Secureworks®

WHITE PAPER

SecOps Hacks: 7 Small Ideas That Make a Big Difference for Cybersecurity Teams

"Without the nail, the horseshoe was lost. Without the horseshoe, the horse was lost. Without the horse, the rider was lost. Without the rider, the battle was lost. Without the battle, the war was lost. Without the war, the kingdom was lost. And all because of a nail."

- Old proverb

Little things mean a lot — especially when there is a big job to do, with limited resources and a lot of pressure.

While it's important for Security Operations Center (SOC) teams to get the big things right (having great sources of threat intelligence, implementing advanced XDR technology, driving adoption of multi-factor authentication), there are also many seemingly minor SecOps hacks that can have a significant long-term impact on team effectiveness and efficiency. Make no mistake about it, SOC teams must become more efficient. SOC analysts are in short supply, so it is imperative that we do everything in our power to optimize their work time.

Secureworks® has been operating an industry-leading SOC since 1999. We used that experience to purpose-build Taegis™ XDR, which is used by our own SOC staff, as well as the thousands of customers who trust Taegis and Taegis XDR. As part of our commitment to the cybersecurity community, we are sharing best practices discovered from those two-plus decades through seven SecOps hacks in this paper. For additional security tips be sure to visit the Secureworks blog.

SecOps Hack #1
Rigorously and consistently document Key Findings for all investigations

What to do

Every time SOC analysts engage in an investigation, they gather information and make assessments. They may also recommend actions that, once taken, require further assessment. All this investigation-related information, insight, and activity should be fully documented.

SOC analysts should therefore be rigorous and consistent about completing a Key Findings narrative for every investigation. To make sure that narrative is complete, Key Findings should always include the following components:

- An **Incident Summary** section that provides a short, concise overview of the investigated behaviors. This summary should simply provide the basic "what," "who," and "when" of the investigation, without extra details.
- A **Technical Details** section that tells the full story of what was observed—including all relevant alerts and alert details, snippets of code, netflows, persistence techniques, etc. To ensure that the content for this section is complete, it's helpful to clearly define the questions it should answer. Those questions can include:
  - What was the initial infection vector?
  - What are the capabilities of this malware/tool?
  - Did the attack succeed or fail in its objective?
  - Are any other hosts impacted?
  - Is there any evidence of network or phone-home connections?
  - Was the attack commodity/opportunistic or targeted?

- A **Recommendations** section that provides suggested guidance for remediating the subject of the investigation. See **SecOps Hack #3** for a more detailed description of best practices for this section.
- A **References** section that provides links relevant to the investigation. Links should be numbered so they can be accurately referenced in the Technical Details section. Reference links can include:
  - Vendors' explanations of relevant alerts.
  - Open-source intelligence regarding IP or URL reputation.
  - Online articles that explain specific malware or tool capabilities.
  - Information on specific CVEs and vulnerabilities that may have been exploited.
- Information on specific attack and persistence techniques that were used.

Why do it

Key Findings provide vital documentation for anyone working on the activity being investigated and for anyone working on future related incidents. They may also be applicable to compliance audits, legal discovery, and cyber insurance claims. A disciplined approach to the capture of "Key Findings" helps ensure that this documentation is always as complete as possible—while also making it easier for SOC analysts and others to quickly find the information they need, when they need it.

ProTip:

SOC teams should be diligent about footnoting any content in the Technical Details section of Key Findings with relevant reference links. This will be much easier to do if:

- Those links are always included in the References section.
- The links are always numbered in the References section.

SecOps Hack #2
Name investigations consistently and informatively

What to do

Every investigation that is initiated should be named in a consistent, informative manner—no matter who kicks it off. Useful elements to include in investigation names are the date the investigation was created, the purview of the Investigation, and the asset(s) of concern.

Here is an example of an investigation naming convention that has worked well for many SOCs:

- *<Date (YYYY-MM-DD) > - <Threat/Useful Name> - <Asset Hostname/IP>*

If an investigation involves more than one asset, "Multiple Hosts" can be used in place of the <Asset Hostname/IP> field. However, note that using a string like "Multiple Hosts" instead of a specific hostname, may affect the ability to search for investigations by name later.

Using this convention, investigation names might look something like this:

- *2021-10-31 - QakBot Malware Infection – 192.0.2.1*
- *2021-10-31 – Suspected Stolen Credentials – alicex@example.com*
- *2021-10-31 – Suspected Pentest – Multiple Hosts*

This is just one example of a naming convention. Any format that makes sense can be used. The key is to stick to it once it has been created.

Why do it

Investigations are a core SOC activity. By naming them consistently from the very beginning, it eases collaboration and prevents investigation overlap. Consistent naming also makes it easier to keep the investigations organized—which can come in handy when delegating tasks, managing team members' work queues, reviewing team performance, or searching previous investigations for insight that may be applicable to active ones.

ProTip:

To make sure that the team is abiding by the naming convention, briefly review all investigation names every quarter. Any investigations that were poorly named can be identified and the underlying cause(s) addressed. For positive reinforcement, there can be a team reward for achieving 100% (or close to it) conformance to the standard.

SecOps Hack #3
Pay special attention to Recommendations

What to do

SOC analysts often focus so much on the Incident Summary and Technical Details sections that the Recommendations section is too brief. That is why it is often necessary for SOC analysts to be especially diligent about ensuring that their Recommendations sections are clear and complete.

More specifically, SOC analysts should adopt the following best practices for this section:

- **Be clear.** Bear in mind that recommendations may need to be followed by someone who does not understand the technical aspects of the threat in question. So, make sure to take the time to explain the recommendation in clear, concise, and simple language that the reader can understand.
- **Stay focused on the investigation at hand.** It can be tempting to use the opportunity to educate a potential reader more broadly about threats, remedies, and other issues. But that excess information can be distracting for someone who must immediately take well-directed action. Confine the recommendations to actions that need to be taken now to remediate the issue and conduct a broader transfer-of-expertise at a more appropriate time.
- **Itemize all remediation objectives and associated follow-up actions.** Someone reading the recommendations will need to know exactly what they should achieve and how they should do so. Multiple objectives and actions may need to be conveyed especially if there is uncertainty about the exact nature of the suspicious activity. Make sure to itemize those multiple objectives and actions in an easy-to-read format, such as a bulleted list or table.
- **Raise potential consequences of follow-up actions, where appropriate.** Some of the suggested actions may be simple and straightforward. Others, such as restricting access privileges or taking a system temporarily offline, may have consequences that a reader should take into consideration before they perform them. Wherever possible, avoid assuming that the reader will intuitively understand these consequences. Instead, spell them out and provide (brief) context.
- **Reference reputable sources for remediation.** By referencing existing documentation from reputable sources, you can save a lot of work and provide the reader with a lot of potentially useful information on how to resolve the situation at hand.
- **Avoid canned/generic responses. It can be tempting to just cut and paste language from another document into the recommendations.** Be careful about doing this, because the recommendations should be concise and specific to the matter at hand. Also, as noted above, the better practice is to reference that material with a link. The reader can also be directed to a specific section or paragraph in the reference material.

ProTip:

Don't skimp on the Recommendations section just because the investigation is the result of authorized penetration testing (pentesting) activity rather than a real attack. One of the main benefits of pentesting is the opportunity it creates to see how quickly and effectively the organization's end-to-end threat response processes work, so treat pentesting the same as any other threat. Also, because pentesting often generates multiple issues in a short period of time, it's a great opportunity to stress-test processes with more "information traffic" between the SOC and IT than they are likely to experience under typical real-world conditions.

Why do it:

The time invested in ensuring that the Recommendations section is clear and complete pays off in three ways:

- It enables the reader to **implement the recommendations quickly and properly**, so that the threat can be neutralized as quickly as possible.
- It **saves the reader's time**—which may be quite limited—because they make fewer mistakes and don't have to go back to the SOC analyst with questions.
- It **saves the SOC analyst time**—which is definitely quite limited—because they don't have to answer a bunch of follow-up calls by the reader asking for clarification.

SecOps Hack #4
Implement suppression rules wisely and consistently

What to do

SOC analysts create alert suppression rules in an ad hoc manner whenever it appears that innocuous alerts are adding excessive "noise" to their dashboard "signal." Nonetheless, SOC teams should be disciplined and consistent about when and how they create those rules.

- **Double-check that the alerts under consideration are actually benign.** Some alerts, for example, are benign in most situations—but may nonetheless still have value under other conditions as an early indicator of certain types of threats. So, make sure candidates for suppression are evaluated for alert suppression in the context of all possible future scenarios.
- **Determine whether the alerts under consideration are occurring often enough to justify suppressing them.** Resist the temptation to view every trivial alert as a problem that needs to be solved with suppression.
- **Avoid rule duplication and overlap.** Don't create an entirely new suppression rule if modifying an existing one will satisfy the need. For example, an existing rule can simply be expanded to include another host or IP address—rather than creating an entirely new suppression rule.
- Keep track of rules that should be temporary, and routinely disable suppression rules that are no longer necessary.

Why do it

One reason to be careful about suppression rules is obviously to avoid inadvertently suppressing alerts that indicate problematic activity. But, over time, SOCs can also create "rule bloat" that makes it more difficult to keep track of rules and their intended purposes. This bloat wastes the valuable time it takes to scroll through rules whenever:

1. Another alert is identified to be suppressed, necessitating a review of existing rules to see if one can simply be extended rather than writing an entirely new one.
2. There is a need to review existing suppression rules because one may have inadvertently been written too broadly, and is therefore removing potentially important information from dashboards.
3. Another SOC analysts' rule needs to be peer reviewed (see **SecOps Hack #5**).

Being more disciplined about suppression rule creation can save time, and avoids the headaches associated with rule bloat.

ProTip:

Consistent, informative naming of suppression rules will provide the same benefits as the consistent, informative naming of investigations. Useful elements to include in suppression rule names are:

- The purview/scope of the rule (what the rule is matching on)
- What the rule suppresses (the alert name or a brief description of an activity)
- The specific asset being targeted, if there is one (hostname or IP address)

Here is an example of a suppression rule naming convention that has worked well for many SOCs:

- <Threat/Alert Name/ Description of Activity> from <Asset Hostname/IP>

Using this convention, the names of the suppression rules might look something like this:

- Authorized Vulnerability Scanner from 192.0.2.1
- Guest Network Range - 192.0.2.1 to 192.0.2.59
- Authorized Process Execution d597850f62c02287 cd5a6869544b3e06

And remember: If a suppression rule gets modified, the rule's name should also be modified to reflect the change.

SecOps Hack #5
Peer review

What to do

Peer review is an essential aspect of SOC team collaboration. In this example, we'll consider the peer review process for the kind of suppression rule addressed in **SecOps Hack #4** above.

Peer review simply means that, as a matter of routine, SOC analysts always request to have their proposed suppression rules reviewed by another analyst before activation. This is typically done using a collaboration platform such as Slack, Microsoft Teams, or Mattermost.

SOC teams should create a standardized template for these peer review requests. That template should include what the request is for, the name of the tenant, and a link to the rule. For example:

- Request Type: Peer Review Request
- Tenant: *<tenant name>*
- Rule Link: *<link to suppression rule>*

SOC teams should also establish a standard checklist for SOC analysts on the receiving end of peer review requests. In the case of peer reviews for suppression rules, that list might include the following:

- Match criteria to ensure the rule will match as intended.
- Negative match criteria to ensure similar but different alerts are not suppressed accidentally.
- Check the Description field to make sure proper documentation has been added.

If the reviewing analyst finds any errors, they should inform the creating analyst of the error, and if appropriate also suggest how it might best be fixed. After modifying the rule, the creating analyst should then resubmit the rule for another review.

Alternatively, a discussion of the rule may result in both analysts agreeing that the rule is not necessary, in which case it can be abandoned.

Once the reviewing analyst has confirmed the rule is accurate and necessary, they may proceed to enable the rule. The reviewing analyst should then let the analyst that created the rule know that the rule has been enabled.

Why do it:

While it's often counterproductive to duplicate work, it's also very important to avoid errors—even when it comes to what may seem like the trivial task of writing a suppression rule for an annoyingly common alert. Just as professional writers depend on editors to double-check their work, even experienced SOC analysts can make potentially costly errors when performing tasks such as writing rules or creating remediation playbooks.

ProTip:

If the reviewing analyst has questions regarding the function or justification of the rule, they should feel free to reach out to the creating analyst to discuss the rule in more detail. Text collaboration platforms are useful, but sometimes a five-minute conversation on the phone, via videoconference, or face-to-face can spare both parties a lot of time and frustration.

SecOps Hack #6
Use CyberChef to understand and analyze data

What to do

WARNING: *Only use the CyberChef tool that is hosted within Taegis XDR, or a locally hosted and controlled instance to avoid exposing customer data to an online tool.*

Originally developed by the British intelligence agency GCHQ, CyberChef is an opensource tool with a simple, intuitive interface for performing all kinds of operations and analyses relevant to a SOC analyst's job, including:

- Decoding an XOR- or Base64-encoded string.
- Decompressing gzipped data.
- Creating a SHA3 hash.
- Parsing an X.509 certificate to find out who issued it.
- Converting a timestamp to a different format.
- Parsing X.509 and IPv6 addresses.
- Converting data from a hexdump and then decompressing it.
- Decrypting and disassembling AES, DES, and Blowfish shellcode.
- Using parts of an input as arguments to operations.

CyberChef has drag-and-drop capability of files up to 2 GB that can be encrypted/decrypted or compressed/decompressed. It also allows saving and loading 'recipes' as well as many other powerful features. Every SOC and analyst should take advantage of this powerful tool.

Why do it

A primary responsibility of SOC analysts is determining what threat actors are attempting to do and how they are attempting to do it. Threat actors obviously want to make this as difficult as possible, so they employ a wide range of techniques to conceal and obfuscate their intentions. These techniques often entail encoding commands in XOR or Base64, encrypting files, and adding layers of complexity to their code.

By using CyberChef consistently, SOC analysts can more quickly and effectively get to the heart of threat actors' tactics to both counteract immediate threats in the short term and become more knowledgeable about their techniques-of-choice in the long term.

ProTip:

CyberChef is securely hosted and easily accessed directly within the Taegis XDR platform. It can be accessed from the Taegis XDR "Tools" menu. This makes it easier for SOC analysts to quickly examine threat artifacts as part of their investigations, add their discoveries into their Key Findings, and share their insights with their other team members.

SecOps Hack #7
Establish and stick to a consistent routine

What to do

Given the fast-paced and reactive life in a SOC there is a natural tendency to jump right into whatever task appears to be the most urgent at any given moment.

Experience shows that the best first task for any SOC analyst is almost always to start off with a review of new threat intelligence.

For Taegis XDR users, this means first checking the Threat Intelligence Reports Dashboard Panel on the Alert Triage Dashboard. This is where the Secureworks CTU™ publishes Threat Intelligence reports that include tips, Open-Source Intelligence Updates, and webcast information.

In addition, Secureworks Global Partner Advocacy releases CTU Special Advisory Statements as they become available in the Knowledge Base. It may therefore be helpful to review the Partner Knowledge Base | Threat Detections & Investigations | Threat Intelligence; or General | Announcements sections prior to moving to the first Alert or Investigation of the workday.

SOC analysts should apply this same routine/discipline to other tasks as well—including checking and responding to emails, checking into collaboration platform queues, responding to peer review of suppression rules, etc.

Why do it

SOC analysts live under a constant barrage of urgent demands on their time. So, while it may feel necessary to constantly re-shuffle one's personal task queue in response to those demands, the end result usually turns out to be chaos and burnout, reducing the effectiveness and efficiency of the SOC. By adopting routine practices such as checking for new threat intelligence at the start of the day, SOC teams can:

- Properly prioritize the upcoming day's tasks in the context of that day's cybersecurity realities.
- Avoid missing the emergence of a new threat requiring rapid Day One countermeasures.
- Get and keep the whole SOC team on the same page.
- Help instill a team culture of discipline that will pay off in other ways across the SOC's broader set of individual and collaborative tasks and processes.

ProTip:

The Secureworks CTU may release more than one Threat Intelligence report per day, so be sure to scroll through all new reports before responding in a panic to any individual one. If there are multiple analysts on the team, consider assigning a fixed time during the day for each SOC analyst to review the Threat Intelligence Reports Dashboard Panel for a second or even a third time.

Conclusion

SOC success isn't just about having great technical skills, it's also about consistently making the most of everyone's time and energy by developing strong work habits. Those habits don't just help SOC teams better safeguard the organizations they're hired to protect, they are also key to every SOC analyst's personal development as a cybersecurity professional. SOC staff need to embrace discipline and consistency. The results will show in the SOC team's work and psychological well-being.

One measure of a good tool is how readily its creators implement it into their own processes. That is why the Secureworks SOC uses the very same Taegis XDR solution that we provide our customers for our own extended detection and response needs and to protect our ManagedXDR customers. With capabilities that reduce risk, maximize existing security investments, and fill talent gaps that all organizations face at times, Secureworks has put its own solution to the test internally. Taegis XDR leverages the Taegis cloud-native platform, continuously gathering and interpreting telemetry from proprietary and 3rd party sources alike – including endpoints, networks, cloud, and identity systems. This technology automatically identifies and prioritizes threats, enabling SOCs to enact faster and more confident responses.

To learn more about Taegis XDR visit www.secureworks.com/taegis. For more security insights visit the Secureworks blog page at www.secureworks.com/blog.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

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
Otemachi One Tower 17F
2-1 Otemachi 1-chome, Chiyoda-ku
Tokyo 100-8159, Japan
81-3-4400-9373
www.secureworks.jp