HOW (ISC)² IS HELPING MEMBERS THROUGH A WORKFORCE SHORTAGE

InfoSecurity PROFESSIONAL

JANUARY/FEBRUARY 2022

Practical Advice. Actionable Insights.

TRUSTING OTHERS TO MANAGE YOUR SECURITY

+

AWS Pen Testing

vCISO Advice on Conveying Risks

New Workforce Study Findings

(ISC)²®

CCSP® Certified Cloud Security Professional

An (ISC)² Certification

The BUZZ is Real

"The Next Big Thing"
- Certification Magazine

CERTIFICATION MAGAZINE
2021 TOP CERT
CCSP
(ISC)²
THE NEXT BIG THING

Build on Your CISSP Expertise and Master Cloud Security

You've proven your expertise in cybersecurity…now prove yourself as the authority in cloud security for your organization.

The Certified Cloud Security Professional (CCSP) credential was designed to build on your deep technical and managerial CISSP knowledge and position you at the highest level of mastery for cloud security.

- **Grow with (ISC)²** – Validate your specialized skills and invest further into your membership with no additional fees. CISSPs already meet the experience requirements and your CPE credits are transferrable.
- **Cutting-Edge Credibility** – CCSP positions you as an authority in cloud security, highly adept in staying on top of the latest technologies, developments, and threats.
- **Broad Agility** – CCSP's vendor-neutral and multivendor qualifications may be applied across a range of cloud platforms, making your individual skillset more marketable.
- **Soaring Demand and Earning Power** – The demand for cloud security skills is projected to grow 115% over the next 5 years and command the highest premium at US $15,025.

Make Your Move

CONTENTS ▪ JANUARY/FEBRUARY 2022 ▪ VOLUME 15 · ISSUE 1

Is how you communicate with users and assess risks helping or hurting efforts?

PAGE 28

FEATURES

DEPARTMENTS

Cover image by Jan Feindt

Illustration (above) by Alison Seiffer

Illustration (right) by James O'Brien

EDITOR'S NOTE

ANNE SAITA EDITOR-IN-CHIEF

Sí, Se Puede

WHERE I LIVE, we sometimes muster enthusiasm for a dreaded task or ambitious project by invoking a simple phrase: *Sí, se puede.* It most commonly translates to "Yes, you can" or more colloquially, "You can do it!" Modern usage means the more inclusive "Yes, we can."

If someone is struggling with a work or personal issue, *Sí, se puede* can be the needed nod or nudge to soldier on. When faced with seemingly intractable barriers or a series of setbacks, the affirmation reinforces the resiliency in all of us. It becomes a puny-yet-powerful instrument to creating change.

Si Se Puede! was the rallying cry during the 1970s movement to improve wages and working conditions for farmworkers in the United States. We currently see a similar if less organized movement, as millions of employees demand better compensation and reduced hours to combat high job stress. Burnout is very real in cybersecurity, and employers who ignore requests might find themselves short-staffed on short notice—a tough situation given today's cyber threat landscape.

Because of the persistent global workforce gap and our greater dependency on online activity, wages for cyber positions will continue to rise this year. But with better pay comes greater expectations that can undermine the work-life balance we continually seek.

In our inaugural Office Hours column, CISSP Mike Hanna asks us to consider a different approach to planning ahead, one in which we strategically align resources around possible, rather than just preferred, outcomes. He provides a high-level view of a discipline called futures studies that essentially acknowledges both the hopes and limited control we have going forward.

Burnout is very real in cybersecurity, and employers who ignore requests might find themselves short-staffed on short notice—a tough situation given today's cyber threat landscape.

If bringing in outside help is part of your organization's future plans, you'll want to read Matt Gillespie's cover story on working with managed services, especially with the increasing role of cloud services in operations. Speaking of the cloud, CISSP Adam Kohnke shows how to conduct pen testing for Amazon Web Services. Rounding out features is advice from a longtime CISO on communications and assessing risk—two perennial challenges in our industry. Maybe 2022 is the year everything—and everyone—unites to fight the threats and shield networks against attacks. Probably not. But let's believe this year will be better because we believe in ourselves and in each other to make it so. *Sí, se puede.* ●

Photograph by Louise Roup

Anne Saita lives and works in San Diego. She can be reached at asaita@isc2.org.

CONTRIBUTORS

We first introduced Wisconsin's **Adam Kohnke**, CISSP, last summer when he wrote a great piece about demystifying the Cybersecurity Maturity Model Certification, better known as CMMC, for our companion newsletter *Insights*. Adam is back to discuss pen testing AWS, which is the market leader at the moment. He's a regular contributor to the ISACA Now Blog and *ISACA Journal*, holds a B.S. in IT security from Western Governors University, and also earned CISA and GPEN credentials.

Brian Grayek, CISSP, shares some of what he's learned as both a seasoned cybersecurity professional and now an Arizona-based virtual CISO who coaches others, particularly in risk assessments. Brian builds and leads security teams for some of the largest enterprises on the globe, including Cognizant, CGI, Computer Associates, Verizon, Apollo Group and Motorola. At Motorola he reported to one of the few female executives at the time, Randine "Randi" Hoefer, whom he credits for making him the long-term professional he is today.

Chicago technology writer **Matt Gillespie**'s byline has appeared in previous issues of this magazine and both *Insights* and *Cloud Security Insights*. In this issue, he outlines when it might be time to bring in outside help—and talks to experts to determine the best way to do just that.

Living and working in Berlin, Germany, illustrator **Jan Feindt** created this issue's eye-catching cover image. Feindt studied illustration at the Vital – Center for Graphic Design in Tel Aviv. His notable clients include *The New York Times*, *Rolling Stone*, *Dazed and Confused* and more.

CONTENTS

InfoSecurity PROFESSIONAL

Practical Advice. Actionable Insights.

(ISC)² ® INSPIRING A SAFE AND SECURE CYBER WORLD

isc2.org community.isc2.org

READ. QUIZ. EARN.

Earn Two CPE Credits for Reading This Issue and Taking the Online Quiz

In order to earn the two CPE credits, you must pass the issue quiz. Please provide your name and (ISC)² member number so that we can award the two CPE credits to your account. This typically takes up to 15 business days to be added to your account.

https://www.isc2.org/InfoSecurity-Professional/Magazine-Archive/Quiz/Jan-Feb-2022

Learn about more opportunities to earn CPE credits at https://www.isc2.org/Membership/CPE-Opportunities

ADVERTISER INDEX

For information about advertising in this publication, please contact Vendor Sponsorship: Lisa Pettograsso, lpettograsso@isc2.org.

(ISC)² CCSP: The Buzz is Real	2
(ISC)² 20 Tips for Secure Cloud Migration	6
Center for Cyber Safety and Education	8
SEM	13
Penn State	14
(ISC)² Enterprise Cybersecurity Training Guide	16
(ISC)² Community	32
(ISC)² Professional Development Institute	34

(ISC)² MANAGEMENT TEAM

EXECUTIVE PUBLISHERS
Chris Green
+44-203-960-7812
cgreen@isc2.org

Tim Garon
571-303-1320
tgaron@isc2.org

DIRECTOR, CORPORATE COMMUNICATIONS
Jarred LeFebvre
727-316-8129
jlefebvre@isc2.org

CORPORATE PUBLIC RELATIONS MANAGER
Brian Alberti
617-510-1540
balberti@isc2.org

MANAGER, MEMBER COMMUNICATIONS
Kaity Pursino
727-683-0146
kpursino@isc2.org

COMMUNICATIONS COORDINATOR
Dimitra Schuler
727-316-9395
dschuler@isc2.org

EDITORIAL ADVISORY BOARD

Brian Alberti, (ISC)²

Anita Bateman, U.S.

Felipe Castro, Latin America

Brandon Dunlap, U.S.

Rob Lee, EMEA

Jarred LeFebvre, (ISC)²

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

TWIRLING TIGER MEDIA MAGAZINE TEAM

EDITOR-IN-CHIEF
Anne Saita
asaita@isc2.org

ART & PRODUCTION DIRECTOR
Maureen Joyce
mjoyce@isc2.org

Twirling Tiger Media is a women-owned small business. This partnership reflects (ISC)²'s commitment to supplier diversity.

Nudging the Snowball

BY CLAR ROSSO, CEO

Welcome, 2022. It's time to get to work. Let's close the workforce gap.

Do you have enough people in your organization right now? What would you do today if you had more staff? What preventable vulnerabilities could you address if you had more people?

What's your biggest challenge to closing your skills gap? Recruiting? Retention? Upskilling? Convincing business leaders about the value of investment?

I have some good news. (ISC)²'s leadership, board of directors and staff have kicked the snowball off the cliff and momentum is building to address these barriers and clear the hurdles you need to tackle your organization's skills gap.

Recruitment

There are simply not enough qualified candidates, and competition is fierce for the few candidates out there. We are tackling the recruitment conundrum in a number of ways, including:

- Launching a new entry-level certification for those with no experience, creating a stepping stone to the CISSP and other certifications.
- Creating resources to help employers rethink job descriptions and hiring practices, including hiring for non-technical skills and training for technical skills.
- Extending the Center for Cyber Safety and Education's activities to amplify awareness of cybersecurity careers as well as significantly increasing scholarships and grants to support interested individuals.

We also know that cybersecurity degrees vary widely among universities and it's hard to know what skills individuals with degrees will bring to the workplace. In 2022, we are convening academia and employers from around the globe to create solutions that will include embedding certifications in degree programs.

Clar Rosso is CEO of (ISC)². She can be reached at crosso@isc2.org.

Retention

Our research shows retention starts with onboarding. We know that slowing down and addressing retention needs can be tough for the cyber superheroes who are protecting your organizations from threats, so we are making it as easy as possible with tips, tools and webinars that are focused on helping you create maximum impact and stickiness with your team members. From developing clear and consistent onboarding processes to formal and informal mentoring programs, we will roll out resources throughout 2022.

Advancement

We also know that professional development and a focus on career pathing increases employee job satisfaction. We are growing our education and training offerings to enable you to more precisely develop team members without sifting through nonessential offerings.

Our portfolio of certifications is designed to meet the challenges your businesses face, from the CCSP, which allows professionals to more ably manage their entire cloud ecosystem, as opposed to a single cloud-based technology, to the CSSLP, which focuses on secure software development.

Plus, we are committed to making our examinations, education and certifications as accessible as possible and have established goals for adaptation, translation and localization. We also continue to explore how to safely and securely offer online proctored exams.

Making the case

But perhaps what's getting in your way is not recruitment, retention or advancement. Perhaps it's all about helping business leaders understand the value of cybersecurity professionals within your organization. Again, we engage in a host of activities on your behalf to help ensure your team gets the recognition and attention it deserves, from high-profile media placements to legislative and regulatory advocacy, compelling research, webinars and tools.

The groundwork has been laid, and now is the time for us to begin to create an avalanche moment everyone in our profession will remember. We're in and ready to help, but we can't do this without you. There's no more waiting. Seek out mentees. Expand your hiring searches and take a look at diversity of experience and non-technical skills.

All of us working together can prove to the industry—and ultimately the world—how powerful this association of committed cybersecurity professionals can be and the difference we can all make. So, are you in? ●

CONTENTS

CENTER FOR
CYBER SAFETY
AND EDUCATION™

SCHOLARSHIPS 2022

Undergrad • Graduate • Veterans • Women • Minorities

APPLY TODAY!

iamcybersafe.org/scholarships

(ISC)²®

KnowBe4
Human error. Conquered.

OFFICIAL (ISC)² CHAPTER

Raytheon
Intelligence & Space

(Awareness)

FIELD NOTES

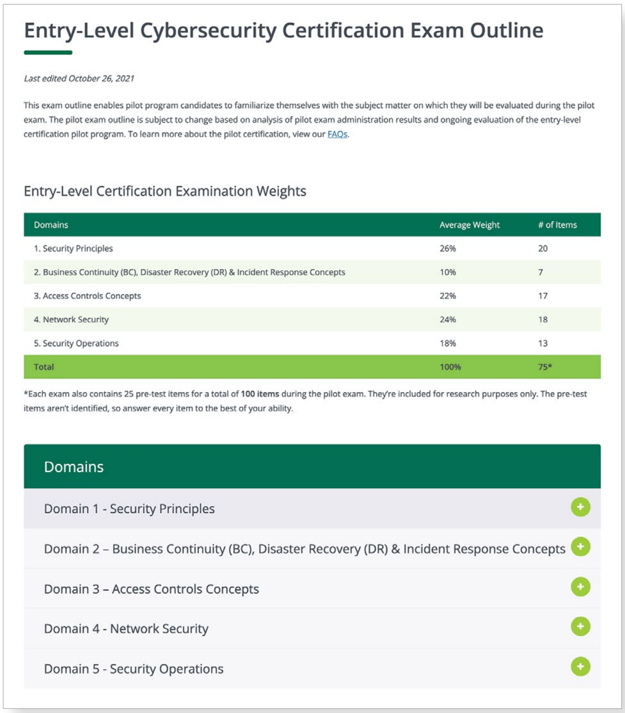
A ROUNDUP OF WHAT'S HAPPENING IN (ISC)^2 COMMUNITIES

New Entry-Level Certification to Remove Experience Barrier

(ISC)^2 WILL BEGIN PILOTING a new entry-level cybersecurity certification exam in January, focused on newcomers to the profession, whether recent college graduates and career changers. The new program will also support employers, providing verification and confidence that certification holders have the needed baseline skills despite lacking the five years of experience many hiring managers currently seek.

All cybersecurity professionals, whether an (ISC)^2 member or not, were involved in shaping the domains included in the exam through a survey. As such, current cybersecurity professionals helped to validate the knowledge, skills and abilities on which the exam will be based.

> **"This certification will give employers the confidence that newer entrants into the sector have a solid grasp of the right technical, ethical and operational practices on which to build and learn."**
>
> *—Dr. Casey Marks, (ISC)^2 chief qualifications officer*



Entry-Level Cybersecurity Certification Exam Outline

Last edited October 26, 2021

This exam outline enables pilot program candidates to familiarize themselves with the subject matter on which they will be evaluated during the pilot exam. The pilot exam outline is subject to change based on analysis of pilot exam administration results and ongoing evaluation of the entry-level certification pilot program. To learn more about the pilot certification, view our FAQs.

Entry-Level Certification Examination Weights

Domains	Average Weight	# of Items
1. Security Principles	26%	20
2. Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts	10%	7
3. Access Controls Concepts	22%	17
4. Network Security	24%	18
5. Security Operations	18%	13
Total	100%	75*

*Each exam also contains 25 pre-test items for a total of **100 items** during the pilot exam. They're included for research purposes only. The pre-test items aren't identified, so answer every item to the best of your ability.

Domains

Domain 1 - Security Principles
Domain 2 – Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts
Domain 3 – Access Controls Concepts
Domain 4 - Network Security
Domain 5 - Security Operations

The new certification is intended to fill pipelines by attracting more people to the cybersecurity field and making job candidates more attractive to employers. Among the primary challenges newcomers to cybersecurity face are typical three- to five-year experience requirements. The pool of qualified job candidates remains in short supply, thereby continuing a global workforce shortage of 2.72 million at last count.

Last year's (ISC)^2 Cybersecurity Career Pursuers Study revealed frustrations with high barriers to entry. The study also reflected more candidates with nontraditional resumes; half of newer cybersecurity professionals (those with less than three years of experience) came from fields outside of IT.

In addition, to help less experienced candidates earn jobs, the foundational certification provides more clarity for candidates who aspire to obtain the CISSP credential.

"This approach underlines our commitment to making cybersecurity a more accessible, inclusive and diverse profession. This certification will give employers the confidence that newer entrants into the sector have a solid grasp of the right technical, ethical and operational practices on which to build and learn," said Dr. Casey Marks, (ISC)^2 chief qualifications officer.

(ISC)²
The Cybersecurity Career Pursuers Study
BUILD
RESILIENT
CYBERSECURITY TEAMS
Stop Chasing 'All Stars' for Short-Term Gain and Develop Your Team for Years of Success

For more information on the pilot program or to provide input into the development process, please visit https://www.isc2.org/New-Cert. ●

There's a Lot of Work to Do in 2022

NEAR THE END OF LAST YEAR, (ISC)² reported that the global workforce gap continues to shrink, dropping from a shortage of 3.12 million to 2.72 million cybersecurity professionals. This is due to bigger supply pipelines that added 700,000 new entrants to the market, as well as slight softening demand thanks to, what else, the pandemic.

"The study tells us where talent is needed most and that traditional hiring practices are insufficient. We must put people before technology, invest in their development and embrace remote work as an opportunity. And perhaps most importantly, organizations must adopt meaningful diversity, equity and inclusion practices to meet employee expectations and close the gap," (ISC)² CEO Clar Rosso said upon the workforce study's release.

> **"…Perhaps most importantly, organizations must adopt meaningful diversity, equity and inclusion practices to meet employee expectations and close the gap."**
>
> *—Clar Rosso, (ISC)² CEO*

The survey drew a record 4,753 cybersecurity and IT/ICT professionals, all of whom dedicate at least 25% of their time to cybersecurity tasks throughout North America, Europe, Latin America and Asia-Pacific.

(ISC)² CYBERSECURITY WORKFORCE STUDY HIGHLIGHTS

Help still desperately needed

Even with 700,000 new entrants, demand continues to outpace the supply of talent. The global cybersecurity workforce needs to grow 65% to effectively defend organizations' critical assets.

Plans going forward to bridge the workforce gap

- More training (36%)
- Providing more flexible working conditions (33%)
- Investing in diversity, equity and inclusion (DEI) initiatives (29%)
- Using cloud service providers (38%)
- Deploying intelligence and automation for manual tasks (37%)
- Involving cybersecurity staff earlier in third-party relationships (32%)

How do you compare?

- A record 77% of respondents reported they are satisfied or extremely satisfied with their jobs.
- Only 38% of female participants started their careers in IT, compared to 50% of male participants.
- The average salary of a cybersecurity professional before taxes is U.S. $90,900—up from U.S. $83,000 in 2020.
- Salaries of certified cybersecurity professionals are U.S. $33,000 higher than those with no certifications.
- Cloud computing security is once again the top priority for cybersecurity professionals' skills development in the next two years.

Unintended consequences when staff is stretched too thin

Participants said they experienced misconfigured systems (32%); not enough time for proper risk assessment and management (30%); slowly patched critical systems (29%); and rushed deployments (27%).

Images by Robert Pizzo

CONTENTS

‘Diversity of thought is a global crisis’

New DEI research reflects experiences of minority cybersecurity professionals

A RECENTLY RELEASED (ISC)² REPORT, *In Their Own Words: Women and People of Color Detail Experiences Working in Cybersecurity*, provides rare access to the personal experiences of minority cybersecurity practitioners, providing a lens through which to view the concepts of equity and inclusion in today’s workplaces.

Researchers asked professionals from nine countries how diversity, equity and inclusion (DEI) are defined and why creating successful DEI programs is so difficult. Minority cybersecurity professionals also outlined work-related challenges and strategies to achieving a truly diverse work culture. The study outlines eight recommendations for improving DEI in cybersecurity teams, from implementing cultural sensitivity training to documenting clear advancement practices.

“What we found is that many issues are universal to the experiences of diverse professionals no matter where they live and work. That tells us that the strategies and solutions to improve organizational practices also have a lot in common, including overcoming unconscious bias, providing pathways for advancement, hiring diverse leaders and championing equitable pay structures,” said Clar Rosso, CEO of (ISC)².

“The diversity of thought is a global crisis. I mean, it needs to be in the cybersecurity workforce or else nothing’s going to be secure in this world,” said one study participant.

You can learn more about establishing a DEI program at your organization by visiting (ISC)²’s dynamic DEI Resource Center.

CANDID COMMENTS FROM PARTICIPANTS

“My organization has made DEI training mandatory and not voluntary like it used to be. They have also hired several women for key leadership positions. I’ve witnessed a change in the past year with more people sharing their ideas and collaborating, rather than everyone trying to protect their territory.”

“I’ve been in meetings where people have used my words. They’ve used my strategies. They have taken my work, and they presented it as their own. They get credit for my talent. It would burn me so bad but, yet, I didn’t really have anyone to lean on.”

“As the only woman in my team, I always had a hard time finding a mentor I could relate to or who gave honest advice. I often felt lonely and had to learn a lot of things through trial and error.”

“It’s easy to start an initiative when the global temperature on diversity is so high. However, DEI initiatives typically don’t get fast results. They are a slow, tedious process that requires ongoing commitment and dedication from the whole organization, along with designated performance metrics that help to track success and keep stakeholders’ motivation up.”

“We see a lot of diverse professionals in entry-level positions. But they don’t stay long enough to advance into higher positions. Exit surveys report they leave because the culture doesn’t support them. They feel lost.”

“Cybersecurity today should be a topic as important as fire safety or health education. We need to start building awareness earlier on, so children start embracing it from a young age, dreaming about becoming a cybersecurity officer just as they dream of becoming a fireman or a doctor.”

Heard Around Security Congress

The recent (ISC)² Security Congress highlighted strategies and tactics to counter today's most pressing threats both within and outside the industry. Everything from inclusion and leadership, malware and misinformation to CISO burnout and legal issues was covered. Here are some snippets from keynotes to keep in mind as we embark on a new year.

"When people don't feel happy, when people don't feel content, they don't have that individual investment in the company or in the city or in the country to which they belong. People will accept some pretty Draconian measures, and they are quite happy to put up with that and keep the secrets, as long as they feel valued and they feel they got a good deal."

—Lisa Forte, Red Goat Cyber Security

"We've got to make it harder for the bad guys to operate here. We've got to target cryptocurrencies to make it harder to transfer money."

—Former CISA Director Chris Krebs, referring to the need to regulate cryptocurrencies at the heart of ransomware attacks

"Cybersecurity and spacecraft engineering share a couple of things. We don't really know what we're doing. That is, we're always inventing solutions to new challenges. When you don't know what you are doing when you are operating at the edge of your capacities, you need all the ideas you can get. The ideas you can find in a diverse, manifold team are more than if everybody has the same perspective."

—Adam Steltzner, leader and chief engineer of the NASA Mars 2020 mission and Rover Perseverance

"If we continue to look for the same skill sets and characteristics in the people we recruit, then our pool will remain the slow-flowing stream of talent that it has been for decades when what we need is a flood of talent."

—Clar Rosso, (ISC)² CEO

"We have to design cultures that support women, and it means rewarding good behavior and calling out bad behavior. … If you witness inappropriate behavior, you should report that. No, it doesn't mean that if you report it, that person is going to get sacked. … What it means is that you will not look the other way. You are safe to do that. You are safe to report it. Because what we want are great environments that work for all people."

—Jane Frankland, author of **IN Security: Why a Failure to Attract and Retain Women in Cybersecurity is Making Us All Less Safe**

Daymond John's Five Shark Points for Success

1. **S**et goals.
2. Do your **h**omework.
3. Have **a** love for what you do and those who support you.
4. **R**emember your personal brand.
5. **K**eep swimming.

CONTENTS

MEMBER'S CORNER

Looking to Expand the Team? Consider Hiring a Military Veteran

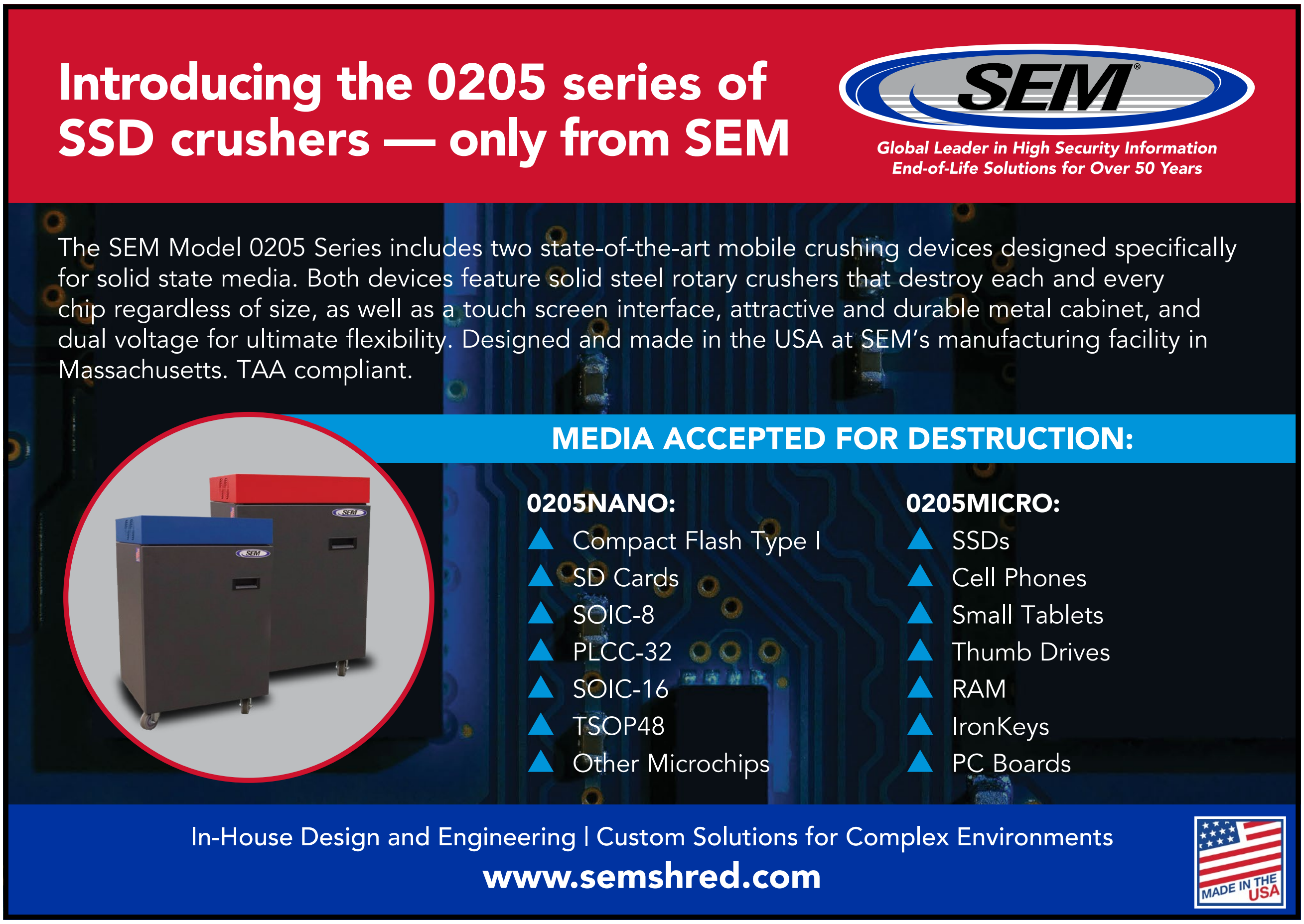
BY JONATHAN SPROULE, CISSP

IT SEEMS LIKE A LIFETIME AGO when I was a professional musician in the Armed Forces, serving in the Band of the Welsh Guards. I spent some time wearing that famous scarlet tunic and performing in great concert halls and theaters around the world.

Now I carry a different tune, one still aligned with my military experience. I think every employer looking to replace or expand their cybersecurity team would be wise to consider hiring those with military experience. Military musicians, and other Armed Forces personnel for that matter, might not seem an obvious hiring choice; however, they possess a multitude of in-demand skills employers seek.

Many organizations have a set of core values that attempt to define and articulate their culture. Similarly, the Armed Forces have a set of values instilled into each person who serves. These values and standards aren't treated as something to tick off on a checklist; active duty military members live and breathe them. These values are so engrained that they often carry into the next phases of veterans' lives entering a second career.

Forces personnel are mission focused and goal orientated,



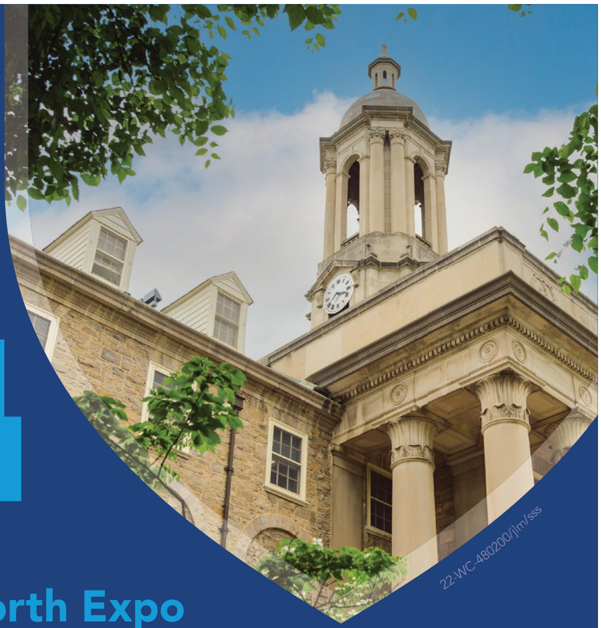
Jonathan Sproule, CISSP, is an experienced information security professional and military veteran with a background as a professional musician. Sproule lives and works in the U.K.

day in and day out. They also understand the true meaning of teamwork. Serving personnel must balance the ability to be independent while contributing to a collective to achieve common goals. This is also important for security operations teams, which must work with minimal guidance yet remain attached to other units in order to protect assets, prevent malicious penetration and stay abreast of threats.

Military musicians also possess something that isn't particularly abundant in IT: emotional intelligence. They can read both warning signs and "a room" to understand when someone with influence, such as a board member, doesn't agree with their analysis or business case. They can sense when a team member isn't acting quite like themselves and can intervene before a personal crisis spills into a professional one. We need people with these skills, as we are not only a system of technology and processes but also of people. Never forget we all work with human factors.

Homogenous teams tend to think alike, with assumptions never truly challenged. Everyone is encouraged to just "go with the flow." Armed Forces personnel recognize strength in diversity and understand cultures other than their own. Challenging assumptions and bringing different perspectives allows for better risk elicitation and overall greater visibility of risk across the enterprise. Why? Military personnel are not comfortable with "that's the way it's always been done," where continual improvement is stifled.

We need our cybersecurity ranks to be filled with the suitably trained. That includes former military members who truly understand what security is. The next time you're looking for that new hire, consider someone who served their country and now wants to do the same for your company. ●



They Can Code, But Can They Also Collaborate?

BY DEBORAH JOHNSON

Getty Images

Yes, technical proficiency is a key measurement when hiring additions to a cybersecurity team. But however adept and knowledgeable the candidate, if they don't have the right mix of "soft skills," that technical talent may be wasted.

"It's creativity, curiosity, compassion, collaboration and critical thinking. Those things are important in every single job," says Ben Eubanks. As chief research officer at Huntsville, Alabama's Lighthouse Research & Advisory, Eubanks tracks candidate data for employers and hiring managers.

Hiring managers want someone who can manage their time well, solve problems, resolve conflicts and build teams. Finding someone as good at coding as collaborating is one reason for a growing soft skills gap in the tech industry.

Talent Works, a global tech recruiter with offices in Manchester, U.K., and Boston, Massachusetts, last June surveyed 400 U.S. and U.K. tech leaders. Almost eight out of 10 U.S. respondents and 64% in the U.K. said they "feel candidates who apply to their organization are missing the necessary soft skills to succeed."

"It's the *soft* skills that are *hard*. Hard to learn. Hard to replicate. Hard to coach. Hard to excel at. And it's the soft skills that determine success too." That's the challenge for hiring managers, writes recruitment professional Greg Savage on his blog.

In reviewing candidates, especially in the technology arena and cybersecurity, it may be a challenge to assess a person's soft skills, especially with a majority of job interviews still taking place remotely.

"Ask open-ended questions," suggests Eubanks. "If you ask someone, 'Are you a team player?' or 'Is compassion important?' there's only one correct answer and the candidate knows exactly what it is. Instead, ask: 'Tell me about a time you had to join a new work team' or 'Tell me about a time when compassion played a part in your work.' That allows you to see past behaviors, and, like it or not, past behavior is a predictor of future behavior."

Other interview tips to gauge someone's soft skills:

- Ask the candidate to assess their soft skills and give examples.
- Note how well the candidate is organized in presenting themselves and listening actively.
- Present the candidate with a problem your team faced (and solved) to assess critical-thinking skills.
- For a finalist candidate, present them with a short project to collaborate on with an in-house team.

The need to collaborate, communicate and problem solve only grows as automation leaves more time for team-based innovation, posits Eubanks. "The more automation that comes into the work—whether it's a little bit or a lot—the more we need to focus and prioritize those human skills in the work that we do." ●

Photograph by Louise Roup

Deborah Johnson lives and works in San Diego. She can be reached at djohnson@twirlingtigermedia.com.

CONTENTS

(ISC)²
The Enterprise Guide to Establishing a
CYBERSECURITY
TRAINING PROGRAM

Trusting Others

TO MANAGE YOUR SECURITY

Is outsourcing all or part of a security function a good fit for your organization? How should you go about it?

BY MATT GILLESPIE

SOMETIMES WE ALL NEED TO ASK FOR HELP. That necessarily means placing trust in someone else, but wisely choosing where to place that trust helps mitigate your vulnerability.

Bringing in managed security services can help overcome gaps and other shortcomings in your security posture, but it requires a leap of faith.

Taking the *right* leap transforms risk into preparedness.

ILLUSTRATION BY JAN FEINDT

ADMITTING YOU HAVE A PROBLEM

It's all well and good to target building an airtight security posture and bringing in experts to make it happen, but life is seldom that simple.

Organizations that find themselves considering managed security services providers (MSSPs) are typically doing so in response to a problem state, whether that means recovering from a breach or just acknowledging that their security function is lacking.

There may also be broader issues throughout the IT infrastructure, such as data siloes, excessive manual processes, and unreliable or incomplete system and service monitoring. Mergers and acquisitions are a common source of redundancy, non-integration and similar issues.

> "Oftentimes an organization buys another entity … but with it comes all of the sick children, the poorly maintained technologies, and a serious load of tech debt."
>
> *—Shaun Drutar, senior manager for managed security services, Wipro*

Shaun Drutar, senior manager for managed security services at Wipro, says, "Oftentimes an organization buys another entity … but with it comes all of the sick children, the poorly maintained technologies, and a serious load of tech debt."

These realities mean that bringing on an MSSP and getting the full value from the relationship requires fixing issues that may be longstanding and deeply embedded in the organization. For example, Michael Restivo, director for cybersecurity sales at Verizon Business, says, "Number one, the majority of customers have too many tools. Number two, they need to consolidate. When they do consolidate, they need to tweak and alter and refine."

Organizations typically have a two-part dilemma when it comes to getting value from their security tools: ingesting logs and other data from all the relevant sources, then making full use of the data that is available.

While both these challenges are significant, connecting to data is the smaller issue of the two. And as legacy systems give way to software-as-a-service (SaaS) subscriptions and cloud-native infrastructure, problems related to connectivity and interoperability are slowly waning in importance and quantity.

Tuning security platforms to make full use of log and alert data is both more critical and more complex than connecting to the data in the first place, especially because it's difficult to know when you're done.

A significant requirement in this space is to bring under control the floods of data that may be flowing into the security operations center, which can easily overwhelm human responders.

Optimizing those data flows requires both the right tools and the right implementation. Machine learning typically plays a role to correlate discrete-but-related events into composite incidents, reducing noise and adding insight. At the same time, emerging threats such as new generations of polymorphic malware constantly require new approaches.

This ongoing complexity highlights the challenge of hiring and retaining security expertise from an increasingly overtaxed and under-resourced pool of talent. As it becomes more difficult and expensive to recruit candidates, keep their skills up to date, and get them to stay in their roles, filling requirements using an MSSP may be an attractive alternative.

DON'T DEPEND ON THE GRAPEVINE

EVERY SALES TEAM knows the value of customer references, but MSSPs face particular obstacles providing them.

"The big problem we have as providers is customers want references, [but] due to the nature and privacy of cyber, nobody wants to be a reference," according to Michael Restivo, the director for cybersecurity sales at Verizon Business.

Indeed, the most compelling stories a sales rep could share probably have to do with past security incidents, which the affected organization may not want to talk about publicly. Customers can therefore be well advised to de-emphasize the role of references during vendor selection of an MSSP.

—M. Gillespie

BUILDING A SOUND RELATIONSHIP

MSSPs run the gamut from small, boutique providers promising specialized white-glove services to multinationals with massive reach in terms of services and geography. Depending on circumstances, either could be the right fit.

Some organizations, particularly

CONTENTS

smaller companies, prefer to work with smaller MSSPs, from which they hope to get more personalized and responsive service, even without a large budget. Others seek out first-tier providers that have the broadest scope of resources and expertise available and which can scale on demand.

For MSSPs of any size, word of mouth should play a role in assessment of an MSSP, especially in the early stages of the search. There is no replacement for hearing unvarnished accounts of real-world experiences, and an informal survey of industry peers is simple and useful.

In the case of the larger providers, their reputations will precede them. Restivo says, "If I'm going to put myself in the shoes of the customer, the first thing I'm going to look at is the analyst reports. I'm going to look at IDC MarketScape, I'm going to look at Forrester, I'm going to look at Gartner, and I'm going to see where those providers are ranked."

> "If I'm going to put myself in the shoes of the customer, the first thing I'm going to look at is the analyst reports."
>
> *—Michael Restivo, director for cybersecurity sales, Verizon Business*

Beyond issues of competence and the quality of protection an MSSP can offer, the actual day-to-day interactions between the MSSP and customer should also be considered from the outset.

Reporting not only of incidents but of regular operations status should not be overlooked. Are dashboards needed to keep decision makers informed of key performance indicators? What are those metrics? Customers need to define what insights they need on an ongoing basis into the overall health of security systems, issues that arise, and mitigations applied, for example.

The counterpart to that need for communication is to delineate the separation of roles and responsibilities between the MSSP and customer.

It can be hard to parse expectations for both parties across the full range of circumstances, from normal operation to crisis response. Moreover, there is a significant dimension of legal and financial responsibility.

Restivo added, "It's hard to build SLAs and SLOs with a clear line of delineation or demarcation where response begins and ends. That's a very touchy, complex subject to legally build terms and conditions."

One common approach is to separate duties according to existing categories, such as the customer retaining responsibility for Level One incidents and making the MSSP responsible for everything that escalates to Level Two or higher. It's worth noting that arrangement doesn't avoid the issue entirely, as it is still necessary to create strong guidelines about when to escalate.

In fact, creating a hybrid model of shared responsibility between internal resources and the MSSP is messy, and it often leads to finger-pointing between parties that runs counter to delivering the best results possible.

"The best, most well-run services provided to customers are when we, the MSSP, take 100% onus from alert notification to determining the foundational root cause and analysis of an incident, for example, and then actually remediating it," Restivo says.

WHERE TO DRAW THE LINE

Outsourcing the entire security function is obviously more strategically significant to an organization than just adding managed resources to cover staffing deficits or skill gaps. While the gravity of that decision may make executive decision makers hesitate, the potential advantages are clear.

BEWARE OF HOLES IN THE UMBRELLA

PART OF THE DUE DILIGENCE needed when bringing on an MSSP is to make sure the relationship covers all your needs, now and into the future.

For example, can the provider offer full protection and control over mobile devices (including BYOD)? How does it fit into your cloud transformation plans? What if you decide to expand the relationship later to include full SOC-as-a-service?

Even more than other vendors, assessing an MSSP requires strategic planning. Picking the right partner for the long haul is a critical choice for avoiding pain in the years to come.

—M. Gillespie

In addition to providing crisp separation of duties and responsibilities, full outsourcing can support putting the MSSP advisory function in charge of security assessment and strategic planning, which can help create a more comprehensive security posture, minimizing gaps and redundancies.

While illustrating a hypothetical MSSP strategic approach, Drutar says, "You build out … a total security program document, runbooks for varied scenarios, your incident response plans … and you put all those pieces together to get you to that final state of, 'Yes, we have all data sources integrated, accounted for, we know what's up, we know what's down, and we know how to act when we see an alert.'"

While the possibility of contracting out every aspect of cybersecurity can be enormously attractive, that shouldn't be confused with the notion of totally outsourcing responsibility and liability for breaches and losses.

"Organizations are coming to [MSSPs] to 'Take our mess for less! Handle our mess and help us save on costs, and by the way, take all of the liability associated with it.' And nobody's really going to sign up for that."

—Shaun Drutar, senior manager for managed security services, Wipro

"Organizations are coming to [MSSPs] to 'Take our mess for less! Handle our mess and help us save on costs, and by the way, take all of the liability associated with it.' And nobody's really going to sign up for that," Drutar says.

Much like insurance, contracting with an MSSP can help reduce potential losses, but there are distinct limitations to the viability of this approach to eliminate financial and operational cyber risk. Looked at from the opposite point of view, an imprudent SLA or other agreement stipulation can easily expose an MSSP to losses that exceed the revenue potential of an engagement.

RECOGNIZE THE SCALE OF WHAT YOU'RE DOING

WHILE TOO MANY SALES TEAMS tout their wish to be "partners" with their customers, the fundamental and pervasive nature of MSS makes that partnership real.

By the same token, MSS adoption is likely to be a more strategic than tactical undertaking. Getting buy-in from senior management early in the process can therefore be a wise protection of overall success.

—M. Gillespie

On the other hand, an MSSP relationship can augment cyber insurance to protect businesses. In fact, a comprehensive security plan with demonstrated effectiveness can help make the case for lower premiums, with an attractive impact on the bottom line.

As a related matter, organizations should build out plans to check the effectiveness of MSSP controls and measures, using regular third-party assessments and penetration testing, for example.

Wherever MSSPs are adopted, such verifications are part of a broader need to embed services into the needs of the business, rather than just into the technology enterprise. "Instead of providers coming in and talking to customers and selling them the new shiny tool or platform and making recommendations, it's looking at the business problems and what you're trying to solve," Restivo advises.

As MSSP providers rise to that strategic imperative and help businesses construct better security roadmaps, the entire industry stands to benefit. ●

Matt Gillespie is a technology writer based in Chicago. He can be found at www.linkedin.com/in/mgillespie1.

CONDUCTING AMAZON WEB SERVICES PEN TESTS

BY ADAM KOHNKE, CISSP

AS OF 2021, Amazon Web Services (AWS) had more than a million active users spread across 190 countries with a service portfolio offering 200 unique products, according to Astra Security. AWS has spent the last four years leading the Gartner Magic Quadrant in cloud hosting solutions, showing no signs of slowing down.

Being "King of the Cloud" makes AWS a prime target for attackers and advanced persistent threats. That's why it's helpful to conduct internal AWS penetration testing methodologies.

I have experience in developing techniques to simulate the potential for abuse against common AWS services. Please keep in mind that this article is not meant to serve as direct, enterprise-specific security advice or guidance. It can, however, facilitate improved protections for such a pervasive cloud computing platform.

ILLUSTRATION BY JAMES O'BRIEN

CONTENTS

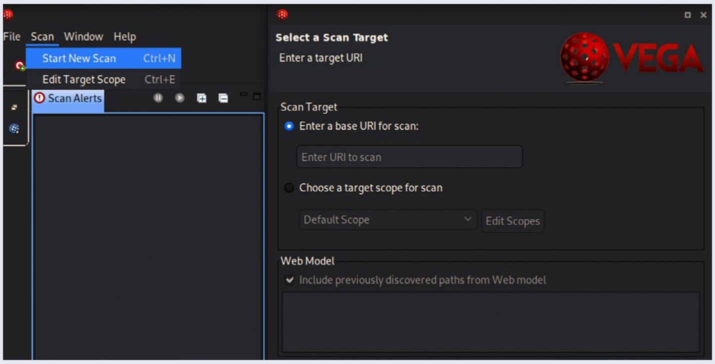
PLANNING AND SCOPING AWS PENETRATION TESTS

AWS requires announcement of penetration testing for most of its services prior to any activity. As such, pre-announcement should be part of all planning efforts. Last time I checked in late 2021, AWS EC2, RDS, CloudFront, Aurora, API Gateway, Lambda, Lightsail resources and Elastic Beanstalk do not require testing announcements in advance.

To help scope the test and drive efficiency, other early planning considerations for an AWS penetration test should include a review of AWS billing statements to understand which resources exist, which AWS accounts those resources exist in, and how many instances of each resource exist within in-scope accounts.

From there, establish partnerships with internal stakeholders and in-scope vendors to fully define the testing expectations, detailed target lists, testing timelines and escalation paths for pre-existing indicators of security breaches. Also prepare for possible disruption caused by testing procedures and obtain formal permission to conduct the testing (the proverbial "Get out of Jail" card).

FIGURE 1 – **WHAT YOU SEE WITH BASIC VEGA SCAN**



Select a Scan Target

Enter a target URI

Scan Target

● Enter a base URI for scan:

Enter URI to scan

○ Choose a target scope for scan

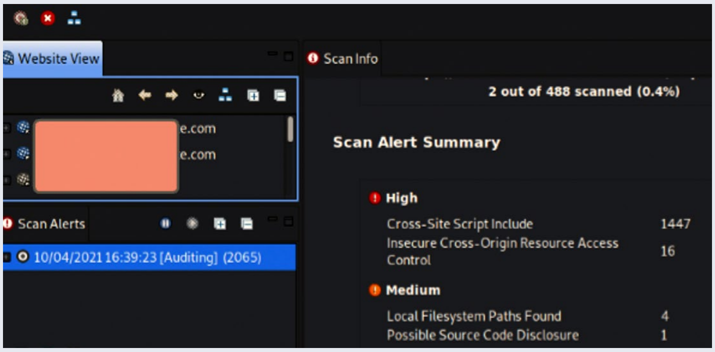
Default Scope

Web Model

✓ Include previously discovered paths from Web model

Clicking the "Start a New Scan" button initiates the scan process. Then, on the right-hand side, choose a target URI or website address to probe.

FIGURE 2 – **BASIC VEGA SCAN RESULTS**



[redacted]e.com
e.com

10/04/2021 16:39:23 [Auditing] (2065)

2 out of 488 scanned (0.4%)

Scan Alert Summary

High	
Cross-Site Script Include	1447
Insecure Cross-Origin Resource Access Control	16
Medium	
Local Filesystem Paths Found	4
Possible Source Code Disclosure	1

Website mappings from the Vega crawler are displayed on the left, opposite an alert summary showing details and severity of discovered vulnerabilities.

INFORMATION GATHERING, ENUMERATING AND FOOTPRINTING AWS ACCOUNTS

Let's assume that front-end web resources have been deployed by the "victim" organization connecting to its AWS infrastructure. In this scenario, an AWS access key was leaked, inappropriately shared or discovered by would-be attackers. User enumeration may be achieved through the use of tools such as theHarvester or Hunter.io, allowing discovery of email addresses associating to the victim organization.

The resulting email addresses can be paired with man-in-the-middle frameworks, such as Evilginx2, to perform low-cost and sophisticated phishing campaigns leading to further exposure and exploitation of AWS user credentials.

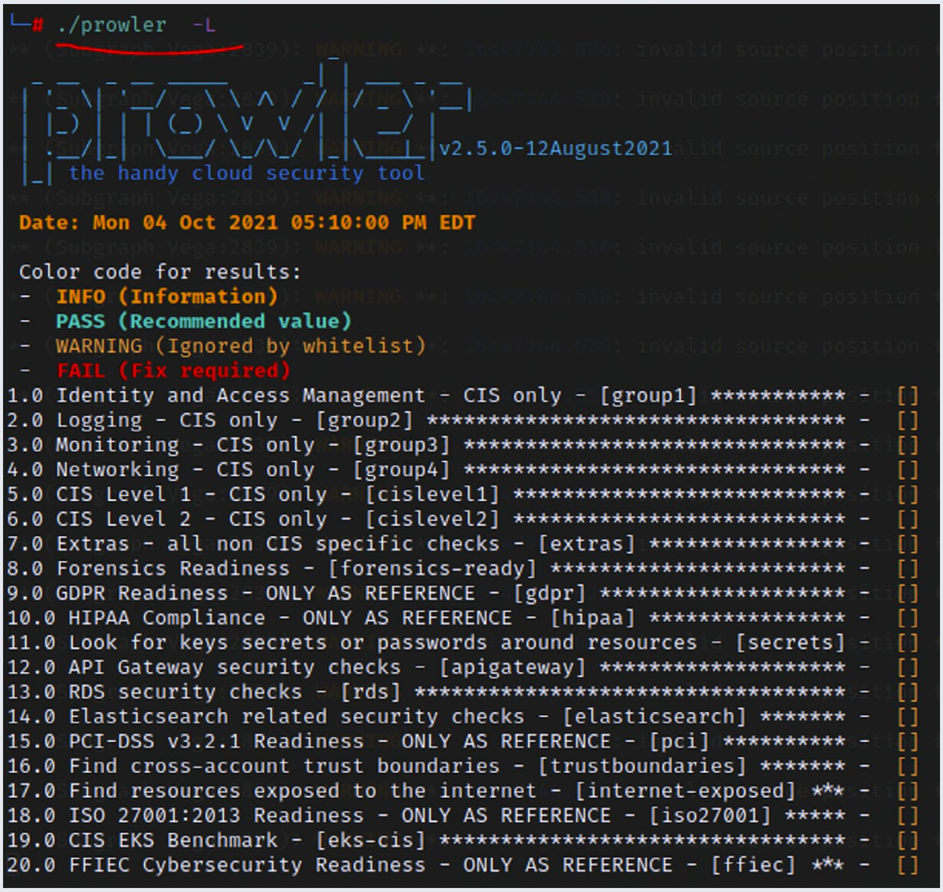
User enumeration and exploitation tools should be explored by internal pen test teams to assess the organizational user level of exposure to social engineering and multi-factor bypass techniques. Evilginx excels in achieving the latter.

To obtain a full accounting of the organization's attack surface, it is beneficial to perform vulnerability scanning regardless of whether an AWS key has been provided for testing or not.

Subgraph's Vega vulnerability scanner is an open-source scanning tool that covers a variety of needs for web application and cloud penetration testing. Vega can perform common and specialized vulnerability tests such as SQL injection, API testing, cross-site

CONTENTS

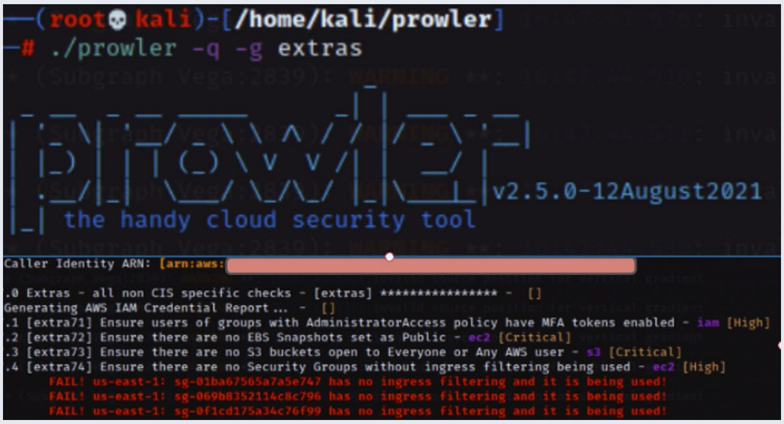
FIGURE 3 – PROWLER SECURITY CHECK CATEGORIES



```
└─# ./prowler  -L

                                    v2.5.0-12August2021
 |_| the handy cloud security tool

 Date: Mon 04 Oct 2021 05:10:00 PM EDT

 Color code for results:
 -  INFO (Information)
 -  PASS (Recommended value)
 -  WARNING (Ignored by whitelist)
 -  FAIL (Fix required)
1.0 Identity and Access Management - CIS only - [group1] *********** -  []
2.0 Logging - CIS only - [group2] ********************************* -  []
3.0 Monitoring - CIS only - [group3] ****************************** -  []
4.0 Networking - CIS only - [group4] ****************************** -  []
5.0 CIS Level 1 - CIS only - [cislevel1] ************************** -  []
6.0 CIS Level 2 - CIS only - [cislevel2] ************************** -  []
7.0 Extras - all non CIS specific checks - [extras] **************** -  []
8.0 Forensics Readiness - [forensics-ready] ************************ -  []
9.0 GDPR Readiness - ONLY AS REFERENCE - [gdpr] ******************** -  []
10.0 HIPAA Compliance - ONLY AS REFERENCE - [hipaa] **************** -  []
11.0 Look for keys secrets or passwords around resources - [secrets] -  []
12.0 API Gateway security checks - [apigateway] ******************** -  []
13.0 RDS security checks - [rds] *********************************** -  []
14.0 Elasticsearch related security checks - [elasticsearch] ******* -  []
15.0 PCI-DSS v3.2.1 Readiness - ONLY AS REFERENCE - [pci] ********** -  []
16.0 Find cross-account trust boundaries - [trustboundaries] ******* -  []
17.0 Find resources exposed to the internet - [internet-exposed] *** -  []
18.0 ISO 27001:2013 Readiness - ONLY AS REFERENCE - [iso27001] ***** -  []
19.0 CIS EKS Benchmark - [eks-cis] ********************************* -  []
20.0 FFIEC Cybersecurity Readiness - ONLY AS REFERENCE - [ffiec] *** -  []
```

The groupings of security checks Prowler can do. Use -g to target groups of interest such as './prowler -g group1' to perform identity and access management checks.

FIGURE 4 – FOCUSING PROWLER ON THE FAILED CHECKS



```
─(root💀kali)-[/home/kali/prowler]
─# ./prowler -q -g extras

                                   v2.5.0-12August2021
|_| the handy cloud security tool
Caller Identity ARN: [arn:aws:[redacted]
.0 Extras - all non CIS specific checks - [extras] **************** -  []
Generating AWS IAM Credential Report... -  []
.1 [extra71] Ensure users of groups with AdministratorAccess policy have MFA tokens enabled - iam [High]
.2 [extra72] Ensure there are no EBS Snapshots set as Public - ec2 [Critical]
.3 [extra73] Ensure there are no S3 buckets open to Everyone or Any AWS user - s3 [Critical]
.4 [extra74] Ensure there are no Security Groups without ingress filtering being used - ec2 [High]
       FAIL! us-east-1: sg-01ba67565a7a5e747 has no ingress filtering and it is being used!
       FAIL! us-east-1: sg-069b8352114c8c796 has no ingress filtering and it is being used!
       FAIL! us-east-1: sg-0f1cd175a34c76f99 has no ingress filtering and it is being used!
```

Using the -q switch to focus testing on only failed test results paired with -g to focus on specific testing groups allows for a quick, efficient and effective use of Prowler. Tests Extra71-73 are displayed but not actually assessed by the tool.

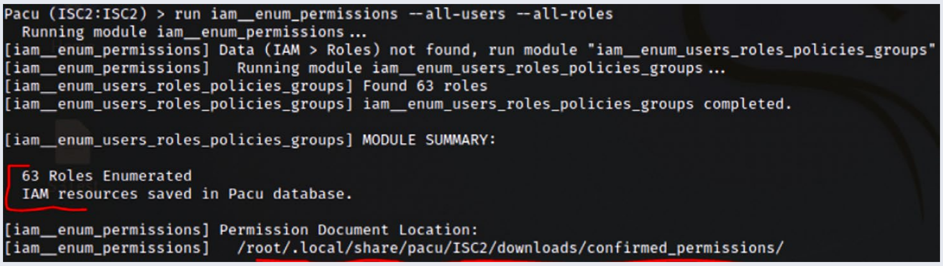
scripting and assessing adequacy of Transport Layer Security (TLS) configuration. It includes an intercepting proxy for more tactical-based network traffic inspections.

Vega does require that Java8 be installed and then set as the current version, so keep this in mind during installation and use. Vega scan results should be jointly assessed with internal stakeholders and the pen test team to filter out false positives and determine which vulnerabilities deserve threat modeling effort and remediation prioritization. *(See Figures 1 and 2 for a basic Vega scan configuration and displayed results.)*

Pivoting into the target AWS account using the supplied AWS key, internal pen test teams may perform

CONTENTS

FIGURE 5 – **ENUMERATING IAM WITH PACU**



```
Pacu (ISC2:ISC2) > run iam__enum_permissions --all-users --all-roles
  Running module iam__enum_permissions ...
[iam__enum_permissions] Data (IAM > Roles) not found, run module "iam__enum_users_roles_policies_groups"
[iam__enum_permissions]   Running module iam__enum_users_roles_policies_groups ...
[iam__enum_users_roles_policies_groups] Found 63 roles
[iam__enum_users_roles_policies_groups] iam__enum_users_roles_policies_groups completed.

[iam__enum_users_roles_policies_groups] MODULE SUMMARY:

  63 Roles Enumerated
  IAM resources saved in Pacu database.

[iam__enum_permissions] Permission Document Location:
[iam__enum_permissions]   /root/.local/share/pacu/ISC2/downloads/confirmed_permissions/
```

Useful details on IAM user accounts, their group memberships and permissions levels are captured by Pacu and saved locally. This data may be useful for social engineering or other credential-based attacks like password brute forcing if multifactor authentication is not enabled or weak password policies are enforced.

Pacu is also excellent at evading AWS GuardDuty by changing its user agent data upon starting the tool.

a more thorough analysis of potential targets and resources within the AWS account using Prowler. A command-line security auditing tool, Prowler performs approximately 150 individual checks against recognized security and privacy standards like Center for Internet Security (CIS), SOC2 and HIPAA.

Prowler leverages the AWS command line interface (CLI) under the covers to perform its checks, so installation of the AWS CLI is an installation prerequisite. Invoking Prowler requires some caution. Using the base './prowler' command will run all 150 checks for both controls that are adequately secured and those that fail. That produces a lot of noise, wasting precious test and analysis time. Internal penetration testers and malicious actors are interested in where the vulnerable resources and control failures are, so a better use of time is focusing on specific checks of interest to meet engagement objectives—and only the checks that produce failures. Use of the -q switch limits results to only failed checks, and the -g switch focuses on specific groups of controls to assess allowing Prowler assessments to focus strictly on risky AWS resources. *(See Figures 3 and 4.)*

ENUMERATING IAM USERS WITH PACU

Developed by Rhino Security, Pacu is a command-line, Python-based exploitation framework that focuses specifically on providing an end-to-end solution for internal security teams to simulate an AWS cyber breach across the entire cyber kill chain.

Similar to Prowler, Pacu leverages compromised AWS credentials to perform its assessments and provides the penetration testing team (or would-be attackers) numerous modules to execute a variety of attacks on AWS resources.

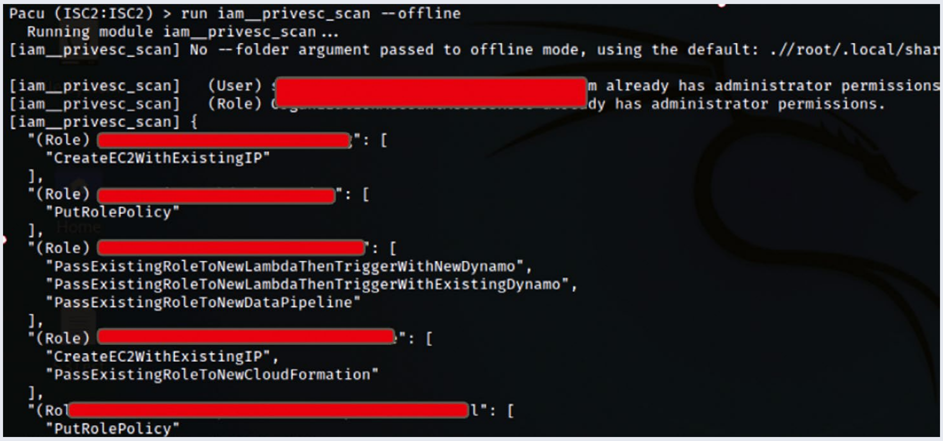
Pacu is also excellent at evading AWS GuardDuty by changing its user agent data upon starting the tool. Beginning with identity and access management (IAM), Pacu's first beneficial use is to enumerate the current privileges offered by the provided (leaked) credentials, fully enumerate all other IAM users or roles within the account and see if current access can be escalated to an administrative level.

In Figure 5, the 'run iam__enum_permissions –all-users –all-roles' command is issued performing full enumeration of AWS IAM users and roles, producing results in a JSON format. A follow-up command to enumerate all resources in the account is 'run aws__enum_account.' Pacu also provides the ability to enumerate spend reports, specific services like EC2 or S3, and download EC2 user metadata for analysis to find additional or alternate avenues of access compromise.

CONTENTS

> **Attempting privilege escalation will present all available options to the penetration testing team with prompts provided as necessary.**

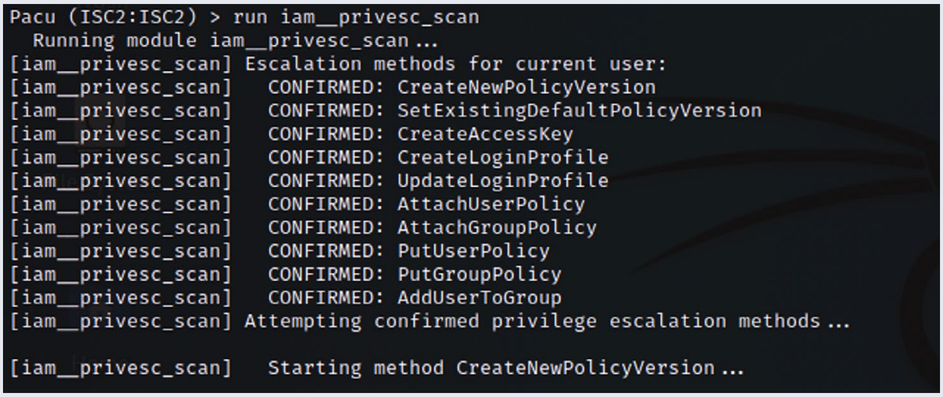
FIGURE 6 – **IDENTIFYING PRIVILEGE ESCALATION VECTORS WITH PACU**



```
Pacu (ISC2:ISC2) > run iam__privesc_scan --offline
  Running module iam__privesc_scan ...
[iam__privesc_scan] No --folder argument passed to offline mode, using the default: .//root/.local/shar

[iam__privesc_scan]   (User) [redacted]m already has administrator permissions
[iam__privesc_scan]   (Role) dy has administrator permissions.
[iam__privesc_scan] {
  "(Role) [redacted]": [
    "CreateEC2WithExistingIP"
  ],
  "(Role) [redacted]": [
    "PutRolePolicy"
  ],
  "(Role) [redacted]": [
    "PassExistingRoleToNewLambdaThenTriggerWithNewDynamo",
    "PassExistingRoleToNewLambdaThenTriggerWithExistingDynamo",
    "PassExistingRoleToNewDataPipeline"
  ],
  "(Role) [redacted]": [
    "CreateEC2WithExistingIP",
    "PassExistingRoleToNewCloudFormation"
  ],
  "(Rol[redacted]l": [
    "PutRolePolicy"
```

Pacu's Privilege Escalation scan details existing IAM users or roles that have an available path for access abuse via escalation. Any results of this command should be investigated with internal stakeholders to determine risk and required mitigation.

FIGURE 7 – **ATTEMPTING PRIVILEGE ESCALATION WITH PACU**



```
Pacu (ISC2:ISC2) > run iam__privesc_scan
  Running module iam__privesc_scan ...
[iam__privesc_scan] Escalation methods for current user:
[iam__privesc_scan]   CONFIRMED: CreateNewPolicyVersion
[iam__privesc_scan]   CONFIRMED: SetExistingDefaultPolicyVersion
[iam__privesc_scan]   CONFIRMED: CreateAccessKey
[iam__privesc_scan]   CONFIRMED: CreateLoginProfile
[iam__privesc_scan]   CONFIRMED: UpdateLoginProfile
[iam__privesc_scan]   CONFIRMED: AttachUserPolicy
[iam__privesc_scan]   CONFIRMED: AttachGroupPolicy
[iam__privesc_scan]   CONFIRMED: PutUserPolicy
[iam__privesc_scan]   CONFIRMED: PutGroupPolicy
[iam__privesc_scan]   CONFIRMED: AddUserToGroup
[iam__privesc_scan] Attempting confirmed privilege escalation methods ...

[iam__privesc_scan]   Starting method CreateNewPolicyVersion ...
```

Removing the –offline switch from Pacu's Privilege Escalation scan command will turn the command toward assessing and executing a privilege escalation scan against the current user credentials being used within the tool.

ATTEMPTING PRIVILEGE ESCALATION AND ESTABLISHING PERSISTENCE

Using the 'run iam__privsec_scan –offline' command, Pacu will produce a report showing the privilege escalation paths available within the account for all IAM users and roles. Removing the –offline switch will run the privilege escalation module for the current user account.

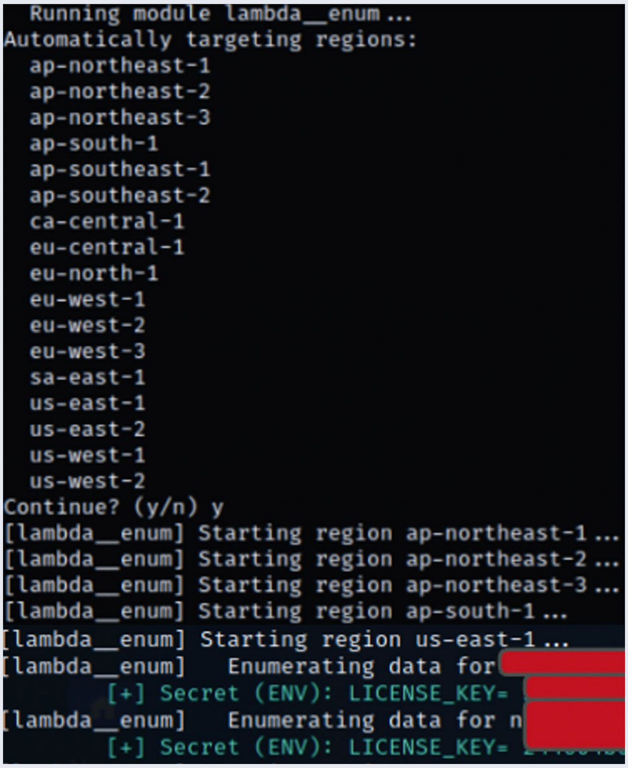
The first command has tremendous value and should be reviewed with internal stakeholders even if the current user fails to escalate privileges. Why? Because it may highlight instances where other IAM user accounts or roles have unnecessary access permissions that should be removed.

Attempting privilege escalation will present all available options to the penetration testing team with prompts provided as necessary. Once escalated privileges are achieved the module stops.

Persistence may be achieved in several ways depending on how privileged access was obtained. One method is to create a primary or secondary IAM key under another existing IAM user in the account if allowed. *(See Figures 6 and 7.)*

CONTENTS

FIGURE 8 – **ENUMERATING AND EXPOSING SECRETS IN LAMBDA FUNCTIONS**



```
  Running module lambda__enum...
Automatically targeting regions:
  ap-northeast-1
  ap-northeast-2
  ap-northeast-3
  ap-south-1
  ap-southeast-1
  ap-southeast-2
  ca-central-1
  eu-central-1
  eu-north-1
  eu-west-1
  eu-west-2
  eu-west-3
  sa-east-1
  us-east-1
  us-east-2
  us-west-1
  us-west-2
Continue? (y/n) y
[lambda__enum] Starting region ap-northeast-1...
[lambda__enum] Starting region ap-northeast-2...
[lambda__enum] Starting region ap-northeast-3...
[lambda__enum] Starting region ap-south-1...
[lambda__enum] Starting region us-east-1...
[lambda__enum]   Enumerating data for [redacted]
        [+] Secret (ENV): LICENSE_KEY= [redacted]
[lambda__enum]   Enumerating data for n[redacted]
        [+] Secret (ENV): LICENSE_KEY=
```

Pacu's Lambda Enumeration module is useful for quantifying where functions exist and if unsafe practices such as storing access credentials or license keys in environment variables within functions are occurring. Two license keys were exposed in the above example.

ENUMERATING S3 BUCKETS AND DOWNLOADING PUBLICLY ACCESSIBLE CONTENT

Pacu also provides a 'run s3__download_bucket' command that allows it to enumerate and download S3 bucket content.

If the previous IAM privilege escalation attack was successful, it is likely admin privileges were achieved and it's game over already. An online web tool called GrayHatWarfare provides the external discovery of publicly accessible S3 buckets that may allow attackers to access the contents remotely to either inappropriately access or modify data depending on bucket permissions. GrayHatWare bucket searches use keyword strings to locate publicly accessible buckets. Simply enter a company name or common terminology seen on company webpages or social media sites and you may produce buckets of interest.

Using Pacu or GrayHatWarfare for routine S3 reviews ensures inappropriate public access to buckets is identified and quickly remediated where necessary.

ENUMERATING AND ABUSING LAMBDA FUNCTIONS

Pacu's Lambda enumeration module is useful for revealing upfront whether secrets (license keys, access keys, etc.) are being stored within environment variables, which may grant escalated access to the current AWS environment or to external applications and systems.

If the enumeration command doesn't reveal secrets upfront, Lambda is architected to be quite promiscuous with what it is willing to share through the download and inspection of stored code associated to Lambda functions.

Using Bandit, static analysis of Python code may reveal exploitable vulnerabilities that can be leveraged for lateral movement, data exfiltration or privilege escalation. Within Pacu, issuing the 'aws lambda get-function –function-name <name> –profile <pacu profile> –region <function region>' will provide the download URL for the functions code.

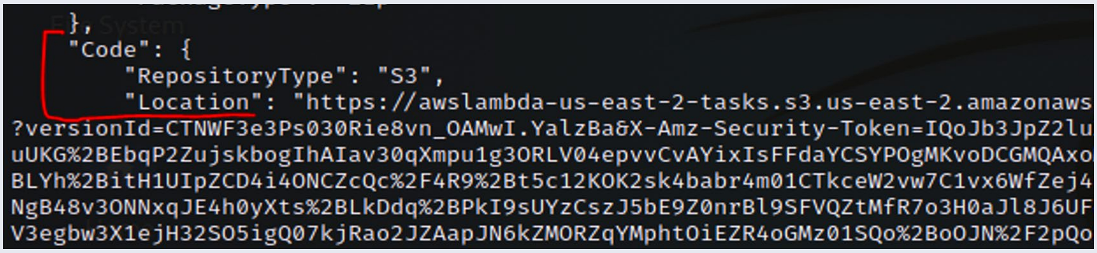
Once in the directory containing the extracted Lambda code, Bandit is executed using the command 'bandit -r <vulnerable function name.py>' to perform static application security testing (SAST) or static code scanning. Review potential items of interest with internal stakeholders as SAST scanning tools are prone to a high volume of false positives. Further inspection of Lambda event source mappings and resource policies using the AWS CLI may reveal predictable routines or execution schedules that can be exploited for expanded environment access. *(See Figures 8 through 11.)*

ENUMERATING, SCANNING AND BRUTE FORCING RDS DATABASES

Pacu's 'rds__explore_snapshots' command allows for the automated enumeration and copying of RDS database instance snapshots, satisfying numerous data exfiltration needs for attackers, such as every region where a database resides. The AWS CLI and the 'aws rds describe-db-instances --region <enter region name>' command, paired with NMAP scans, can be used to further enumerate RDS instances, service versions and open ports that

CONTENTS

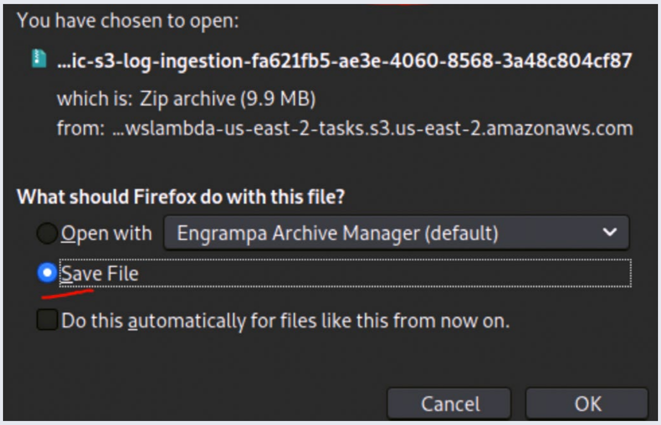
FIGURE 9 – **PUBLIC URL FOR LAMBDA CODE**



```
    },
    "Code": {
        "RepositoryType": "S3",
        "Location": "https://awslambda-us-east-2-tasks.s3.us-east-2.amazonaws
?versionId=CTNWF3e3Ps030Rie8vn_OAMwI.YalzBa&X-Amz-Security-Token=IQoJb3JpZ2lu
uUKG%2BEbqP2ZujskbogIhAIav30qXmpu1g3ORLV04epvvCvAYixIsFFdaYCSYPOgMKvoDCGMQAxo
BLYh%2BitH1UIpZCD4i4ONCZcQc%2F4R9%2Bt5c12KOK2sk4babr4m01CTkceW2vw7C1vx6WfZej4
NgB48v3ONNxqJE4h0yXts%2BLkDdq%2BPkI9sUYzCszJ5bE9Z0nrBl9SFVQZtMfR7o3H0aJl8J6UF
V3egbw3X1ejH32SO5igQ07kjRao2JZAapJN6kZMORZqYMphtOiEZR4oGMz01SQo%2BoOJN%2F2pQo
```

Enumerated Lambda functions can be viewed in more detail and have their stored code downloaded for offline static analysis using Bandit. Simply copy and paste the Location URL for the code in a web browser, unzip it and scan it with Bandit.

FIGURE 10 – **DOWNLOADING LAMBDA CODE**



You have chosen to open:

...ic-s3-log-ingestion-fa621fb5-ae3e-4060-8568-3a48c804cf87

which is: Zip archive (9.9 MB)
from: ...wslambda-us-east-2-tasks.s3.us-east-2.amazonaws.com

What should Firefox do with this file?

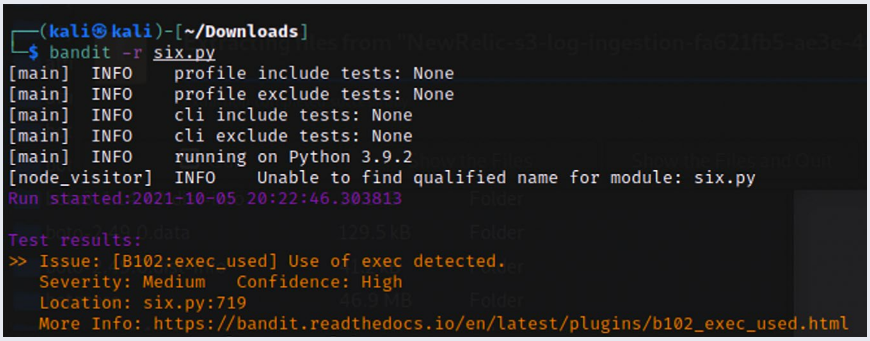
○ Open with Engrampa Archive Manager (default)

● Save File

□ Do this automatically for files like this from now on.

An example for demonstration purposes of the prompt to download code associated to enumerated Lambda functions.

FIGURE 11 – **STATIC ANALYSIS WITH BANDIT**



```
┌──(kali㉿kali)-[~/Downloads]
└─$ bandit -r six.py
[main]  INFO    profile include tests: None
[main]  INFO    profile exclude tests: None
[main]  INFO    cli include tests: None
[main]  INFO    cli exclude tests: None
[main]  INFO    running on Python 3.9.2
[node_visitor]  INFO    Unable to find qualified name for module: six.py
Run started:2021-10-05 20:22:46.303813

Test results:
>> Issue: [B102:exec_used] Use of exec detected.
   Severity: Medium   Confidence: High
   Location: six.py:719
   More Info: https://bandit.readthedocs.io/en/latest/plugins/b102_exec_used.html
```

Bandit performing static analysis of stored code in the Lambda function. A medium issue is flagged along with reference documentation describing the vulnerability detected.

further identify potential vulnerabilities while enabling exploitation of the database. Based upon the results of enumeration, information including the master username, encryption status of the RDS instance and other useful details may be revealed to support password brute forcing or other attacks.

What I've outlined is a basic approach to assessing a small fraction of what's available within AWS using simple techniques that may be used to exploit an AWS environment leveraging leaked access keys. Routine assessments from both an internal and external penetration testing angle may assist in the early identification and remediation of exploitable vulnerabilities.

To achieve positive security outcomes, security teams should focus time and resources adopting offensive security techniques and tools to mimic their adversaries. They should seek to understand AWS weak points from a holistic control perspective and communicate relevant risks to internal stakeholders for timely remediation. A special thanks to Rhino Security, Packt publishing, Subgraph and all those wonderful white hats out there helping us security folks get smarter through collaboration. ●

Adam Kohnke, CISSP, has more than 12 years of experience in IT operations, incident management, IT audit and information security management. He is currently a cybersecurity architect for Charter Next Generation where he oversees the company's information security policies, processes and technologies.

CONTENTS

NO ONE SAID IT WAS EASY

A vCISO reflects on lessons learned, especially when it comes to risk assessments. **BY BRIAN GRAYEK, CISSP**

ILLUSTRATION BY ALISON SEIFFER

HAVING MORE THAN 40 YEARS in the information security industry gives a person a unique view on the profession.

I've presented to audiences all over the world. One thing I learned, particularly while speaking in China years ago, shaped how I would explain any complicated topic, including concepts surrounding cybersecurity, to any audience, not just one of my peers.

The Chinese often speak with metaphors and similes, such as "being flexible like bamboo" or "happiness is the best cosmetic." In those few words, they convey much about a subject or person to someone both inside and outside of a field or discipline. I learned from them an effective way to explain a complex theory or concept to someone who may not be as technical as I am. I use a simple metaphor—emphasis on the simple. Don't overcomplicate.

CONTENTS

One of my personal favorite expressions when discussing information security is: "Why bother to lock the doors if you've left the windows open?" In other words, why go through all the trouble of doing something we all should be doing (locking our doors) to protect yourself from theft if someone else (or you) is going to leave the windows open for a burglar to easily use?

If you're having difficulty getting through to people in your office or even family members at home who fail to follow established best practices in cybersecurity, consider changing how you communicate with them. Use more examples and anecdotes and see that look of recognition when they finally get what needs to be done—and then go and do it.

One of my personal favorite expressions when discussing information security is: "Why bother to lock the doors if you've left the windows open?"

MENTOR AND COACH

In my various executive management positions, I've enjoyed being a mentor and coach to those with less experience or new to the industry. I believe it's important that those of us with tenure in cybersecurity make the time to guide those coming up the ranks. It's good for our organizations, communities and for our own individual growth and professional legacy.

During my five years at telecom giant Verizon, I worked on the annual Verizon Data Breach Investigations Report, a highly anticipated research study on current data breaches. One of the most gratifying moments in my career came from audience members later telling me they decided to go into information security after hearing me speak about that report.

To have that type of impact, you need to be a great speaker. And, in addition to speaking clearly and with authority, you need to convey passion for your work and a willingness to share your wisdom. That will help you migrate from an information security subject matter expert to an industry influencer.

I've also been involved in some of the largest information security investigations, stopping two of the largest bot herders in another country, and presenting with the director of the U.S. Federal Bureau of Investigation and others on the White House Strategy to Secure Cyberspace. We are all bound not just by our skills, but by wanting to make our worlds safer—and better.

SHARE WHAT YOU LEARN

During a recent webinar, I mentioned that with all the government and industry regulations to date, the only one that has really been successful is PCI. It basically has teeth that other U.S. security and privacy legislation still lacks. If a company handling credit card information is found to violate PCI DSS guidelines for information security, your ability to continue processing credit card transactions will heavily influence the business's solvency. Who doesn't now accept credit and debit card payments, especially since the pandemic discouraged certain cash transactions?

People will argue that some regulations, like SOX or HIPAA, have improved security. And newer regulations and laws like the EU's General Data Protection Regulation and U.S. state equivalents contribute to an increase in overall security and privacy posture. Yet how often do we hear of a major data breach at an organization that failed to follow regulatory or legislative mandates surrounding cybersecurity and consumer privacy?

I've seen firsthand the initial resistance to some massive government entity forcing compliance through legislation. If we want to achieve mass compliance, we need to make regulations simple to follow and provide incentives for companies to adopt guidelines because they are advantageous to them, not just their customers. And, above all, whatever is required must be actionable and measurable.

ADHERE TO BASICS AND BEST PRACTICES

One of the most basic practices we all face is the ability to fully patch our systems in order to reduce the risk of attacks and zero-day exploits. Every day there are more and more vulnerabilities found than companies can quickly and easily install patches for. We are, as a profession, literally drowning in the backlog of patching.

It's overwhelming. And when we're continually fighting to keep up, we tend to partially surrender and prioritize patching to seal the security holes most likely to cause us harm and save the rest for later. Software will always be released with unknown vulnerabilities, and we've made strides within DevSecOps to embed security during a product's development. But unpatched systems remain one of the most widely used methods of breaking into networks.

About half of my career has been in the operational side of information security, helping make my employer more secure. The other half has been on the services side, offering products or services to help secure a company. I found that I prefer being on the "helping side" working for a consulting company that supports multiple organizations, over working for a single company as their security expert.

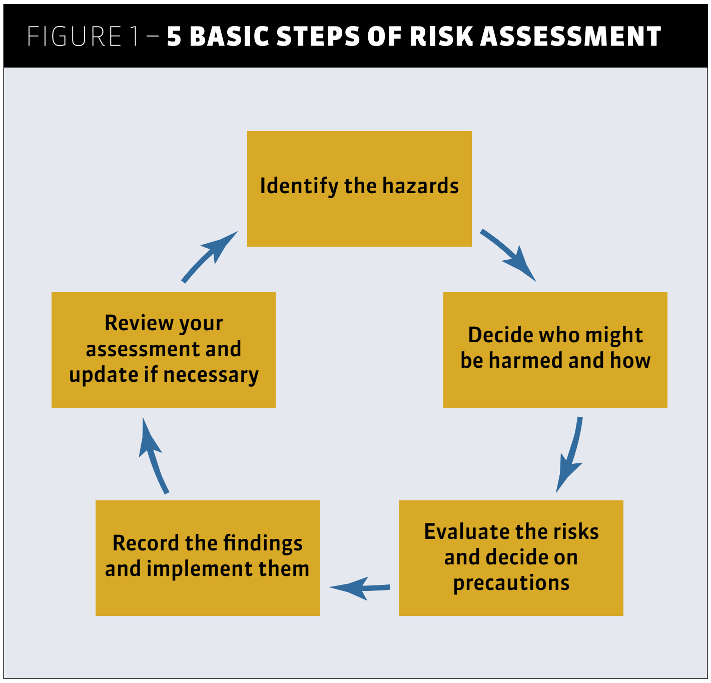
COMPLIANCE IS NOT SYNONYMOUS WITH SECURE

I'm currently a virtual CISO for a company that assists small to mid-sized businesses in becoming information security compliant with various regulations (SOC, CMMC, ISO 27001, etc.). Or, they may just want to improve their overall security posture through our fractional CISO services. I only mention my role as it is significant to this article.

In this role, I've learned that many companies go to great lengths to put intricate plans in place for attacks that are relatively rare, while not taking minimal efforts to thwart vectors using tools that are widely known to work. Why? Because they are trying to be "compliant," as that is perceived as the only path forward.

One of the first things we recommend to any company that doesn't know its current cybersecurity posture, or wants to know how much it will take to meet the various, recent compliance standards, is to arrange for a fairly simple risk assessment.

FIGURE 1 – **5 BASIC STEPS OF RISK ASSESSMENT**


Identify the hazards
Decide who might be harmed and how
Evaluate the risks and decide on precautions
Record the findings and implement them
Review your assessment and update if necessary

Most cybersecurity professionals know the important role of a risk assessment, especially one based on a set of established standards or frameworks such as those offered by NIST. This is a great way to start down the path to a more secure infrastructure.

But how do we get more companies to understand just how much they can gain from the assessment? After completing a recent risk assessment, I was struck by the thought: Are we assessing against the right criteria? We were using the latest NIST risk assessment tools developed by government and industry experts. They must know the best way to perform a risk assessment.

That's when I returned back to the basics. *(See Figure 1.)*

The five basic steps to any risk assessment are easy to understand, if not always simple to apply.

START BY IDENTIFYING HAZARDS

It's important to note a NIST-based risk assessment, or any entity's version of a risk assessment,

CONTENTS

includes that organization's definitions of hazards, harms and recommended remediations.

Recalling my earlier metaphor about securing your house doors while leaving windows open to intruders, I reexamined the results from every recent industry security report I could access online to see if the NIST-based assessment was looking at the same vectors that criminals were using to infiltrate our systems. To my amazement … they weren't. The shocking discovery led me to then compare the list of intrusions from the industry reports against other regulations such as HIPAA, SOX, CMMC, FAR, DFAR and others. While some capture "elements," none of them covered them all—even when an organization follows the rules and regulations of all at the same time. *(See Figure 2.)*

Figure 3 is a list of the primary industry industry regulations that are meant to eliminate those intrusions through the introduction of controls that target those specific intrusion vectors. Note that each regulation "covers" a certain number of those known vectors and partially overlaps with other regulations.

Then last, Figure 4 demonstrates the "gap" of the known intrusion vectors when you apply many of these known regulation controls. There appears to be a significant gap in the coverage of the regulations when comparing them to the known intrusion vectors.

This illustrates a problem when enterprises falsely believe being compliant is the same as being secure. It also explains why it is so important to develop and regularly deploy dynamic risk assessments that boil down the most important controls from all the regulation and cross-identify them against the majority of known attack vectors (methods) to come up with a smaller and actionable list of risks that any company can use as a guide to know what they should fix in priority order. *(See Table 1.)*

FIGURE 2 – **ALL THE VARIOUS INTRUSION VECTORS FROM ALL THE SECURITY REPORTS**

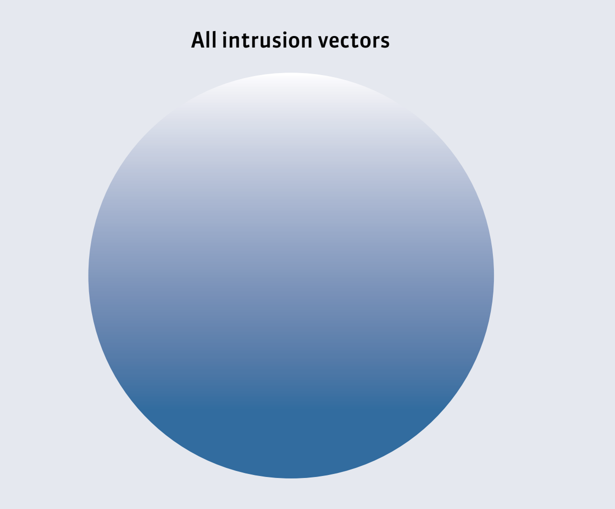


FIGURE 3 – **PRIMARY REGULATIONS THAT IMPACT INFORMATION SECURITY**

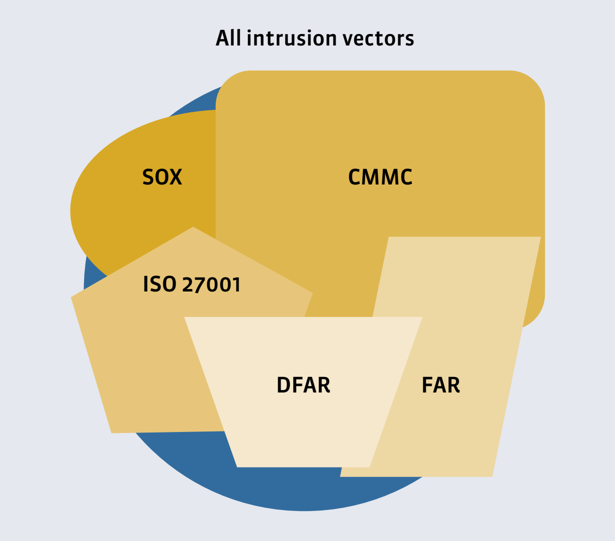


FIGURE 4 – **THE "GAP" OF THE KNOWN INTRUSION VECTORS**

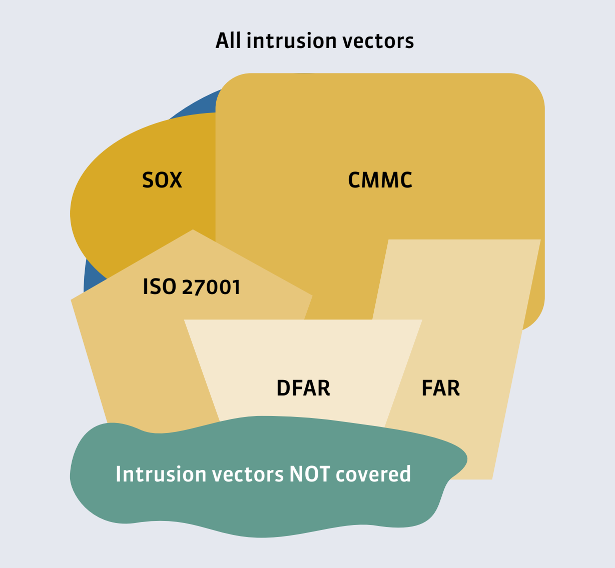


TABLE 1 – **EXAMPLE OF ALIGNING RISK ASSESSMENTS WITH CURRENT THREATS**

Attack Vector	Method of Protection
Phishing Attack with Ransomware	Email Filtering
	Security Awareness Training
	Computer Systems backup – offline
	Multi-Factor Authentication

One thing that years of experience has taught me is that if we take advantage of what we already know and apply the same methodologies we've successfully used in the past, then eventually we all land on a workable solution.

Our company now refers to this as our Essential Risk Assessment.

We've found that we can review this relatively small list with a potential customer and within hours know where that customer should focus efforts to reduce their cybercrime risks in the greatest ways possible, in the shortest time, and at the least cost. Our customers are seeing immediate reduction in risks against the most prevalent intrusions for very little costs. Not a silver bullet, but more like body armor for the business.

I would invite others to investigate for themselves the controls of the most important security frameworks, along with any security report they can come across, and I'm quite confident that they'll find the same thing.

One thing that years of experience has taught me is that if we take advantage of what we already know and apply the same methodologies we've successfully used in the past, then eventually we all land on a workable solution. Whether it's for analyzing threats, preventing attacks, or in this case, assessing risks. ●

BRIAN GRAYEK, CISSP, currently is a virtual CISO for a cybersecurity agency based in Arizona.

Here's to the Futures

BY MICHAEL HANNA, CISSP

Current and aspiring technology and security leaders undoubtedly know that strategic thinking is one of the most important traits of a successful leader. Without this skill, it is extremely difficult, even impossible, to operate effectively at the senior level. I argue that this is a characteristic that can be developed with training and using the right tools. One such tool is the use of a futures mindset and framework, which stems from research in the futures studies field. At the executive level, futures is a highly strategic function that promotes significant positive outcomes for the organization, your department and your personal achievement.

Before going any further, let's get a few things straight. There are three laws to futures implementation that must be kept in mind:

The future is not predetermined. A single predetermined future is never inevitable or fate. There are many potential futures, and it is our job to assess these possible outcomes.

The future is not predictable. Futures are not about predicting the future, nor can we expect this to occur at any level of precision. Even if a future was predetermined, it is not possible to collect the necessary data to develop a model of explanation for the predetermined future. Relax, we are not trying to become fortune tellers.

Future outcomes can be influenced. The future can be shaped by our actions today, but it is important to remember that every action has a consequence (positive or negative) and should be chosen after considerable consideration. We can foster a desired future throughout society and the organization.

When we explore possible, plausible, probable and preferable futures, leveraging a systematic framework will generate well-conceived outcomes and promote the strategic plan for leaders to steer toward a desired future outcome. If you are new to futures thinking, there are four additional concepts I would like to leave you with:

Mapping and scanning. Examine the past, present and future. The past and present provide us with clues as to how events have unfolded. Couple this with the examination of emerging signals and information sources around us and we can begin formulating potential outcomes. Here's an example to tie this concept together. Currently, we are in the fourth industrial revolution. By examining societal and economic events from past industrial revolutions and correlating them with today's culture, technology and global economy, we can begin to paint pictures of the future.

Interpretation, anticipation and creation. Analyze scanning hits for significant findings to produce appropriate plans and policies to support later phases of the framework. Seek to identify potential future issues, opportunities and disrupters within your problem space. For example, with the explosive growth of artificial intelligence, potential issues may include lack of workforce support due to perceived reduction of employment. The use of causal layered analysis is beneficial in creating possible futures.

Transforming the future. Remember Law No. 3? Future outcomes can be influenced. Select the desired outcome and deliberately take actions to inspire stakeholders toward the end game. We've all heard the importance of change management, right?!

Whether you are a strategic chess mastermind or developing this skill toward your journey to the C-suite, the use of futures thinking can take you to the next level. Give it a try. Your future self might thank you. ●

Dr. Michael Hanna is a leader and a university professor within the field of information technology and cybersecurity. He specializes in developing high-performing teams, artificial intelligence and cybersecurity. You can reach him on LinkedIn at Michael Hanna. The views expressed here are solely those of the author, and do not necessarily reflect those of the Department of the Navy, Department of Defense or the United States government.

CONTENTS