For: Security &
Risk Professionals

Security Operations Center (SOC) Staffing

by Ed Ferrara, August 2, 2013

KEY TAKEAWAYS

The SOC Is A Complex And Sometimes High-Pressure Environment

The SOC is an orchestration of activities, skills, processes, and procedures much like a symphony orchestra. Technology is not enough; it takes a very dedicated and talented team of analysts and engineers to interpret what the technology is telling them to successfully protect against a growing list of cyberthreats and regulatory requirements.

The Best Analysts Have A Portfolio Of Skills And Talents -- Hard And Soft

Good SOC analysts have a long list of skills and personality traits that make them successful. Key attributes include technical expertise, intelligence, curiosity, flexibility, patience, passion, and fortitude. All SOC analysts take pride in their technical skills, but the best also recognize the need to work well with customers and colleagues.

Staffing A SOC Is A Challenge -- But You Can Find Skills In Unlikely Places

In today's competitive cybersecurity talent market, finding qualified staff can be difficult. However, you can find SOC engineers in the most unlikely places; SOCs employ former lawyers, salespeople, financial advisors, and network engineers. When evaluating candidates, prioritize personality and professionalism as much as technical chops.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617.613.6000 | Fax: +1 617.613.5000 | www.forrester.com

Security Operations Center (SOC) Staffing

People Make The SOC Successful

by Ed Ferrara
with Christopher McClean, Rick Holland, and Thayer Frechette

WHY READ THIS REPORT

Building and operating a security operations center (SOC) requires massive investment and difficult decisions, and one of the critical gating factors of success is skill availability. While technical experts and software vendors have done great work building solutions, a SOC is nothing without the right people. We interviewed more than 30 MSSP professionals to determine the best traits to look for in a SOC analyst. We considered several factors in our interviews, including experience, training, personality, character, temperament, and hard technical skills. We also considered the personal and professional growth of these individuals, including career development, mentoring, and job satisfaction. Across all of the people and companies we spoke with, clear patterns emerged. This research describes these patterns and serves as a guide for hiring a SOC analyst or engaging a managed security firm and judging the quality of its people.

Table Of Contents

Notes & Resources

Forrester interviewed more than 30 MSSP professionals to determine the best traits to look for in a SOC analyst.

Related Research Documents

The Forrester Wave™: Emerging Managed Security Service Providers, Q1 2013
January 8, 2013

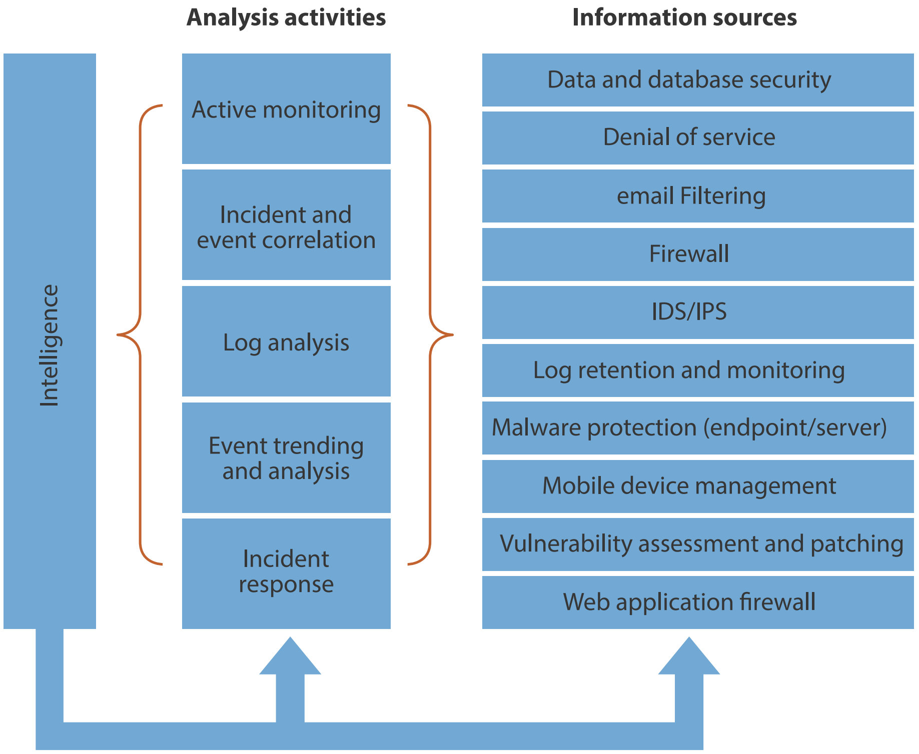
Understand The State Of Data Security And Privacy: 2012 To 2013
September 20, 2012

Recruit And Retain An Information Security Team
June 14, 2012

THE SOC IS A COMPLEX AND OFTEN HIGH-PRESSURE ENVIRONMENT

During security incidents, the SOC staff is under serious pressure to quickly identify the nature of an attack, determine its source, and mitigate the threat. Input comes from a large number of sources, including intrusion detection systems (IDS), intrusion protection systems (IPS), system logs, network proxies, databases, servers, routers, and switches (see Figure 1). Things can happen quickly, and the speed and accuracy of event detection and response can mean the difference between a large financial loss and public relations fiasco and a minor event that will quickly fade from public view.[1]

Figure 1 SOC Activities



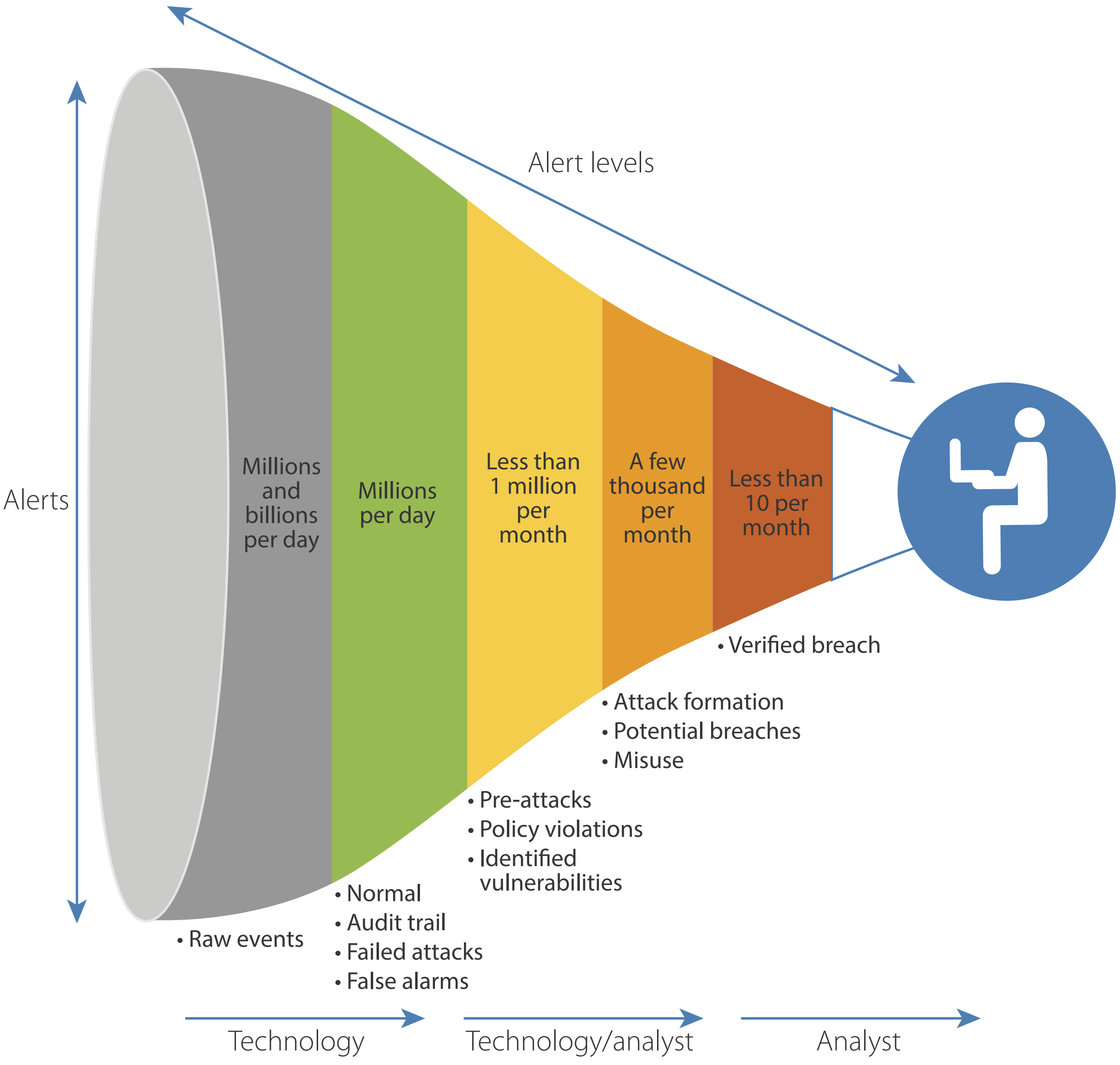
95241 Source: Forrester Research, Inc.

Billions Of Threat Events Are Funneled Into The SOC, Requiring Human Analysis

Visiting a SOC is impressive. Large 80-inch screens line the walls, each with its share of bar charts and graphics. The workspaces for the employees have the same look and feel as the operations center for the NASA Mars rovers.

Behind the scenes, SOCs deploy security event correlation and management (SECM) technology with sophisticated behavioral analysis to detect advanced persistent threats (APTs), insider attacks, and other malfeasance.[2] And although these systems are better than ever at reducing false positives and negatives, analysts still need to review the alerts generated by these systems and make the right call — potential breach, breach, or no breach (see Figure 2). The best detection and response method is still proving to be good "old-fashioned" human intuition and deductive reasoning. The SOC analyst still needs to look at the multitudes of data streams and alerts, filter out all the noise, and ultimately determine: "Something doesn't look right."

Figure 2 The Information Security Alert Funnel



95241 Source: Forrester Research, Inc.

STAFFING THE SOC IS A CHALLENGE

Finding the right staff, with the right training and experience, remains a challenge. There is an estimated shortage of more than 600,000 skilled security professionals worldwide, which creates a distinct problem for all companies hoping to build an effective security team.[3] Finding or building the correct blend of traits — curious, suspicious, dogged, and thoughtful — is especially difficult, with organizations of all sizes and industries aggressively competing to do the same.

This challenge largely stems from the specialized nature of the job. The work is part science, part art form. Sometimes called cybersecurity tradecraft, the process is a methodical and systematic approach to identifying and mitigating cyberthreats, and every SOC uses a similar process.[4] The best SOC analysts think like their adversaries and train to counter threats and attacks using a combination of inductive and deductive reasoning as well as great technical knowledge. In some ways, you're looking for the cybersecurity equivalent of George Smiley and MI6's "The Circus," popularized in John le Carré's famous spy novels.[5]

You May Be Surprised Where Talent Comes From

There is no single place to find the right people for the job. There is also no specific technical or professional certification that will tell you if a person will excel. Technical capacity is at the root of success and is a fundamental requirement, but how an individual has gained or will gain this expertise differs dramatically. Forrester studied the SOC staff within some of the best-managed security service providers (MSSPs) to determine what makes them successful and found great analysts with a wide range of backgrounds and experiences. For example:

- **Mike Pagel from Solutionary dabbled in a little bit of everything.** Mike, like many others in security, tested several other fields before jumping at the opportunity to pursue this longtime interest. "When I went to college, security was not an option. I came into security by complete luck. There was a seven-year gap between my college experience and the start of my security career. I tried a lot of things before this. My brother owned his own computer business — I worked there for a while, and then I dabbled as a financial advisor, and dabbled into a few other things and then took the one chance to get back into the computer field."

- **HP's Brett Hornick was a bored architect.** Numbers never lie, and in this case they told Brett that his data processing skills would serve him well in the security field. "I took a lot of architecture classes in school. I thought I might have wanted to be an architect. In class I would draw multidimensional pictures, of a screw for example — I got bored with that. I then went into accounting and also took a lot of math courses. I started using computers in math class and fell in love with electronic data processing (EDP)." Brett went on to tell us that he later "fell in love" with the security space. He's now more passionate than ever to be working in the SOC and doing something that is intellectually challenging and that he believes is making a difference.

- **Justin Lachesky of Lockheed Martin was a management trainee.** Justin just fell into the SOC. He joined Lockheed Martin's Rotational Leadership Development Program in engineering, communications, and finance. This was an early career opportunity that allowed Justin to rotate through different parts of the business. Justin explained to us that he was looking for an opportunity to do more project management and was interested in how Lockheed Martin provided cybersecurity. He explained: "As part of my leadership program, I joined the SOC product team, I learned the product, and I saw what the analysts were doing; I became really interested in that. I really like that we deal with hard problems and that there is also a human factor to it as well."

- **Dave Collison, a 31-year veteran of AT&T, used to be a salesman.** Dave is enthusiastic about his sales experience and the role it plays in his current position as a senior-level SOC analyst. "I would say that my background in sales has really helped with the job. I am very much a people person. I like talking to customers." Dave felt that he was sometimes more effective working with clients because of his sales experience. Dave is very technical but likes to put his soft skills in balance with his technical skills. Dave says of new candidates: "We are looking for a little bit of both technical and people skills, as someone [with only technical skills] may not be the very best to put with the customer."

- **IBM's Eric Hanratty was a Windows admin, video game buff, and roller derby referee.** Eric's system administration experience helped him transition to a full-time security role, which he found in IBM's SOC through relationships he built in the online gaming world. "I was doing Windows system administration and also played EverQuest with my current boss."[6] Talking with his future boss really got him interested in the SOC role, although it wasn't the first time one of his avocations introduced him to the industry. In the past, Eric had been a roller derby referee, and he found it funny that many people who played roller derby were also really into information security.

THE BEST ANALYSTS AND ENGINEERS HAVE A PORTFOLIO OF SKILLS

It takes a special person to be able to look at a series of apparently dissimilar events and make the call that an attack is in progress. This requires technical skill, intelligence, curiosity, flexibility, patience, passion, and fortitude. The best SOC analysts never stop learning — nor does the job let them if they're doing it right. Having a balance of skills is a big enough challenge in itself, but all the analysts interviewed said that keeping up with the "bad guys" was their greatest challenge and motivation.

Hard Technical Skills Are A Must . . .

There is a strong hands-on element to SOC work, and all analysts — from junior to senior — work very hard to maintain their technical chops. Most SOCs are organized into two operational groups. The first is the SOC operations team, which continuously monitors screens looking for potential anomalies that either the SECM technology detects or that they detect based on their own analytical skills. This group addresses tier 1 and 2 issues. The second is the incident response team, which addresses actual breach events. These engineers have more-advanced skills and are typically responsible for forensic investigation, advanced malware analysis, SECM rule updates, and training and mentoring more-junior staff. The best organizations have tight integration between these two groups (see Figure 3).

SOC engineers who become more experienced perform more-complex functions, such as forensic investigations, malware analysis, and the development and update of SECM correlation rules. Senior engineers also create and update threat response planning playbooks.[7]

Figure 3 SOC Analyst Emergency Skills

	SOC team	Advanced team
Activities	Tool administration Vulnerability scanning Tiers 1 and 2 event support	Forensics Investigation Tiers 3 and 4 support
Skill sets	Applications, attacks, chain of custody, compliance (HIPAA, PCI, others), databases, directories, ethics, IDS, IPS, investigative processes, multiple hardware platforms, malware (all types), network protocols (TCP-IP, MPLS, etc.), programming languages (Python, Perl, etc.), networking equipment (routers/switches/firewalls), and operating systems (Windows, Linux)	

95241

Source: Forrester Research, Inc.

. . . But Soft Skills And Proper Attitude Are Keys To Long-Term Success

In the past 10 years, the SOC engineer has largely been focused on implementing the right technologies, yet there has always been a need to complement these tools with talented security experts. There has been a tendency to gravitate to college majors, technical backgrounds, and certifications as indicators of desirable SOC talent. However, the real measurements for success can often be found within a SOC analyst's softer skill set. SOC engineers will put in tremendous hours, sometimes working around the clock to deal with a security event. Having the correct professional attitude when the business calls during a security event can make all the difference between ultimate success and failure. If the SOC team projects calm and confidence, the business client feels it has the right team working the problem.

FINDING, DEVELOPING, AND RETAINING THE RIGHT TALENT IS A TOUGH PROCESS

In any situation like this, employers have two options — hire junior people and build these skills, or hire experienced staff with the needed chops to work in the business. Success is measured in two ways: the ability of people to do their job and the retention of staff. Instill staff with the understanding that they're involved in activities that are bigger than they are. It's a big boost for the SOC staff to know they're making a difference.

Some people are cut out for working in the SOC, others are not; the analysts that find it's not a good fit opt out very quickly. The need for analyst skills is very high, and analysts have choices where they can work. However, retention may not be as difficult as you might think. All of the analysts we interviewed loved the challenge of their job, and it was these technical challenges and the ability to learn new things that kept them most engaged. Retention was clearly correlated with a growth in skills and experience — interestingly, salary was not as important. The best SOC analysts and engineers stand out because:

- **They have a strong drive to stay current with the latest technology.** Information security from a technical perspective is constantly changing. The fear of not staying current is ever-present in the SOC, and this fear was evident in everyone we spoke to, including managers and employees. The best SOC analysts and engineers constantly track security forums, manuals, and other information on the Internet. Some have security labs in their homes. The threats keep changing. The challenge is not in keeping pace with a known adversary, it's in understanding that what's true today may not be true tomorrow.

- **They have a wonderful sense of optimism.** Not a single person we interviewed for this report could see himself or herself doing any other career. They all felt "called" to be a part of security; it's not only a job, but also a vocation. Despite the constant stream of new bad actors and attacks, the SOC engineer has a real sense of pride in trying to fight the "bad guys." Despite nonstop threats, the SOC engineer upholds a positive attitude.

- **They have excellent customer knowledge.** When it comes to security threats and issues, there is a vast array of customers, from those that don't understand the ones and zeros to those that are technically savvy. These SOC analysts understand that as they begin conversations with a customer, it's important to determine why the customer is asking and what the customer wants. That way, they can tailor their service to what the customer wants.

- **They're adaptable and deal well with change.** Experienced hires come with preconditioned thought processes — that may include some baggage from their past employers. Experienced hires that have the ability to adapt to new processes are real finds. Dave Collison of AT&T, for example, says, "Ideally, you find the person that has the ability to adapt, because there are so many people looking for security skills. There is very little routine about this job." He believes that staying ahead of the "bad actors" means there is always something new every day, so "dealing with change is a very critical skill."

- **They're investigative and curious by nature.** Good SOC analysts are always questioning the environment and finding different ways to do things. The technology itself is mostly about detection. The bulk of what SOCs do is building analysis back into the system. The SOC analysts themselves must get to the bottom of every threat and discover new ways of detection and mitigation.

- **They collaborate well with colleagues and clients.** SOCs need a team that can come together quickly to address and mitigate the impact of threats to customers as soon as possible. The SOC engineer role requires the ability to communicate feedback, back and forth, among all of the team members. The staff has to be open, honest, and sometimes blunt when it comes to identifying where they think the problems lie. According to all those interviewed, the key to success is involving the team, helping team members feel they have input into their daily job, and helping them continuously improve.

- **They communicate well and maintain great client focus.** The ability to communicate can make the difference between success and failure. This is true for many jobs, but it's especially true in the highly pressurized SOC environment. The best SOC analysts and engineers can very quickly explain a situation as it unfolds to assure the best possible response. They can also explain complex security issues in nontechnical terms. One analyst described it as the ability to "visualize the issue" so that the client can understand what's happening.

- **They have an analytical mindset.** The explosion of big data requires that analysts develop an understanding beyond signature-based threats to identify abnormal behavior patterns and launch an appropriate investigation. This requires a continuous move toward analytics and away from a static mindset. It means an incredible level of dedication, reading, homework, labwork, and an intense ongoing pursuit of knowledge.

- **They have composure even in the most stressful moments.** Successful SOC analysts and engineers work under significant pressure during breach events. The ability to work under pressure and still maintain a professional demeanor is important for an analyst or engineer to remain effective during a breach event.

- **They have high confidence in their ability to solve problems.** The SOC engineer likes solving puzzles, such as Sudoku and the Rubik's Cube. This problem-solving nature translates well into figuring out how the bad guys are acting and for discovering patterns from malicious emails.

- **They love their jobs.** The security field has a tendency to attract and retain staff. And although burnout can be a problem, you wouldn't know it from the analysts we interviewed. Dave Collison of AT&T told us that he lives 90 miles from his office — "I commute 4 hours per day. I love my job. I could have had a job that was within 15 minutes of my home, but it was not in security. It was not what I was interested in." The field does a good job of finding very dedicated people that love their jobs.

- **They never give up, and they demonstrate an incredible amount of dedication.** The best SOC engineers never give up. They are tenacious. Many report working extraordinary hours to solve a problem or stop a breach. Since these professionals are dealing with many unknowns, and many days can bring new puzzles, the ability to push on through adversity is a great character trait and a sign of success.

ON-THE-JOB TRAINING TRUMPS FORMAL EDUCATION AND CERTIFICATIONS

Learning and collaborating among staff members — both formally and informally — is essential to forming a successful organization. When asked to give a breakdown of formal versus informal training in the security field, the majority of our interviewees saw the split at 70% on-the-job training and 30% formal training. There was 100% agreement from all we interviewed that the best teacher was experience and that working with more-experienced staff was the best way to learn:

- **Certification must be augmented with experience.** Certifications are good for candidate selection triage, but certification importance disappears over time. Having the skills is more important than having the certification itself. CompTIA Security+ and the (ISC)2 CISSP remain the most common, and perhaps, popular, certificates in the field; however, almost all of the staff interviewed were also pursuing other certifications, including Global Information Assurance Certification (GIAC), and vendor technical certifications such as Cisco, Dell SonicWall, HP ArcSight, and IBM Q1 Labs.[8]

- **Classroom training can't match hands-on experience.** Many of the firms interviewed for this research felt that some formal training was necessary. One, Lockheed Martin has a nine-week internship offered to employees and external candidates alike. Lockheed calls its center for security operations a Security Intelligence Center (SIC). This is because a key part of Lockheed's cybersecurity tradecraft is focused on using threat intelligence to recognize, track, and defeat attackers. The training immerses each student in a succession of complex exercises derived from real-life attack scenarios defeated by Lockheed's Cyber Intel analysts. Successful completion of the internship is a key requirement to becoming a Cyber Intel analyst at Lockheed Martin. Other firms provide incentives for employees to get advanced certifications in both technology and general security topics.[9]

- **On-the-job training is the best way to gain new skills.** Not all learning needs a formal teacher, but instead comes from a constant exchange of tips and tricks among team members. Michael Horsley of IBM reported: "I don't know that I would say that I have a mentor here. I don't know that I would call myself a mentor. But I do train people on a daily basis. We all train each other." Nothing builds confidence like experience.

- **Informal mentoring was ubiquitous.** Mentors can help create a comfort zone so that everyone feels OK asking any question at any time. Marcel Storms of AT&T told us: "As far as a mentoring program — I have had people that are mentors. They have walked down the road, so they have helped me. If you ever have a problem, I'm not afraid to call. I never feel like I am alone. They really make you feel comfortable. I have no problem critiquing my own work; bring a clean slate so they can help you mold you into a new process. If a person brings baggage as to how something is done, it can create friction."

- **Learning from others was expected.** A quality security team member can, at times, exude knowledge. Antony Gummery of HP spoke about how he learns. "I don't get a lot of mentoring myself. I watch everyone — I am always looking at how people conduct themselves. Those individuals that I am impressed by I try to spend as much time with as possible. I am always looking at my managers to learn. They love their job and their experience is a really good lesson."

WHAT IT MEANS

THE RIGHT PEOPLE MAKE YOUR SOC SUCCESSFUL

You will never find the dream team all at once, but with patience and persistence you can build a very competent and credible team. This will not be without cost, and taking the time to develop a qualified team may not meet your time frame for a successful SOC implementation. Not all companies will be successful in building a SOC and hiring the right staff. However, continuous monitoring is a core competency for all security organizations. Finding the right staff is critical if this function is to be successful. If you can't fully commit to the time and effort involved in building a SOC, outsourcing security is a very viable option, and the skills highlighted here are just as applicable when choosing your vendor.

SUPPLEMENTAL MATERIAL

Companies Interviewed For This Report

AT&T

HP

IBM

Lockheed Martin

Solutionary

ENDNOTES

[1] Organizations collect, create, use, and store information of all types, and this information has real value. Today, it's common to refer to information as gold, oil, or the secret sauce behind the business. Regardless, it's a target for cybercriminals, and the mishandling of data is a public relations fiasco waiting to happen. Personally identifiable information (PII) and intellectual property (IP) are the types of data that cybercriminals or unwitting employees are most likely to compromise today. PII fuels a lucrative underground data economy, and the demand for IP comes from both corporations and nation-states seeking to engage in espionage to cut innovation costs or get a leg up on the competition or adversaries. For more information, see the September 20, 2012, "Understand The State Of Data Security And Privacy: 2012 To 2013" report.

[2] SIM and SIEM are older terms that don't do justice to some of the newer technology providing security event detection and correlation capabilities. The term "security event correlation and management" (SECM) better reflects the nature of these next-generation security event correlation and management systems.

[3] The (ISC)2 2013 Global Information Security Workforce Study (GISWS) found that the shortage of skilled information security professionals is having a profound effect on the global economy, as it is leading to

more frequent and costly data breaches. Source: Michael Suby, "The 2013 (ISC)2 Global Information Security Workforce Study," Booz Allen Hamilton and Frost & Sullivan (https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf).

[4] Tradecraft is a term historically used in the intelligence community to describe the process of gathering and analyzing intelligence. Source: Center for the Study of Intelligence, Central Intelligence Agency, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," March 2009 (https://www.cia.gov/library/publications/publications-rss-updates/tradecraft-primer-may-4-2009.html).

[5] George Smiley is the name of the main character in John le Carré's famous spy novels. The most well-known of his novels is Tinker, Taylor, Soldier, Spy. There was also a movie of the same title released in 2011, starring Gary Oldman. Source: John le Carré, Tinker, Tailor, Soldier, Spy, Knopf, 1974.

[6] EverQuest is a 3D fantasy-themed massively multiplayer online (MMO) role-playing game with more than 100,000 players globally. According to the game's website, the game is one of the "richest and most expansive gaming experiences ever created." Source: EverQuest (www.everquest.com/faq).

[7] Most SOC organizations use a threat dossier system to document malware and associated threats. The dossiers or files kept on different threat types are extensive and require significant research and testing to document the necessary countermeasures for the threat.

[8] This is certainly not an exhaustive list. The analysts and managers we spoke with had differing opinions of the value of certifications. Many companies strongly encourage staff to have them, and others less so. Certifications fall into two categories — technical and professional. Technical vendor certifications are the most popular among SOC staff. All interviewed agreed that these vendor certifications were the most applicable to daily job responsibilities.

The most common professional certifications held by those interviewed include the Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), Global Information Assurance Certification (GIAC), Information Systems Security Architecture Professional (ISSMP), and Information Systems Security Management Professional (ISSMP). However, everyone agreed that certifications were no guarantee that an analyst would be successful as a SOC analyst. There was a consensus among the managers interviewed that a certification might earn a candidate an interview, but it was not a guarantee of a job offer. Some managers even reported hiring an uncertified candidate over a certified one.

Within the security community, the hard skills are almost synonymous with certifications. These acronyms, which propagate with alarming regularity, are popular within the security community and are often worn as a badge of honor (sometimes literally!). These certifications started as the best intentions of an immature industry, but now many organizations are jumping on the bandwagon in the hunt for profit. Whether you believe them to be a true indicator of talent or a marketing cash cow is irrelevant — certifications are here to stay, and the choice of certification does say something about the applicant See the June 14, 2012, "Recruit And Retain An Information Security Team" report.

[9] The list of potential certifications is too long to enumerate for this research document; however, it was clear that technology certifications from the major technology providers (Cisco, Fortinet, Juniper Networks, SonicWall), as well as general security certifications from (ISC)2 SANS-GIAC, were the most popular.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 13 key roles at major companies providing proprietary research, customer insight, consulting, events, and peer-to-peer executive programs. For more than 29 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com. 95241