. Ensure these services have the latest patches and are configured using best practices. Verify that Multi-Factor Authentication is enabled on any public facing applications where applicable.

INCIDENT SUMMARY

During this timeframe, your security team responded to a total of **5 incident reports**. This page provides summary metrics, broken down by incident severity, threat indicators, top AV detections, and most targeted devices.

INCIDENT SEVERITY & SOURCE

5
Total

- **2** Critical
- **3** High
- **0** Low

- **4** Footholds
- **1** Managed AV
- **0** Canaries

TOP REPORTED AV DETECTIONS

- Behavior:Win32/Shortcut...
- Behavior:Win32/KovterLa...

MOST TARGETED DEVICES

- CORP-DC1-SCRANTON
- CUST-SVC1
- KEVIN

INCIDENT SAVINGS

A cyber incident that is identified and remediated in a timely manner can save your company thousands if not millions of dollars depending on the size of your organization and the value of your data. You can explore the potential cost of an incident for your business here.