A SANS Whitepaper

A SANS 2021 Report: Top Skills Analysts Need to Master

Written by **Ismael Valenzuela**

April 2021

Sponsored by:

DomainTools

Introduction

As more organizations invest in improving their security operations—either by building their own security operations centers (SOCs) or by engaging managed security services—the demand for security-related roles is higher than ever. It reached 3.5 million unfulfilled positions in 2021, according to a Cybersecurity Ventures jobs report[1]

But from all of the cool jobs in the security industry, security analysts stand out from the rest. In the United States alone, the U.S. Bureau of Labor Statistics reports that information security analyst jobs are projected to grow 31% from 2019 to 2029, much faster than the average for all occupations.[2] As one of the highest-paid jobs in the field, security analysts must become masters of all trades, essentially "all-around defenders" who are highly competent in threat detection, while also possessing excellent analytical and communication skills. But what are the technical and nontechnical skills required to acquire mastery in this role? And how can industry security solutions augment analysts' capabilities to become more effective?

To answer these questions, this report will first explore what makes a security analyst successful. This critical step is often overlooked. That can lead to the wrong expectations for both analysts and employers, thus resulting in higher attrition and burnout. Next, we will examine the top skills security analysts need to master to be effective at defending organizations across endpoints, networks, and the cloud, as well as aligning to the models presented in the report.

[1] "The Mad Dash to Find a Cybersecurity Force," www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html

[2] www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Analysts Are “Time Machines”

In his book, “Your Brain Is a Time Machine,” neuroscientist Dean Buonomano explains how the human brain is continuously making real-time predictions, not just of “what will happen next” but also of “when it will happen.”[3] To do so, with memory and cognition, our brains become time machines: We can travel back and forth in time.

Time has always been a critical component of warfare, and cybersecurity is not an exception. A security analyst, as an all-around defender, is in a constant battle where time is a critical factor.

However, our product-centric industry often drives security professionals to focus too much effort on learning tools and technologies, without paying enough attention to the quality of their analysis. In fact, one of the most important skills successful analysts need to acquire is to understand when and why certain tools or products must be used. Understanding this can make a difference between winning or losing the battle against an adversary that is attacking an organization.

> *“The brain only has two purposes: to remember what it has sensed from its environment and to anticipate (predict) the future.”*
>
> —Dean Buonomano[4]

Fortunately, analysts can use several security models and frameworks to develop and improve their skills. Some of the more effective ones are:

- **MITRE ATT&CK®** is a framework that all analysts should be familiar with, because it allows us to know the adversaries we are defending against.[5] The MITRE ATT&CK Matrix for Enterprise can be seen as a chessboard. Every square in the board can be compared to an attacker’s tactics, techniques, and procedures (TTPs)—a specific movement or a combination thereof—at one moment in time. It can be argued that thinking like an attacker can help analysts predict the future, or anticipate possible movements to a certain extent, making them better defenders. But becoming familiar with attackers’ behaviors also helps analysts understand what happened in the past, allowing their brains to become time machines, traveling back and forth across an attack chain. Although ATT&CK provides a language to describe attackers’ behaviors, it doesn’t provide a language or a taxonomy to describe defenders’ actions and thinking. The following models helps us to describe those.
- **Time-Based Security (TBS)** provides a methodological, quantitative, and mathematically proven method to understand how much security a product or a technology provides by answering questions such as:

  a. How long are systems being exposed?

  b. How long before we detect a compromise?

  c. How long before we respond?[6]

[3] “Your Brain Is a Time Machine,” Dan Buonomano, (W.W. Norton & Co, 2017)

[4] “Your Brain Is a Time Machine,” Dan Buonomano, (W.W. Norton & Co, 2017)

[5] https://attack.mitre.org

[6] “Time Based Security,” https://winnschwartau.com/wp-content/uploads/2019/06/TimeBasedSecurity.pdf

This simple model is essential for security analysts to understand the importance of time in their day-to-day jobs. While TBS can be used to assess the efficacy of security architectures, it also puts the emphasis on the efficacy of the detection and response process that analysts are part of in the SOC, stating that when it takes longer to detect and to respond to an intrusion than the amount of protection time afforded by the security measures—that is, if P < D + R—then the attacker wins. See Figure 1.

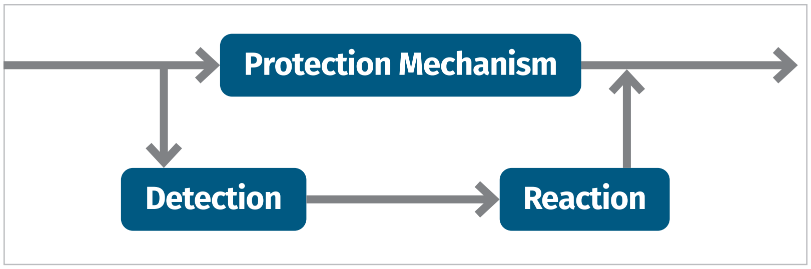

Figure 1. Time-Based Security Model[7]

- **The OODA (observe-orient–decide–act) loop** originated in 1976, when U.S. Air Force Col. John Boyd published abstract concepts about gaining combat superiority in aerial fights. Boyd's key concept was that of the decision cycle—the now-famous OODA loop (see Figure 2).

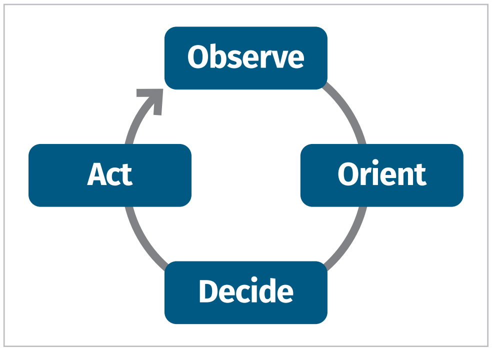

Figure 2. OODA Loop

In this model, Boyd postulated that victory is awarded to the combatant who is able to react most quickly. Both attackers and defenders operate under time constrains, but a defender who is able to react to changes in a dynamic environment faster than the attacker can gain a competitive advantage in that situation. Once again, we see how time is a critical factor to consider for any security analyst. The four steps of the loop are:

- **Observe—**Sense the environment, gather information, and survey the situation.
- **Orient—**Analyze the data gathered to form a hypothesis and obtain perspective.
- **Decide—**Develop an action plan for a situation based upon the previous phases.
- **Act—**Put the decision in motion.

The keys to this loop are the activities and critical thinking that take place in the orientation phase and the fact that it is an iterative feedback model that allows analysts to adapt their decision making based on the results of their analysis. Without feedback, an analyst won't be able to modify decision making in light of new evidence, new data, or previous experience.

[7] "Do you want to learn how to 'Blue Team'? Start with 'Time Based Security,'" www.linkedin.com/pulse/do-you-want-learn-how-blue-team-start-time-based-ismael-valenzuela

Fewer Tasks and More Critical Thinking

Security analysts are problem solvers, and solving problems requires specific skills. In fact, it can be argued that an analyst is essentially an investigator. An investigator also can be described as a thinker—someone who is inquisitive, methodological, and, yes, analytical. Investigative skills are essential in many professions, including journalists, statisticians, doctors, and archaeologists. How do they investigate, and can we learn those skills? The key to learning any new skill is to define it and break it down into logical steps, establishing a progression that can be followed and repeated systematically. The process of investigating is no exception and can be effectively explained in this manner.

Investigative Tasks vs. Investigative Thinking

To understand the process of investigation, it is necessary to make a distinction between investigative tasks and investigative thinking, also known as *creative thinking*. Investigative tasks relate to the information-gathering process that feeds into creative thinking (e.g., OODA loop), the process of analyzing information and creating theories or hypotheses to develop an investigative plan. Let's consider the sub-processes that are part of each of them and the skills that relate to them, as follows:

> *"In solving a problem of this sort, the grand thing is to be able to reason backwards."*
>
> —Sherlock Holmes[8]

- **Investigative tasks—**These duties are common across several cybersecurity roles. SOC analysts, forensic analysts, incident responders, and threat hunters perform tasks related to identifying evidence, gathering information, collecting evidence, and, in many cases, preserving evidence. The main difference among the roles is where the process starts. Whereas SOC analysts typically start off their investigations from an alert, threat hunters start their work from hypotheses or questions.
    - What are some of the critical skills that analysts need to master in this category? Most are related to data collection and transformation. Programming and automation skills are critical to gather data from networks, endpoints, applications, and other log repositories such as security information and event management (SIEM) or data aggregation tools. These skills are useful for manipulating data at scale as well. Learning a programming language that is readily available across multiple platforms, such as PowerShell or Python, can be of tremendous help, as can OS-specific command-line scripting, such as Bash.
    - On the network side, having the ability to capture traffic with tcpdump, Wireshark, or other network traffic monitoring tools will be helpful in many circumstances where the network may add important evidence to our analysis.

[8] "A Study in Scarlet" Arthur Conan Doyle, (Ward Lock & Co., 1887)

- **Investigative thinking—**Unfortunately, as mentioned earlier, analysts spend too much time performing investigative tasks and very little time on critical thinking or investigative thinking. Imagine how ineffective a detective who only collects evidence—but never analyzes it to draw conclusions—would be! This is why many analysts end up operating in autopilot mode rather than implementing the recurring phases of the OODA loop.

  Instead, security analysts must make use of investigative or critical thinking. Critical thinking can be honed by developing skills aimed at analyzing the information collected, developing theories about what happened and the way events occurred, leveraging context and intuition, and establishing reasonable hypotheses. How can analysts do that? First, we must take time to reflect on how we make decisions based on what we see and hear. This implies having a skeptical mindset with the aim of exploring all alternatives as objectively as possible.

  Best practices for analysts include:

  - **Ask questions.** Humans learn through questions, and investigators solve cases through questions too.[9] For many years, investigators from the CIA and law enforcement have used the Analysis of Competing Hypotheses (ACH) model.[10] ACH is an analytic process that identifies a set of alternative hypotheses and assesses whether data available are either consistent or inconsistent with each hypothesis. The hypotheses with the most inconsistent data will be rejected. Through asking questions, an analyst carefully weighs evidence and considers alternative explanations or conclusions. This structured method helps an analyst overcome, or at least minimize, some of the cognitive limitations common in many SOCs. This scientific method of employing questions and hypotheses is not new to many of us in digital forensics either. Many security professionals and researchers have written about using this approach in the cybersecurity field.[11] While an experienced analyst asks more questions up front, earlier in the investigative process, newer ones tend to make assumptions and start making decisions and taking actions without much questioning. Most of the time, investigations start with broad questions that eventually lead to more specific questions that can take us to the discovery of further evidence. Those questions allow us to gather additional context and scope when facing a situation of uncertainty during an investigation.

  - **Reason backward.** Reasoning backward from crime scene clues allowed fictional character Sherlock Holmes to discern the past events that brought about the clues. Similarly, reasoning backward allows an analyst's brain to be used as a time machine, reasoning over past events in concrete ways, hypothesizing about what must have occurred at each stage of the attack to arrive at the alert that is displaying in our security console. Because backward thinking is just a type of cause-and-effect thinking, knowing the logical steps of attacks by using models, such as Lockheed Martin's Cyber Kill Chain®[12] or MITRE ATT&CK, are key to supporting these inferences and deductions.

[9] "The Need for Investigation Playbooks at the SOC," https://content.sans.org/sites/default/files/2021-03/The%20Need%20for%20Investigation%20Playbooks%20in%20the%20SOC.pdf

[10] "Analysis of Competing Hyphotheses," https://isc.sans.edu/forums/diary/Analysis+of+Competing+Hypotheses+ACH+part+1/22460

[11] "How Analysts Approach Investigations with Diagnostic Inquiry," https://chrissanders.org/2016/05/how-analysts-approach-investigations

[12] www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

- **Don't think linearly.** It's been said that attackers think in terms of graphs, while defenders think in terms of lists.[13] This refers to the fact that many security analysts rely on static and linear playbooks to respond to threats. Although response playbooks can be helpful when responding to known threats, many times analysts are faced with new events, challenges, and puzzles that have not been seen or solved before. This highlights the need for analysts to think critically and to consider one or more plausible pathways using the tools and methodologies described in this report.

- **Be detail-oriented, fight unconscious bias, and don't miss the gorilla.** Attacks can be difficult to spot in highly dynamic environments like our networks. In cognition-intensive jobs, it can be easy to focus our attention on certain things, while missing fully visible but unexpected events. This is called *inattentional blindness*. A well-known example of this is the "invisible gorilla" experiment developed by Daniel Simons and Christopher Chabris in 1999.[14] In it, study participants are asked to watch a video in which two teams, one in black shirts and one in white shirts, are passing a ball.[15] The participants are told to count how many times the players in white shirts pass the ball. Midway through the video, a gorilla walks into the scene, stands in the middle, pounds his chest, then exits. When study participants are asked if they saw the gorilla, more than half of them acknowledge that they missed it entirely. So as to not miss similar invisible gorillas, information security analysts must pay careful attention to the systems they're investigating and watch for deviations or changes in behavior or performance. Taking notes on each step of the investigation and using methods such as ACH can help fight inattentional blindness as well as unconscious biases.

- **Be like a kid—curious and flexible.** Curiosity is probably one of the most important skills an analyst must continually foster and cultivate. Being curious can help a security analyst to be intrigued, pull threads, explore, and ask questions (instead of merely reacting in autopilot mode). One way to cultivate curiosity is to develop interdisciplinary skills. Many great analysts don't have a formal background in computer science or engineering, and come instead from other fields related to arts, for example, or enjoy hobbies that have little to do with technology. This provides them with a wider set of experiences that helps them to perceive the world differently, through a different lens, and that helps them to see outliers. Finally, kids are also flexible. They are not ashamed of changing their mind or accepting that they don't know everything. On the contrary, they're usually flexible enough to adapt and learn. Security analysts also must be ready to learn and adapt (again, think about iterative feedback in the OODA loop). Just like in aerial combat, the keys to gaining advantage in any arena are flexibility and agility within highly dynamic environments.

[13] "Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win." https://github.com/JohnLaTwC/Shared/blob/master/Defenders%20think%20in%20lists.%20Attackers%20think%20in%20graphs.%20As%20long%20as%20this%20is%20true%2C%20attackers%20win.md

[14] "Hunting Adversaries with Investigation Playbooks & Open CNA," https://www.youtube.com/watch?v=8qM-DnmHNv8&t=1s

[15] www.theinvisiblegorilla.com/gorilla_experiment.html

Investigations and the OODA Loop

At this point, it should be obvious that critical thinking skills as well as models such as the OODA loop and TBS help us to become better security analysts. Table 1 summarizes some of the top skills security analysts must master to be effective at defending their organizations across endpoints, networks, and the cloud. As you go through this table, think about this: How long does it take me to go through each of these steps, and how granular do I need to get at each point in the loop?

Table 1. OODA Loop Top Skills

Critical Thinking and OODA Loop	Description	Goal	Questions	Analyst Techniques and Skills
Observe	Every investigation starts with an observed event. This is often an alert coming from a security system such as an endpoint solution, IPS, or SIEM—but it can also be from endpoint, network, cloud, or application performance tools, or in the form of a call or some other sort of escalation or notification.	To leverage enough monitoring "sensors" across endpoints, networks, clouds, and applications to identify anomalous behavior that warrants investigation.	What happened? Is the attack real? Is the attack still occurring? What's the priority? Where is it occurring? Was there any response? Was it appropriate? Who are the users and what systems are involved? What do we know about them? Is this common or uncommon activity?	**Data gathering—**Automation and programming (e.g., PowerShell and Python). **Documenting and sharing—**Results of our investigation.
Orient	John Boyd identified orientation as our way to survive and grow within a complex and ever-changing world. This could also be identified as converge and understand.[6]	To contextualize our observations and make logical connections to understand what has happened; to identify what is vital and what is not to your investigation; and to identify biases and what evidence is missing that can impact decision making.	Are we missing anything? What are the relationships? What are the different perspectives or hypotheses? How does this relate to my knowledge of adversaries' behaviors and TTPs? How does this relate to my knowledge of the business, the assets and the data I'm defending? What is the prevalence of this artifact locally and globally? How much data do I need to add or remove to my analysis to increase/decrease the granularity of my orientation?	**Pivoting—**Using a field of interest from one data source to search in a different data source (e.g., searching an IP address found in an IPS alert on your endpoint detection and response). **Synthesis—**When we analyze something, we break a problem apart, but when we synthesize, we put the pieces together again to create something new that perhaps didn't exist before. That's how we obtain more than knowledge; we develop understanding. For example, an analyst can orient an investigation by synthesizing disparate log files to widen and augment analysis. **Data exploration—**Basic data science skills, including statistics, Excel pivot tables, and Python and Pandas DataFrames to perform aggregation, expansion, reduction, and data visualizations (e.g., aggregating all user_agents found in gateway logs, sort on unique values and perform long-tail analysis). **Documenting and sharing—**Results of our investigation.
Decide	To decide among the alternatives identified in the orientation phase. This can help us predict or anticipate the adversary's next move.	Using the ACH model, an analyst would rule out the impossible hypothesis and focus on the most plausible one, based on key evidence vs. less relevant artifacts. You will challenge and verify your assumptions, trying to fight bias, but remain aware of the danger of paralysis by analysis.	What evidence will disprove any of these hypotheses? What evidence am I missing that could make any of these hypotheses true? What is the best course of action to mitigate impact and contain the threat? What action will lead to the fastest recovery?	**Analysis of Competing Hypotheses (ACH)—**Seeking to disprove a hypothesis is usually a faster route than trying to prove a hypothesis, because we can never be sure we have all possible evidence available for analysis. **Reductio ad absurdum—**Assume a statement to be true and see what conclusions you can discern from it. If you find you get a contradiction, you know the initial statement is false. **Playing devil's advocate—**Here you are trying to prove the opposite of what you theorized and disprove the hypothesis considered. Essentially, you are trying to prove the limitations of your analysis. **Documenting and sharing—**Results of our investigation.
Act	According to Boyd, actions should be rapid, surprising, ambiguous, and ever-changing.	To carry out your decision, knowing that the adversary might be watching your actions; to learn and improve detection, investigation, and incident response processes by incorporating the feedback loop.	What did I learn in this cycle? How can we augment our prevention, detection, and response efficacy? What type of internal and external feedback did I receive? How can I use this feedback to improve my OODA loop when the cycle starts again?	**Automation tools—**Use to decrease response time. **Coding skills—**Able to use and customize **response playbooks** to the analyst's environment (e.g., SIEM/SOAR, XDR and other **automation tools**). **Documenting and sharing—**Results of our investigation.

[16] "The Critical Thinker's OODA Loop," https://jamieschwandt.medium.com/the-critical-thinkers-ooda-loop-6a69e878c153

Analysis Is a Human-Machine Teaming Effort

"Harvard Business Review" refers to AI as "the most important general-purpose technology of our era" and compares it to the internal combustion engine in its ability to reshape everything we do and transform every industry, including cybersecurity.[17] However, automation and current AI solutions depend upon a human observing and understanding a threat, then building a model or writing code. The time gap between the human observing a phenomenon and the machine helping is the reason why attackers often have the upper hand.

Although that cycle will certainly shorten over time, the truth is that even with the rise of AI, analysts will continue to be needed as much as we will still need doctors and criminal investigators. The difference is that those new AI systems will continue to learn and interact directly with practitioners at the SOC rather than replace them, so the security analysts can focus on what humans are best at: intuition, context, ethics, creativity, and strategy. Machines will improve the search for and collection of information, summarization, pattern matching, generalization, and hypothesis testing, in what the industry has named "human-machine teaming."[18]

In this new era of cyber defense, it will be key for vendors to provide solutions that can help transform the data in a way that can augment analysts' cognitive skills, taking directional feedback from them, organizing high-context data sources in a way that augments analysts' performance, and learning by observing their work. For example, an expert system could learn how to reduce false positives in real-time monitoring by dismissing the alerts that humans have investigated and dismissed in the past. These types of solutions will continue to empower security analysts to perform highly cognitive tasks, resulting in faster OODA loops, faster detection and response, and ultimately a more effective defense.

[17] "AI Is the Future of Cybersecurity, for Better and for Worse," https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse

[18] "Human-Machine Teaming Systems Engineering Guide," www.mitre.org/publications/technical-papers/human-machine-teaming-systems-engineering-guide

Conclusion: Analysts Are Not Born, They Are Developed

Contrary to what many may think, no one is born a security analyst. A security analyst is essentially an investigator, and investigators are critical thinkers. Much of the shortage we have today is due to the heavy emphasis the industry places on tools and technologies vs. the thought processes or skills required to investigate.

The good news is that critical thinking is an ability that can be learned. We can and we should encourage the development of these skills. As this report has highlighted, investigations have clear and defined processes that can be explained and depend on skills that can be acquired. Security models such as TBS and the OODA loop are good starting points to understand the mindset and the skill sets needed to be a successful analyst. Hands-on training that emphasizes analysis and critical thinking will help shorten the time needed to develop these skills.[19]

Organizations also can foster a culture of analysis and help grow these skills through internal defend-the-flag exercises, forensic challenges, and purple teaming exercises that simulate specific attack and defense scenarios, generating datasets for analysis. Finally, cybersecurity vendors can help address the gap by providing solutions that augment analysts' cognitive skills and implementing human-machine teaming concepts.

[19] www.sans.org/blue-team

About the Author

Ismael Valenzuela is co-author of the cyber defense and blue team operations course, SANS SEC530: Defensible Security Architecture and Engineering. Ismael is a senior principal engineer at McAfee, where he leads research on threat hunting using machine-learning and expert system-driven investigations. Prior to his current role at McAfee, Ismael led the delivery of SOC, IR and forensics services for the Foundstone Services team within Intel globally. Before that, Ismael worked as global IT security manager for iSOFT Group Ltd., one of the world's largest providers of healthcare IT solutions, managing their security operations in more than 40 countries. Ismael has participated as a security professional in numerous projects across the globe in the past 20 years, including as the founder of one of the first IT security consultancies in Spain.

Sponsor

SANS would like to thank this paper's sponsor:

DOMAINTOOLS®