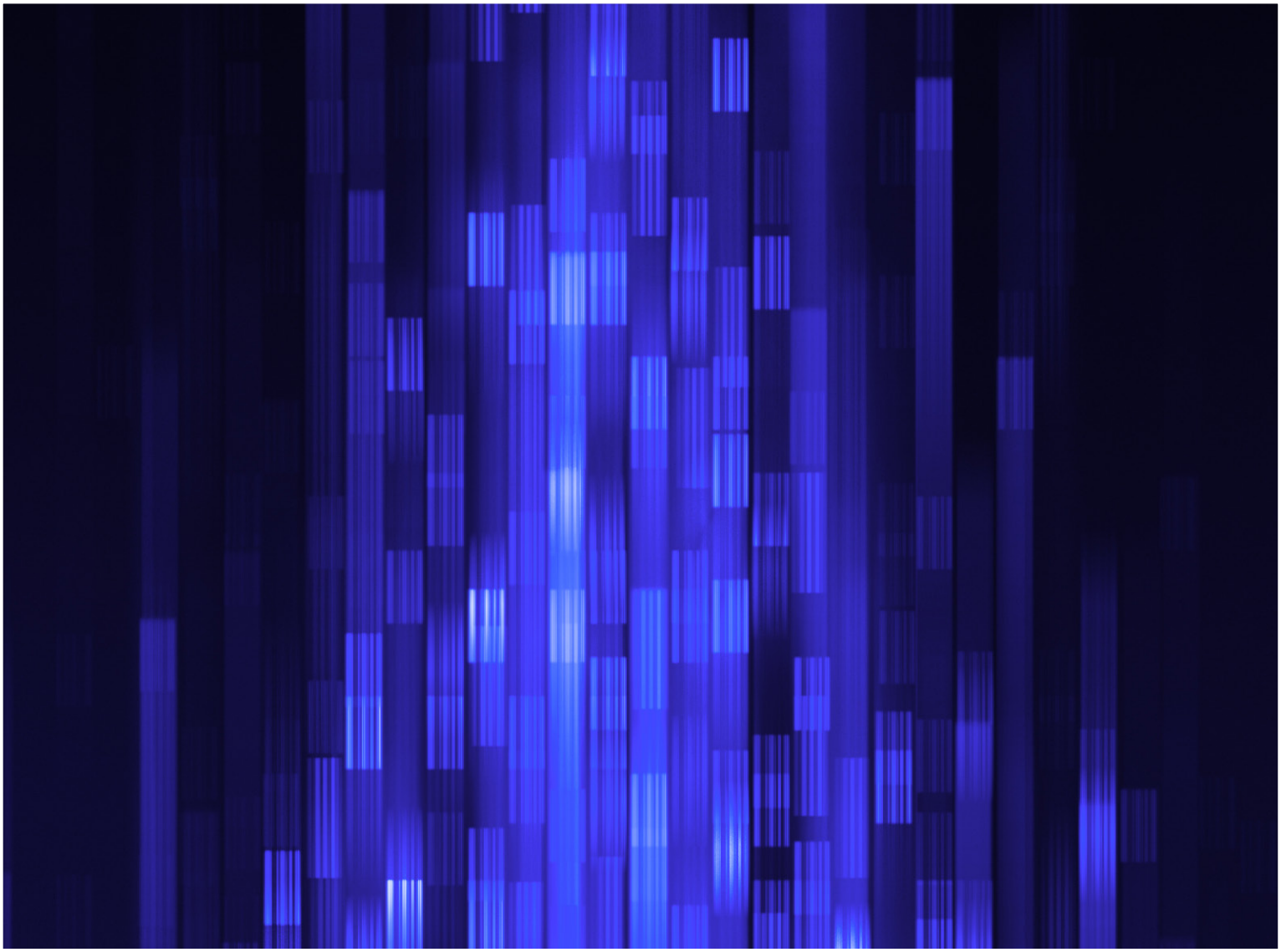
Secureworks®

WHITE PAPER

7 Common Questions Asked of Our Counter Threat Unit™ Researchers



1. What threat groups are targeting my vertical?

There really is a much better question security leaders and practitioners should ask here, based on our experience observing and engaging the bad guys.

Threat actors engaged in targeted intrusions have various reasons for infiltrating an organization and do not necessarily focus on a single vertical. Any organization that makes something that is perceived to be valuable, has access to something valuable, or has a trust relationship with someone who makes or accesses something valuable can be (and very likely already is) a target.

Rather than dismissing intelligence about a particular threat group because it has not been observed targeting organizations in the same vertical, IT and IT security professionals should ask themselves instead, "If these techniques, tactics and procedures (TTPs) were used in an intrusion against my company, would we detect them?"

Here's why. Our Counter Threat Unit (CTU) researchers use data obtained from targeted threat response engagements to identify patterns and trends in adversary operations. In one example that addresses the prioritization question, intrusions attributed to Bronze Faculty (Bronze Faculty — a Secureworks™ designation) were plotted over time and by industry vertical. The findings revealed Bronze Faculty playing a game of "vertical hopscotch."

While the data used only represents Bronze Faculty activity observed by CTU researchers, it demonstrates that threat groups victimizing a particular vertical today may infiltrate new verticals tomorrow. Organizations should never dismiss the threat from groups that seem to only target other verticals. CTU researchers recommend carefully mapping threat group tactics, techniques and procedures (TTPs) to security controls and planning mitigation strategies as feasible.

The Secureworks Counter Threat Unit™ (CTU™) is composed of more than 85 top threat researchers recognized for their expertise in countering cyber threats. It is the intelligence developed by the CTU that supports all aspects of Secureworks operations and services.

2. How do we know when we're successful against a threat?

The threat actor will, by their own behavior, telegraph your success. From our engagements, we see threat actors universally try to get right back into the environment when they first realize they have been removed. Being able to kick out the actor and then observe their failed attempts to reenter the environment is often a clear signal you've carried the day.

Other general indicators for winning often include:

- You've reduced the Time-to-Detect window
- You've reduced the Time-to-Respond window
- You've increased your organization's ability to combat threat actors in the future

Regarding this last bullet, the figure below illustrates the ability to consistently keep from being owned by D teams, then C teams, and so on. Winning also means your team is able to counter more and more sophisticated teams that may seek to exploit your environment, applications and data.

3. What does winning look like?

In this example, a client became aware of threats residing in its environment. The client worked with our Incident Response team for two months to improve its security posture and forensic readiness, culminating with an eviction of all threat groups by simultaneously executing a coordinated closeout plan.

The client saw the importance of planning and protective measures, and decided to move forward with an ongoing consulting engagement where our security and risk consultants would assess their environment on a regular basis. The next intrusion was identified in four days (versus five months). This substantially reduced the cost of responding from the last engagement. The client understood they would never be free of a threat group's attempt to infiltrate their environment, but could always control how they would respond.

4. How can we determine when a threat is targeted?

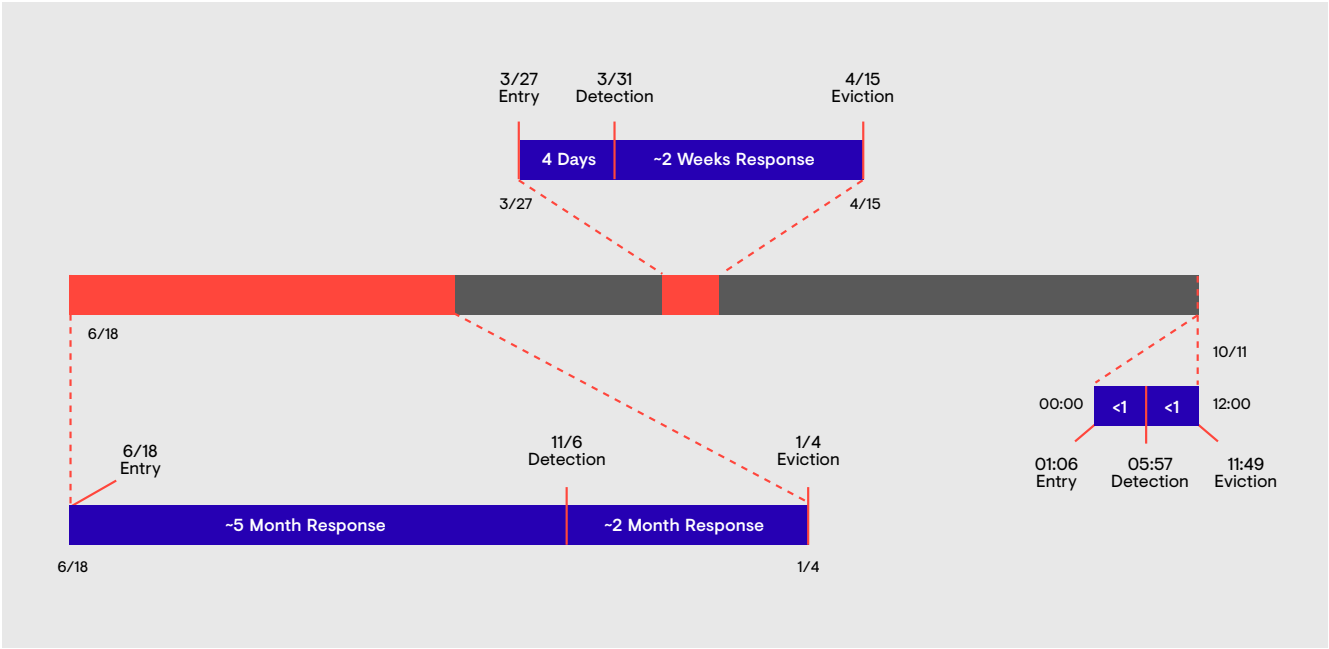
It is virtually impossible for organizations to determine at the outset whether a threat is targeted. As a result, security teams must consider every threat as potentially targeted. Organizations need visibility, context and experience to answer this question.

Visibility

The term "targeted" is relative and implies a distinction from normal, i.e., "common" or "un-targeted" threats. Understanding what is "normal" is a challenge for most organizations, whose instrumentation may only permit visibility within their perimeter.

More mature organizations often will supplement their visibility with publicly available reports or publications by security organizations, or they will participate in trusted communities, which share threat intelligence information among their members. This helps to extend their visibility beyond their borders. However, the visibility remains limited to what the group can observe and/or what they are permitted to share. Determining whether a threat is targeted presents a greater challenge for an individual organization to determine, based on the level of visibility possessed by its staff.

If you consider the MSSP model with thousands of clients across the globe, we can observe the threats impacting clients, representing a wide variety of industry verticals and multiple geographic regions. This broad visibility provides a baseline from which Secureworks can objectively determine when a threat is common to the threat landscape as a whole, common to specific verticals or geographic regions, or unique to a small pocket of clients, which may indicate a more targeted threat.



Context

All business decisions, especially decisions about risk posture and threats, involve making determinations of how to apply limited resources (time/money/people) to a given problem. Context is the key to making accurate and effective determinations and is a derivative of the organization's visibility. The greater the visibility, the greater the pool of information from which an understanding of the threat can be built.

In our case, Secureworks leverages its broad visibility to gain a comprehensive understanding, including the historical context of a threat, which can help identify the difference between a "rare" threat and a "targeted" threat. The historical context is critical for targeted threats. Response teams need to understand when and how the threat and threat actor gained entry, what the actor might have deployed, how the actor moved within the environment and, ultimately, whether the actor was successful in completing actions on objective (for example, exfiltration of sensitive data).

We have engaged adversaries directly in numerous Target Threat Hunting and Response engagements, allowing our researchers to build comprehensive threat actor/group profiles to help answer these critical questions and, ideally, prevent threat actors from achieving their objectives.

Experience

Targeted threat actors represent a more complex adversary because of the human element. This kind of actor is intent on bypassing security defenses and remaining in the environment undetected until they can achieve their objective.

For the security professional, first-hand day-in and dayout experience countering the tactics, techniques and procedures (TTPs) of the adversary is critical. Experience allows response teams to know where to look for clues, connect the dots and determine how best to respond. Experience also provides the context allowing response teams to identify changes in the actors' TTPs, which may indicate a response to stimuli introduced by defenders.

From our perspective, identification of new TTPs allows Secureworks' researchers to develop new methods of detection and response for deployment across our client base, providing for greater visibility into the threat. This allows researchers to use new information to retroactively hunt for indicators of compromise and inform the affected parties, who may be unaware of what is happening within their borders.

5. How do we protect our organization from threats where there isn't any prior knowledge of the threat (the "unknown unknowns")?

The first step is to baseline an environment in order to learn what expected operations looks like. We often find people don't know their network well enough to identify what's good, versus what's unknown and thus could be bad. While some threat groups will stand out like a sore thumb by making lots of noise in a network, others will work diligently to mimic known operations or leverage existing IT tools to conduct their operations. For example, threat actors have been observed using a company's endpoint management platform to move laterally and execute commands.

The process of hunting for threat actor tradecraft goes beyond searching for known static criteria like network and file indicators. It requires thinking like a threat actor who is trying to evade traditional security controls and identifying behaviors used to achieve nefarious goals.

6. What do you see as a top priority for new security investments in the next 3-5 years?

Simple. Endpoint security. Endpoint controls are not a passing fad. Though the nature and integration of these solutions are still evolving, their core capabilities – detection, forensic readiness and response – provide organizations a window into their endpoints, and an opportunity to reduce the time and effort required to respond to suspected breaches. It's worth the investment.

7. What are the top 3 improvement opportunities organizations can make to their security posture?

We see clear opportunities for improvement in the identification of your "key terrain," network segmentation and in the auditing of privileged account access and usage.

First, organizations need to understand what constitutes their "key terrain," i.e., the systems and data you would never want out in the open, and where they reside. It's very hard to build a resilient security architecture if security teams don't have key terrain identified and well understood. A lot of organizations we engage with can't answer the question of what constitutes their most valuable assets.

Second, organizations should segment their networks. Network segmentation allows you to segregate data from your users and, more importantly, your crown jewels from your users. For example, segmenting servers from workstations, or segmenting your network topology with regard to business functions such as HR and Finance.

Last, organizations should audit their privileged account usage. We find many organizations have no idea how many domain admin accounts they have and how they are used. This means a privileged threat actor could be operating freely in the environment. For those organizations that do monitor activity, we find they may log "denied" but not "accepts." Staff needs to log both.

Secureworks®

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

We combine visibility from thousands of clients, aggregate and analyse data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defence 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
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
UK House, 180 Oxford St
London W1D 1NN
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

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
www.secureworks.com.au

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