Secureworks®

WHITE PAPER

# How Leading-Edge Threat Intelligence Improves Incident Response

## Threats are Evolving Rapidly – Effective Detection and Response Requires you to Keep Up

We often hear that the threat landscape is constantly shifting – but is that really the case? Sometimes it can feel like nothing really changes – criminal threat actors continue to try and make money, and government-sponsored groups continue to use cyber intrusions to achieve their objectives. However, if you look within the details, you will see a constant evolution of tools, tactics, and infrastructure. Many organizations struggle to stay current with these changes in a way that allows them to protect themselves effectively.

To detect and stop malicious activity in your environment, you first need to know what today's malicious activity looks like. Most organizations get threat intelligence from somewhere, but how credible is your source? Where are they getting their information from?

In this paper, we discuss what makes threat intelligence effective, and why it's such an important consideration when choosing an Incident Response (IR) partner. Very few organizations, however good their defenses, can avoid a breach forever. Many find out when a breach occurs that they have not prepared adequately to respond, contain, and remediate without help. A partial explanation for this is the perception among some business leaders that incident response is a reactive activity, when in fact it should be part of cybersecurity preparedness. This misconception can present an additional challenge for organizations responding to a breach – choosing the right incident response supplier at very short notice.

Not all IR suppliers are equal, and to make the right choice, it's important to understand why. For instance, some incident response providers focus only on deadbox forensics. Crucially, many more fail to bring a broad aperture and an understanding of the threat to bear. Yet an incident response team without a full picture of the threat landscape will struggle to identify and contain threats in a prompt manner.

That's why one of the most essential factors to consider in choosing an IR partner is their aperture of the threat. That aperture comes from having scale, a global perspective, and a comprehensive understanding of the threat landscape.

**Not all IR suppliers are equal, and to make the right choice, it's important to understand why. For instance, some incident response providers focus only on deadbox forensics.**

## Exceptional Threat Intelligence, Better Incident Response

Our deep understanding of the threat landscape comes from intelligence generated from each Secureworks customer engagement, and from the threat intelligence work of the Secureworks Counter Threat Unit™ (CTU). This is an 80-strong research team with 20 years of experience is a key factor in Secureworks' accreditation by the U.S.'s National Cyber Security Cyber Assistance Program (NSCAP) and the U.K. NCSC's Cyber Incident Response (CIR) scheme. Our CTU research, combined with our IR experience, enables us to operate a continuous feedback cycle: IR incidents feed threat intelligence, which allows us to detect new incidents.

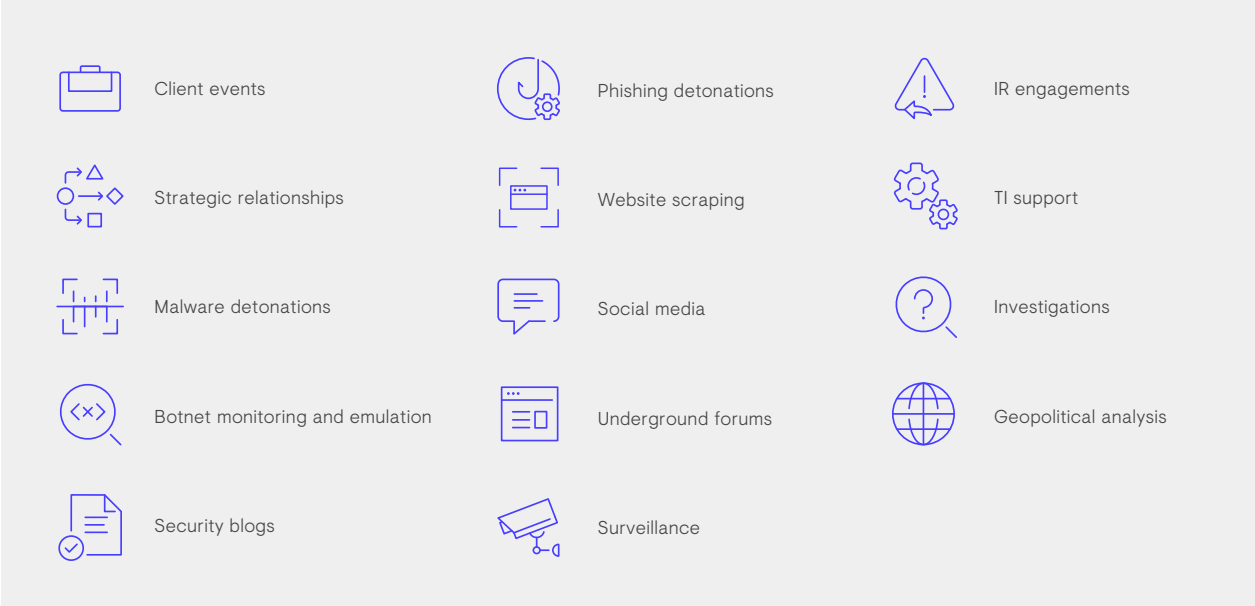
CTU researchers actively monitor over 200 threat groups and analyze over 340 billion security events generated daily by 4,300 Secureworks customers across 55 countries. This includes data generated by Red Cloak™, our endpoint monitoring agent that is installed on over 2 million endpoints around the world.

Other customer sources include 55 terabytes of intelligence gathered from 500+ emergency incident response engagements per year. These cover everything from sophisticated government-sponsored threat actor incidents, using custom malware, through to post-intrusion ransomware, using an unsecured remote desktop protocol (RDP) server as an entry method. All of these tools, behaviors, and modus operandi are broken down and added to our body of knowledge.

Other inputs include knowledge from our malware detonations. CTU processes identify and analyze thousands of malware samples per day, enabling us to determine which malware family they belong to, whether or not they are evolving, or if the code represents something we haven't seen before. Our botnet monitoring and emulation activities allow us to determine how malicious campaigns evolve and how threat actors are evolving their TTPs.

The CTU team also runs a surveillance service, using personas we maintain across a variety of platforms including within invite-only forums, as well as setting keyword alerts for customers that we monitor.

The result is the Secureworks Collection Management Framework, which describes the various sources of data from which we gather our threat intelligence. The Framework covers both low volume/high fidelity and high volume/low fidelity data.




Secureworks Collection Management Framework

Data from all of these sources is merged into our custom Threat Intelligence Management System (TIMS), which enables us, through analysis and investigations, to turn raw data into actionable intelligence.

This intelligence is then published to our customers as threat intelligence products spanning all four industry standard threat intelligence quadrants: Strategic, Tactical, Operational, and Technical. It helps our customers to distinguish the wood from the trees, to know where to focus and how to be prepared. It also powers countermeasure creation and indicator dissemination that benefit every one of our customers. And it feeds back into supporting each individual incident response engagement by giving our incident response team the context and insight it needs to swiftly and effectively contain attacks.


Secureworks threat intelligence products

## A Two-Way Relationship and a True Virtuous Circle

The overall result is that our visibility into malicious activity is second to none. This unusual degree of reinforcement between Secureworks Threat Intelligence and Secureworks Incident Response creates a true virtuous circle. This is the Secureworks Network Effect. Every customer is part of our network and instantly and exponentially benefits from the entirety of the work we do protecting our whole customer base.

Each Secureworks incident response engagement profits from support from our threat intelligence team. The body of knowledge that comes with this support enriches and adds context to our investigations while also making us more efficient. We see this in action every day; examples in recent months have included:

- A single command from a threat actor on a compromised endpoint provided the initial breadcrumb that helped us identify them.
- A specific RDP hostname used by a prolific ransomware actor gave us a great early warning system for a crippling ransomware attack.
- A regular pattern of behavior from another attacker allows us to gauge how much time remains until the ransomware deployment.

These are all actionable pieces of intelligence that our experience and processes let us collect, interpret and use to identify and prevent the adversary's next steps. This removes delays and wasted time, and allows us to concentrate on returning the customer to normal operations as soon as possible.

In return, every IR engagement captures understanding to fold into our intelligence repositories. First-hand observation of what actors do is gold – it establishes the ground truth, enabling us to rapidly create countermeasures, benefiting all our customers and further boosting the virtuous circle.

## A Better, More Effective Customer Experience

Secureworks is one of the few companies offering both incident response and threat intelligence.

Our globally scaled incident response team provides a full range of services, from emergency incident response assistance to retainer-based services that help organizational readiness and responsiveness. In addition to providing technical IR support, our IR team can also provide Incident Commanders, providing not just technical, but leadership support too. That enables us to create a truly coordinated response, even when multiple teams or vendors are involved.

Whether a customer is under attack, wants to stress test their IR processes, or needs to validate threat detection abilities, the Secureworks IR team is there to help. In every customer interaction, we bring to bear experience from each of the 1000+ IR engagements carried out by Secureworks every year, each informed and enabled by this exceptional visibility and comprehensive threat intelligence picture. Our breadth of focus helps us swiftly find and expel attackers maintaining persistence on the system.

Together, these two functions combine to create a vastly improved experience for the customer, meaning a faster, more efficient return to normal operation for our customers.

Secureworks®

## Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

### Corporate Headquarters

**United States**
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

### Europe & Middle East

**France**
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

**Germany**
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

**United Kingdom**
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

**United Arab Emirates**
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

### Asia Pacific

**Australia**
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

**Japan**
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp