Counter
Craft

CounterCraft The Pulse™

A real-time, deception-powered threat intel feed

Despite being an industry standard, generic, out-of-context threat intel feeds are not actionable.

The fresher the threat intelligence a security team can gather, the better their chances are of defending against a cyber attack. Professionals know this—56% of participants in a survey felt that threat intelligence becomes stale within minutes[1]. Now, with CounterCraft The Pulse™, you can get fresh attack incident data in real time.

The average delay between the discovery of an incident and its reporting is 21 days, and that doesn't include the often months-long threat actor dwell time within the network. That is simply too long to be relevant. With CounterCraft's deception technology, you get a must have: contextualized, 100% actionable threat intelligence. CounterCraft The Pulse™ brings you a near real-time source of Machine Readable Threat Intelligence (MRTI) with an unbeatable signal to noise ratio.

The Pulse™ gives complete threat intelligence of a threat actor's movements within an incident including TTPs, step-by-step actions, IOCs, files, and hashes

What is The Pulse?

The Pulse is a threat intelligence feed of prepared incident data from CounterCraft. The incident data gathered in near real-time using cyber deception shows:

- How attacks are being carried out right now
- Detail and context on the intelligence
- Exactly what CounterCraft is seeing in the wild

Users download only the incidents that are of interest to their organization. There are no filters—security professionals get complete intel exactly as it happened. The Pulse is an incredible value for anyone who is interested in receiving up to the minute threat intel on live incidents in near real-time—incidents are published within 24 hours.

The Pulse is continuously adding new campaigns to CounterCraft cyber deception farms deployed across the internet, which means users get the latest threat intelligence regarding any new relevant vulnerabilities or offensive techniques that are being exploited in the wild. Users can request the addition of any specific software to the deception farms.

Benefits

- Identify exploits before they affect your organization
- Get the details and the context you need to make security decisions
- Prioritize risk mitigation
- Download the complete attacker playbook
- Know exactly how threat actors would exploit your vulnerabilities

Key Features

- Incident tags that allow classifying by CVEs, tech stacks, and more Unlimited API queries
- Continuous monitoring
- Real-time threat intel
- RESTful API that offers incident data in a standardized JSON format
- Events have a built-in human readable summary

[1] https://securityboulevard.com/2022/06/complete-guide-to-cyber-threat-intelligence-feeds/

How It Works

Our team of experts does this:

DESIGN: CounterCraft deploys the assets associated with the service, which can include web-based email service accounts and web-based supporting infrastructure such as servers.

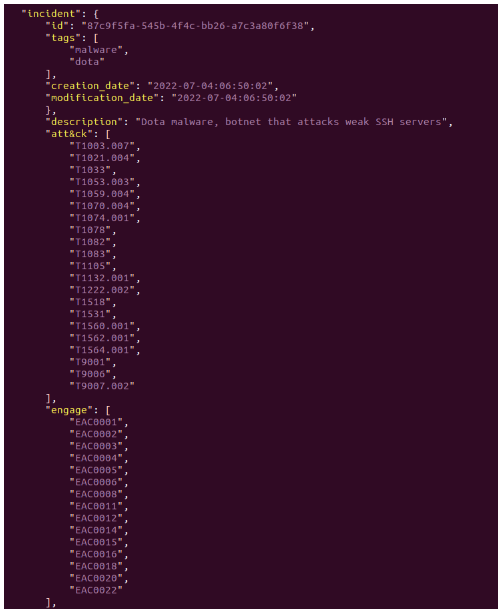
DEPLOY: These campaigns are deployed using CounterCraft's high-interaction deception technology in our own global deception farms, waiting to be compromised.

COLLECT: Detailed telemetry from the deception farms is collected in the Pulse Hub and enriched to create in-depth event data.

CURATE: The event data is managed by CounterCraft and used to create comprehensive Incidents that collect the full attack data into a single file.

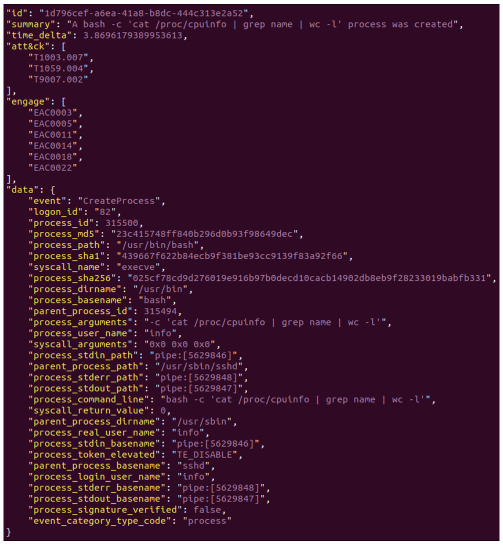
All you have to do is this:

- ✓ Search The Pulse incident database by date, time, or specific interest.
- ✓ Download the data from The Pulse API.
- ✓ Ingest the data directly into your platform of choice.
- ✓ Suggest any new vulnerabilities or malware samples you would like to see in The Pulse.



```
    "incident": {
        "id": "87c9f5fa-545b-4f4c-bb26-a7c3a80f6f38",
        "tags": [
            "malware",
            "dota"
        ],
        "creation_date": "2022-07-04:06:50:02",
        "modification_date": "2022-07-04:06:50:02"
        },
        "description": "Dota malware, botnet that attacks weak SSH servers",
        "att&ck": [
            "T1003.007",
            "T1021.004",
            "T1033",
            "T1053.003",
            "T1059.004",
            "T1070.004",
            "T1074.001",
            "T1078",
            "T1082",
            "T1083",
            "T1105",
            "T1132.001",
            "T1222.002",
            "T1518",
            "T1531",
            "T1560.001",
            "T1562.001",
            "T1564.001",
            "T9001",
            "T9006",
            "T9007.002"
        ],
        "engage": [
            "EAC0001",
            "EAC0002",
            "EAC0003",
            "EAC0004",
            "EAC0005",
            "EAC0006",
            "EAC0008",
            "EAC0011",
            "EAC0012",
            "EAC0014",
            "EAC0015",
            "EAC0016",
            "EAC0018",
            "EAC0020",
            "EAC0022"
        ],
```

Fig: Incident with identifier, tags, Att&ck and Engage clasification



```
"id": "1d796cef-a6ea-41a8-b8dc-444c313e2a52",
"summary": "A bash -c 'cat /proc/cpuinfo | grep name | wc -l' process was created",
"time_delta": 3.8696179389953613,
"att&ck": [
    "T1003.007",
    "T1059.004",
    "T9007.002"
],
"engage": [
    "EAC0003",
    "EAC0005",
    "EAC0011",
    "EAC0014",
    "EAC0018",
    "EAC0022"
],
"data": {
    "event": "CreateProcess",
    "logon_id": "82",
    "process_id": 315500,
    "process_md5": "23c415748ff840b296d0b93f98649dec",
    "process_path": "/usr/bin/bash",
    "process_sha1": "439667f622b84ecb9f381be93cc9139f83a92f66",
    "syscall_name": "execve",
    "process_sha256": "025cf78cd9d276019e916b97b0decd10cacb14902db8eb9f28233019babfb331",
    "process_dirname": "/usr/bin",
    "process_basename": "bash",
    "parent_process_id": 315494,
    "process_arguments": "-c 'cat /proc/cpuinfo | grep name | wc -l'",
    "process_user_name": "info",
    "syscall_arguments": "0x0 0x0 0x0",
    "process_stdin_path": "pipe:[5629846]",
    "parent_process_path": "/usr/sbin/sshd",
    "process_stderr_path": "pipe:[5629848]",
    "process_stdout_path": "pipe:[5629847]",
    "process_command_line": "bash -c 'cat /proc/cpuinfo | grep name | wc -l'",
    "syscall_return_value": 0,
    "parent_process_dirname": "/usr/sbin",
    "process_real_user_name": "info",
    "process_stdin_basename": "pipe:[5629846]",
    "process_token_elevated": "TE_DISABLE",
    "parent_process_basename": "sshd",
    "process_login_user_name": "info",
    "process_stderr_basename": "pipe:[5629848]",
    "process_stdout_basename": "pipe:[5629847]",
    "process_signature_verified": false,
    "event_category_type_code": "process"
}
```

Fig: Activity event example with summary and detailed info of the activity

How to Sign Up

Contextualized threat intelligence is at your fingertips

- Speak with a member of our team
- Provide them with the email and name of your users
- Begin to access up-to-the-minute threat intel immediately

What You Get

When you sign up for The Pulse, you will receive:

- A user account and credentials
- The Pulse API access software
- The Pulse User Guide

About Us

CounterCraft is the next generation of threat intelligence, thanks to a deception platform that offers active defense powered by high-interaction deception technology.

Learn more about CounterCraft. Contact us.

✉ craft@countercraftsec.com

www.countercraftsec.com