

THERE'S MORE THAN ONE WAY TO NETWORK

InfoSecurity PROFESSIONAL

A Publication for the (ISC)²® Membership

NOVEMBER/DECEMBER 2019

ON THE HUNT

Is your security operation
ready to track down threats?

UNDER ATT&CK

MITRE's threat modeling tool

SECURE SOFTWARE

How to add more
protections



(ISC)²

Free Courses & CPEs for Members

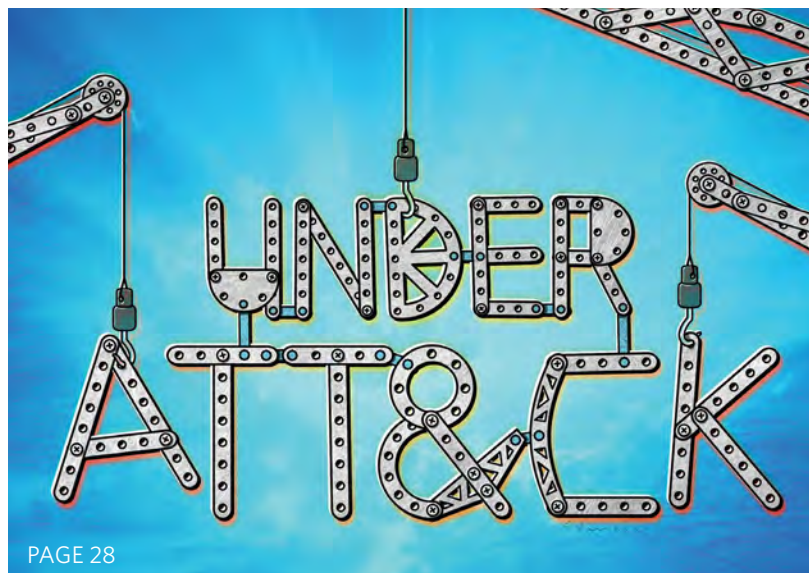
The (ISC)² Professional Development Institute (PDI) takes you beyond your certification with a portfolio of professional development courses and you earn **FREE CPEs**.

Course Types Include:

- **Immersive** – In-depth training on a variety of relevant and timely cybersecurity topics delivered in an online, self-paced format.
- **Lab** – Hands-on courses that enable learners to practice specific technical skills.
- **Express Learning** – Self-paced, short-format courses with on-the-go professionals in mind.

Earn Free CPEs

To receive communications when new courses are released, log in to your (ISC)² account and update your communication preferences to include Continuing Education & Professional Development.



PAGE 28

departments

4 EDITOR'S NOTE

There's More than One Way to Network

BY ANNE SAITA

6 EXECUTIVE LETTER

The Critical Importance of Updating Our Exams

BY CASEY MARKS

8 FIELD NOTES

This year's (ISC)² scholars; easing the pain of ransomware; recommended reading; and more.

16 #NEXTCHAPTER

(ISC)² Peru Chapter

18 ADVOCATE'S CORNER

Remembering Where We Come From

BY TONY VIZZA

43 CENTER POINTS

Is it Time We Made Time to Do More?

BY PAT CRAVEN

44 COMMUNITY

Advice on wiping machines and choosing between SHA-1 and SHA-2

4 AD INDEX

features

THREAT DETECTION

20 Threat Hunting

Is your security operation ready to launch such a program?

BY MATT GILLESPIE

THREAT MODELING

28 Under ATT&CK

How MITRE's methodology to find threats and embed countermeasures might work in your organization.

BY NARESH KURADA, CISSP

SOFTWARE DEVELOPMENT

36 Let's Work Together

An (ISC)² member details a software security integration system that eliminates that '50-page security policy' for developers.

BY MICHAEL BERGMAN, CISSP

Cover image: TAYLOR CALLERY | Illustration above: ENRICO VARRASSO

InfoSecurity Professional is produced by Twirling Tiger® Media, 7 Jeffrey Road, Franklin, MA 02038. Contact by email: asaita@isc2.org. The information contained in this publication represents the views and opinions of the respective authors and may not represent the views and opinions of (ISC)²® on the issues discussed as of the date of publication. No part of this document print or digital may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of (ISC)². (ISC)², the (ISC)² digital logo and all other product, service or certification names are registered marks or trademarks of the International Information Systems Security Certification Consortium, Incorporated, in the United States and/or other countries. The names of actual products and companies mentioned herein may be the trademarks of their respective owners. For subscription information, please visit www.isc2.org. To obtain permission to reprint materials, please email infosecproeditor@isc2.org. To request advertising information, please email lpettograsso@isc2.org. ©2019 (ISC)² Incorporated. All rights reserved.

There's More than One Way to Network

SEVERAL YEARS AGO, I showed up at a security conference social as a favor for a friend, who ended up being a no-show. I didn't know a soul in the place, so I grabbed a cocktail and plate of finger foods and sat alone at a table to sulk and sort out my evening.

Soon someone asked to join me, and we sat there eating our hors d'oeuvres without uttering a word. Then another person sat in on our little silent retreat. We concentrated on our food and on the conversations around us. Finally, I stood up to leave.

"Nice networking with you," one of my tablemates deadpanned. To this day, I don't know if he was being silly or serious.

What I do know is that pretty much everyone hates networking at some point in their careers. It can be difficult to stand alone in a crowd or to carry a conversation even among willing participants.

Organizational psychologist Adam Grant understands this reluctance and offers other ways to both broaden and strengthen our circle of contacts. One suggestion is to master a craft. It doesn't matter what you choose; just really know your stuff and share that wisdom with those who seek it, some of whom are current or future influencers. They'll remember you and recommend you when you need a referral.

Another underappreciated strategy: Be dependable on the job and volunteer in your company or community. By taking on extra work or going the extra mile, you'll elevate your reputation and earn promotions with the help of people who vouch for you.

There are, of course, plenty of opportunities to employ both of these networking tactics as (ISC)² members. You can join a chapter and help with local events. You can expand your influence online. You can submit articles for consideration in this membership magazine. Whether you prefer talking shop at a Security Congress mixer or assisting a peer with a problem on the Community Forum, the key is to share what you know and take in what you don't. ■



Anne Saita, editor-in-chief, lives and works on the U.S. West Coast. She can be reached at asaita@isc2.org.

(ISC)² MANAGEMENT TEAM

EXECUTIVE PUBLISHER

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

SENIOR MANAGER, CORPORATE COMMUNICATIONS

Jarred LeFebvre
727-316-8129
jlefebvre@isc2.org

CORPORATE PUBLIC RELATIONS MANAGER

Brian Alberti
617-510-1540
balberti@isc2.org

CORPORATE COMMUNICATIONS LEAD

Kaity Eagle
727-683-0146
keagle@isc2.org

EVENTS AND MEMBER PROGRAMS MANAGER

Tammy Muhtadi
727-493-4481
tmuhtadi@isc2.org

SALES

VENDOR SPONSORSHIP

Lisa Pettograsso
lpettograsso@isc2.org

EDITORIAL ADVISORY BOARD

Anita Bateman, U.S.
Kaity Eagle, (ISC)²
Jarred LeFebvre, (ISC)²
Yves Le Roux, EMEA
Cesar Olivera, Brazil and Canada

TWIRLING TIGER MEDIA EDITORIAL TEAM

EDITOR-IN-CHIEF

Anne Saita
asaita@isc2.org

ART DIRECTOR & PRODUCTION

Maureen Joyce
mjoyce@isc2.org

MANAGING EDITOR

Deborah Johnson

PROOFREADER

Ken Krause



Twirling Tiger[®] Media (<https://twirlingtigermedia.com>) is a women-owned small business. This partnership reflects (ISC)²'s commitment to supplier diversity.

ADVERTISER INDEX

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

(ISC) ² Professional Development Institute..... 2	(ISC) ² Vulnerability Central.....19	WALLIX.....34
(ISC) ² Training - CCSP Practice Quiz..... 5	MCPc.....19	Amazon Web Services (AWS)..... 35
Enterprise Security & Risk Management..... 7	(ISC) ² Community.....22	Egress.....39
San Jose State University.....11	ExtraHop Networks.....23	Hitachi ID Systems.....44
SecurityMetrics, Inc.....12	Armis.....24	BSI Group America Inc.....45
Purdue University Global.....13	IOR Analytics.....25	ISHPI.....46
Training Camp.....17	Galvanize.....26	Center for Cyber Safety and Education.....47
	Qualys.....27	Cloud Security Alliance.....48
	Acceptto Corporation.....29	
	eSentire.....33	



Certified Cloud
Security Professional
An (ISC)[®] Certification

Are You Cloud Security SAVVY?



Get Ready for
Exam Day

[Take the Free Quiz](#)

The Critical Importance of Updating Our Exams

by Dr. Casey Marks

PART OF THE RESPONSIBILITY that (ISC)² takes on behalf of its more than 140,000 members is to routinely assess the content of its exams and ensure that they cover topics that are relevant and reflective of the current roles and responsibilities undertaken by cybersecurity professionals.

Why is this important? The landscape in which our members work is certainly not static, so neither should be the certifications that are reflective of their knowledge, skills and abilities. As the gold standard for the cybersecurity industry, we need to make sure that the certifications our members hold are considered contemporary and hold up to the harshest scrutiny possible.

The time-intensive process by which these changes are determined is through a detailed Job Task Analysis, which pressure-tests the domains (or core disciplinary areas of focus) on which we test applicants against the emerging requirements of existing certification holders in the real-world environments they protect. This ensures that changes in cybersecurity are included in the knowledge base we're testing during our exam process. It is through updates like these that we maintain the high standards we've set for our certifications and confirm that they evolve in lockstep with what's actually required in the field—and what employers demand from their expert staff.

As part of this process, we recently announced domain refreshes to both the CCSP cloud security certification exam (<https://www.isc2.org/Certifications/CCSP>)—which took effect on August 1—and the HCISPP healthcare cybersecurity certification exam (<https://www.isc2.org/Certifications/HCISPP>)—which took effect on September 1. These are the first updates to either exam since their inception in 2015 and 2013, respectively, and the enhancements are the result of a rigorous, methodical process that (ISC)²

follows to routinely update its credential exams. The details of these changes are outlined in the CCSP Domain Refresh FAQ (<https://www.isc2.org/Certifications/CCSP/Domain-Refresh-FAQ>) and the HCISPP Domain Refresh FAQ (<https://www.isc2.org/Certifications/HCISPP/Domain-Refresh-FAQ>), both found on our website.

While these types of changes may fly under the radar, regularly assessing the rigor and relevance of our exams and preserving their integrity within the industry is of critical importance to the value of the certifications you hold.

The foundational elements of the two exams remain, but in some cases, we have added or renamed domains that are covered, and the weighting of each domain in the full tests has been refined. In the end, this means that the exams accurately reflect the deep knowledge and hands-on experience currently required for cloud security architecture, design, operations and service orchestration, and for healthcare cybersecurity governance, regulation and standards. The content aligns with the Common Body of Knowledge (CBK), which is a comprehensive framework of all the relevant subjects a security professional should be familiar with, including skills, techniques and best practices.

While these types of changes may fly under the radar, regularly assessing the rigor and relevance of our exams and preserving their integrity within the industry is of critical importance to the value of the certifications you hold. And we take that responsibility seriously. ■



Dr. Casey Marks is chief product officer and vice president at (ISC)² and can be reached at cmarks@isc2.org.

ESRM

Enterprise Security & Risk Management

whitehall
media

CONNECTING ENTERPRISE WITH BUSINESS

27 NOVEMBER 2019

Victoria Park Plaza, London

The UK's leading event for Infosec, Cyber Security and Risk Management Professionals across every major business sector.

ESRM 2019 will take place on the 27th November at the Victoria Park Plaza, London. The 9th bi-annual ESRM Conference will bring together over 500+ delegates, who are all pre-screened as Enterprise and Risk Management Decision Makers across every major business sector. The event offers unrivalled networking opportunities and insights on how to design, implement and embed deliverable action plans that balance risk mitigation with the pursuit of business growth.

REASONS TO ATTEND:

- 500+ delegates
- 98% buyers and influencers
- 20+ major suppliers
- Over 3 hours of Networking Opportunities
- Hear from key expert speakers in 8 technical and business led conference tracks, including real world use-cases and discuss your business requirements with over 70 leading technology providers and consultants



At Enterprise Security & Risk Management 2019, you will hear from thought-provoking, inspiring and industry-leading speakers. Supporting the conference sessions will be a series of keynote speakers including:



SARB SEMBHI
Former President, ISACA
London



GREG VAN DER GAAST
Head of Information Security,
University of Salford



OMER MAROOF
Head of IT Risk, Euroclear UK
& Ireland



FRANCESCO CIPOLLONE
Director of Events, Cloud
Security Alliance UK; Head
of Security Architecture &
Strategy, HSBC Global Banking
and Markets

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

(ISC)² Congratulates This Year's Cybersecurity Scholarship Winners

(ISC)² JOINS THE CENTER FOR CYBER SAFETY AND EDUCATION in applauding the outstanding students who earned cybersecurity scholarships in 2019. With the generous support of sponsors, including (ISC)², Raytheon and others, the Center is proud to assist these men and women as they prepare to help meet the critical demand for skilled cybersecurity professionals. The Center has awarded more than \$130,000 in scholarships in 2019.

The 2020 scholarship program will begin accepting applications on December 1 and close on February 17, 2020. For more information, visit <https://iamcybersafe.org/s/scholarships>.

(ISC)² WOMEN'S SCHOLARSHIPS

Sadie Levy
United States,
Northeastern University



"I am deeply appreciative of the Center for Cyber Safety and Education's support.

My goal, upon graduation from college, is to be a part of the growing numbers of women who are joining the cybersecurity workforce."

Minko Romy
Australia, University of
Oxford-Wolfson College



"As a young researcher, and particularly as a woman, this support is invaluable to my career.

I am excited to continue my studies over the next years and am extremely grateful to the Center for making it possible."

RAYTHEON CCDC WOMEN'S SCHOLARSHIP

Claire Seiler
United States, University of Florida

"This scholarship will enable me to continue pursuing combined bach-

elor's and master's degrees in computer engineering and to work toward a career in cybersecurity. I am proud to be a proponent of a mission that cultivates diversity and supports the inclusion of women in cyber."



(ISC)² UNDERGRADUATE SCHOLARSHIPS

Brendan Brown
United States,
Champlain College



"Without the help you have provided me over the past three years, I likely would not have been able to continue studying at Champlain and may have had to choose a different discipline entirely. I am truly grateful toward (ISC)² and am looking forward to giving back in the future in order to allow another student the great opportunity you have provided me."

Asha Pereira
United States, University of Pennsylvania

"I'm incredibly excited to receive this scholarship. With it, I can bridge the

cybersecurity gender gap by using my cybersecurity passion and expertise to inspire burgeoning generations of women to enter the field. I want to let girls know that information security isn't unapproachable or 'just for boys.'"



(ISC)² GRADUATE SCHOLARSHIPS

Christine Anari
Kenya,
University of Derby



"I am very grateful for this life-changing opportunity that will see me transition from a cybersecurity enthusiast to a cybersecurity analyst. Growing up in a third-world country poses a big challenge for students who wish to enroll in technology courses. I will not take the opportunity for granted because I know there are many young Kenyan men and women who share the same passion as myself who are waiting for this golden moment."

Ali Adnan
India,
Carnegie Mellon
University



"I will try to instill the nature of 'giving back' similar to (ISC)², and after completing my MS, I intend to train young professionals on tackling the various cybersecurity menaces in the digital world today. Hence, the scholarship by (ISC)² may be a small drop in the pond, but I hope its ripples may be felt for ages to come, and I will try to make sure it does happen." ■

Image: iStock



2019 (ISC)² Security Congress Keynotes Focus on More than Cyber Issues

ATTENDEES AT THIS YEAR'S SECURITY CONGRESS on October 28 through 30 in Orlando won't want to miss our keynotes. Can't attend this year's conference? No problem. We'll be posting content from the conference on the (ISC)² blog and website both during and after the event.

THE KEYNOTES

Monday, October 28, 8:30 a.m.-9:30 a.m.

Captain "Sully" Sullenberger III

In a singular, heroic moment, Capt. "Sully" Sullenberger landed his troubled jetliner in the middle of New York's Hudson River, saving all 155 passengers. A passionate advocate for airline safety, he will share not only his story, which became a popular movie starring actor Tom Hanks, but how his training and leadership led him to that moment.



Tuesday, October 29, 9 a.m.-10 a.m.

Catherine Price—Author, *How to Break Up with Your Phone*

Catherine Price advocates what she calls a "screen/life" balance. Her work has appeared in newspapers and magazines including *The Washington Post* and *O: The Oprah Magazine*. Her latest book, *How to Break Up with Your Phone*, is being published in 26 countries and translated into 18 languages.



Tuesday, October 29, Noon-1 p.m.

Erik Wahl—Author, *The Spark and the Grind*

Artist Erik Wahl's latest book, *The Spark and the Grind*, reveals what it takes to get from an idea to the action of creating. Wahl consults as a business strategist for many major corporations, including Disney, Microsoft and FedEx. He also is a philanthropist, raising millions of dollars for charity through the sale of his unique artwork.



Wednesday, October 30, 5:30 p.m.-6:30 p.m.

Admiral William H. McRaven, USN (Ret.)

William H. McRaven, a retired U.S. Navy four-star admiral, is also a former SEAL and served as commander of the operation that led to the killing of Osama bin Laden. He brings insight into today's geopolitical climate and shares his thoughts on succeeding through one's experiences. Adm. McRaven is a former chancellor of the University of Texas system and a best-selling author. ■



The increase in reported data breaches last year by U.K. financial services firms

Source: Reynolds Porter Chamberlain, LLC
<https://www.rpc.co.uk/press-and-media/data-breaches-reported-by-financial-services-firms-rise-480-percent-in-a-year-to-145/>

DEFINITION:

Credential stuffing



"...when an attacker uses long lists of stolen login credentials in large-scale automated attempts to log in to various websites. The attackers are relying on the fact that many of us use the same username and password on multiple sites. Thanks to the attacks' automated nature, even if only a small percentage of the stolen login credentials are a positive match, it can still be worth the attackers' while."

Source: CSOnline, 7 Hot Cybersecurity Trends
<https://www.csonline.com/article/3262972/7-hot-cyber-security-trends-and-4-going-cold.html>

Images: iStock

■■■ MEMBERS' CORNER

Breakable Encryption Legislation Violates the Second Amendment

by Brandon Gregory, CISSP

LAW ENFORCEMENT in the United States has been calling for breakable encryption for several years.

- Members of the United States Senate began drafting legislation for encryption with built-in backdoors in 2016, shortly after the terror attack on a San Bernardino, California, government center that killed 14 and wounded 22, when law enforcement couldn't initially gain access to the shooter's iPhone.
- In 2017, then-U.S. Deputy Attorney General Rod Rosenstein opined that unbreakable encryption places an undue burden upon law enforcement.
- In 2018, senators reached out to technology companies to better determine the impact and feasibility of such legislation.
- In July 2019, U.S. Attorney General William Barr, during a cybersecurity conference, claimed that encryption impedes law enforcement's ability to detect and prevent crimes before they occur.

This push for breakable encryption, I believe, runs afoul of the U.S. Constitution, but perhaps not for the reasons you think.

It could be argued that such a law violates the freedom of speech guaranteed by the First Amendment. Any proposed legislation would require technology companies to write code required by the government. Computer code is a language, and government-mandated verbiage has been struck down by U.S. courts before.

It could also be argued that proposed legislation violates Fourth Amendment protections against unlawful search and seizure.

The real argument, however, is that breakable encryption legislation violates the Second Amendment. Yep, you read that right, the Second Amendment, which gives Americans the right to bear arms.

Set aside the argument for gun rights—the argument that says enacting tougher gun laws only makes law-abiding citizens less safe because criminals don't obey the law.

Just focus on the Second Amendment: “A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.”

When the first 10 amendments to the U.S. Constitution (the Bill of Rights) were written in 1791, the Founding

Fathers wanted to protect citizens against governmental overreach and maladministration. What better way to protect against government overreach than to ensure that citizens have the right to obtain the tools and weapons necessary to prevent government intrusion. And that is exactly what encryption is—a tool that protects an individual's digital property.



Brandon Gregory

In a digital world, government trespass on individual rights no longer requires physical access; it can be carried out remotely, without detection.

The Second Amendment doesn't read “...the right of the people to keep and bear *firearms*,” it says “...the right of the people to keep and bear *Arms*.” Arms, meaning those tools and weapons necessary to protect individual rights from government intrusion.

Take this a step further.

Firewalls, passwords, intrusion detection and prevention systems, and anti-malware are all tools used to protect digital property. Encryption is no different. In a digital world, government trespass on individual rights no longer requires physical access; it can be carried out remotely, without detection. Digital arms must be sufficient in strength to ensure the rights of the citizen are not trampled. Breakable encryption doesn't pass that test. ■

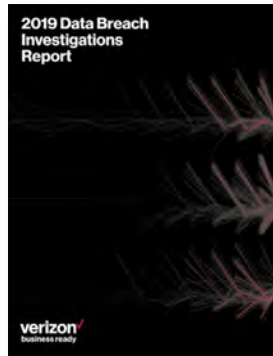
BRANDON GREGORY, CISSP, is a cybersecurity professional currently residing in Maryland. He earned bachelor's and master's degrees in cybersecurity and holds industry certifications in cybersecurity and project management.

Easing the Pain of Ransomware

by Matt Gillespie

RANSOMWARE no longer captures the headlines that it did when WannaCry suddenly spanned the globe two years ago, but the category's reign of disruption continues.

Verizon's *2019 Data Breach Investigations Report* (<https://enterprise.verizon.com/resources/reports/dbir/>) finds that ransomware is the second most prevalent type of malware. Dave Hylender, a senior risk analyst with Verizon, describes ransomware in 2019 as "prevalent and ubiquitous. It's quite lucrative for the attacker; it's high yield and low risk, and I don't expect it to be going away soon."



lent and ubiquitous. It's quite lucrative for the attacker; it's high yield and low risk, and I don't expect it to be going away soon."

Advance measures to keep ransomware at bay

Ransomware-specific threat modeling and assessment is key to reducing the potential impact of attacks. Hylender emphasizes the need for specific planning: "Having a plan in place to respond to ransomware incidents if they do happen is an absolute must-have as opposed to a nice-to-have. We need to have a plan to get back up and running quickly [as well as] what we can do more slowly or at a more measured pace."

Backup and restore is

"Having a plan in place to respond to ransomware incidents if they do happen is an absolute must-have as opposed to a nice-to-have."

—Dave Hylender, senior risk analyst, Verizon



Master's Degree in Informatics | Cybersecurity and Privacy Specialization

Advance your career in cybersecurity with an MS in Informatics degree. The accelerated program starts with a foundation focused on human/computer interaction and builds upon those skills with specialized courses covering information security, digital forensics, and advanced technology tools.

All courses are delivered exclusively online, affording the convenience and flexibility to learn wherever and whenever works best for you.

- ✓ 100% Online
- ✓ Scholarships available
- ✓ No GRE or GMAT required

Learn more and apply online at
<https://ischool.sjsu.edu/ms-informatics>

SJSU SAN JOSÉ STATE UNIVERSITY

a critical part of data protection. Frequent copies of critical data—stored offsite and isolated from production systems—are key to blunt the potential effects of a ransomware attack.

Steering clear of ransom demands

Like any cyber threat, prevention and response measures against ransomware are first and foremost about protecting against business interruption and data loss. At the same time, avoiding being forced to pay a ransom is an important goal in its own right, because payment effectively has a higher cost than just the amount turned over to the criminals.

As Hylender puts it, “I can understand the panic mentality that causes people to just want to pay the ransom,

“I can understand the panic mentality that causes people to just want to pay the ransom, but that is exactly why these attacks persist.”

—Dave Hylender, senior risk analyst, Verizon

but that is exactly why these attacks persist. If people would stop paying these ransoms, we might have a better chance of stopping these attacks from being so prevalent.”

In the final analysis, diligent preparation is the only viable protection against

ransomware. Prevention and response tailored specifically to this class of threats is critical for every organization, and business continuation in the face of attempted or even successful ransomware attacks is not only possible, but mandatory in our time. ■

MATT GILLESPIE is a technology writer based in Chicago. A longer version of this article appears in the August edition of Insights.

securityMETRICS®



Close the Gaps in Your Security and Compliance

A thorough PCI audit consists of many individual components. Our consulting services, gap analysis, and penetration tests work together to provide a comprehensive solution to PCI audit requirements.

Let's talk about your
PCI Audit and Pen Test Needs
801.705.5656
www.securitymetrics.com

Latest Verizon IR Report Shows Shortcomings In Attack Preparedness

A FALL 2019 REPORT from Verizon Enterprise Solutions shows companies still have a ways to go in both preparing and responding to cyber incidents.

Among a survey's key findings:

- Nearly half (48%) of organizations do not have an efficient IR plan in place.
- Almost 6 out of 10 reviewed plans failed to include legal/regulatory requirements for breach notification.
- Some 43% of reviewed plans do not fully designate internal IR stakeholders.
- And 71% of reviewed plans do not describe end user security awareness training.



“Preparing for and responding to data breaches and cybersecurity incidents is never easy,” the report reads. “It takes knowledge of your environment and its unique threats, effective teamwork and, just as importantly, an Incident Response (IR) Plan.”

The *Verizon Incident Preparedness and Response Report* includes best practices in five key areas of IR.

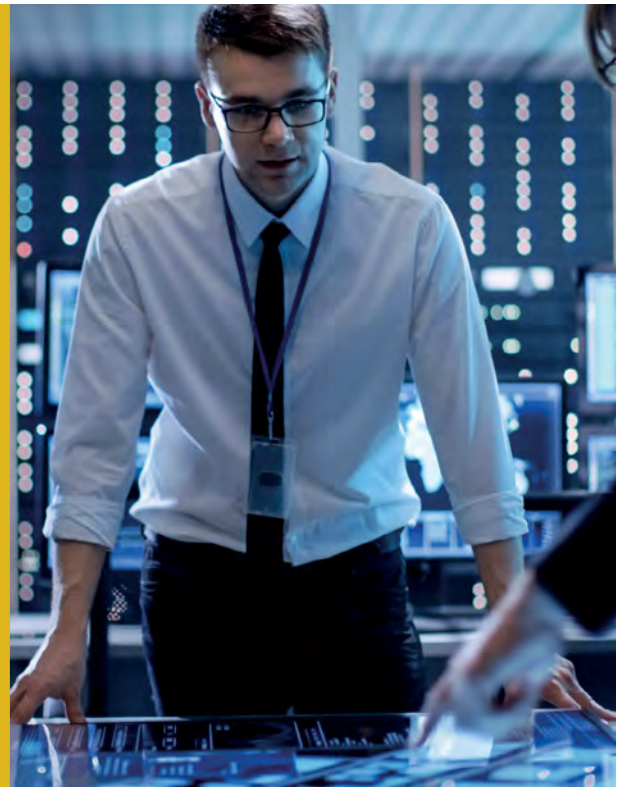
You can read the full report at <https://enterprise.verizon.com/resources/reports/vipr/2019-vipr-full-report.pdf> or view the Executive Summary at <https://enterprise.verizon.com/resources/reports/vipr/vipr-exec-summary.pdf>. ■

THE SECURITY OF MILLIONS IS AT RISK. IS YOUR ORGANIZATION PREPARED?

Cybersecurity-related talent gaps continue to expand. Tackling a shortage of expertise can be challenging on your own. Purdue University Global offers the tailored education solutions you need to help build, grow, and retain your workforce.

Our personal approach to helping you meet core business objectives goes far beyond training your workforce. As your strategic partner, we'll work closely with you to develop a customized plan, whether it's in cybersecurity, IT, or business, and keep your organization prepared for whatever comes next.

Purdue Global—a world-class university that delivers world-class education solutions.



Learn more at Cyber.PurdueGlobal.edu.

PURDUE GLOBAL
UNIVERSITY.

'Trust Audit' Shows Mixed Results

THE ONLINE TRUST ALLIANCE, an initiative of the nonprofit global Internet Society, recently issued its 10th annual "trust audit" to gauge the readiness of organizations, most in the United States, for meeting privacy regulations such as the EU's General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and, beginning January 1, the California Consumer Privacy Act (CCPA).



The basic criteria of the audit:

- Users must be able to request information on why their personal information is being collected.
- Users must be informed if their personal information will be sold or shared with a third party.
- Users must have access to their data and be able to download it and it must be "portable," (i.e., in an easily readable format).
- Users must be able to request their data be deleted.
- Organizations must notify users of their rights in an easily understandable matter.

A review of the current privacy statements of 1,200 organizations evaluated showed mixed results.

Data Sharing:

- 98% alerted users about the status of data sharing, but none had language stating that users must be notified when their data is sold or shared.
- 57% said they held the third parties they worked with to the same data-sharing standards they hold.
- Less than 1% alerted users to the type of data shared with third parties.

User Access:

- 90% provided a link to their privacy statement on their homepage.
- 32% had what OTA characterized as "readable" statements.
- 70% provided an organization contact.

Social Media:

- 52% informed users that the site used third-party social media services.

For the full report on the audit and more information about the Online Trust Audit, go to https://www.internetsociety.org/wp-content/uploads/2019/09/ISOC-Are_Organizations_Ready_for_New_Privacy_Regulations_20190917.pdf. ■



(ISC)² Announces the 2019 ISLA Americas Ceremony Awardees

ISLA Americas:

- **Up-and-Coming Information Security Professional:**
Tomiko K. Evans
- **Community Awareness:**
Andrés Velázquez, CISSP
- **Information Security Practitioner:** Anna Harrison, CISSP
- **Senior Information Security Professional:**
Cassio Goldschmidt, CSSLP, CCSP

ISLA Government:

- **Up-and-Coming Information Security Professional:**
Stephen Czerwinski
- **Workforce Improvement:**
Lisa Carol Holman
- **Technology Improvement:**
William Birchett, CISSP
- **Most Valuable Industry Partner (MVIP) [Team]:**
Dr. Thomas P. Scanlon, CISSP
Additional team:
Dr. William Nichols, Dr. Carol Woody, Dr. Kenneth Nidiffer, Timothy Chick, CSSLP
- **Community Awareness [Team]:**
Julie Chua, CISSP, CAP
Additional team: Erik Decker, CSA 405(d) Task Group Members, CSA 405(d) Steering Committee, Christopher Bollerer, Steve Curren, Nickol Todd, Laura Wolf, Emery Csulak, Nick Heesters, Suzanne Schwartz, Aftin Ross, Seth Carmody, Rose-Marie Nsahlai, Matt Quinn, Matthew Barrett, Nick Rodriguez, Justin Smith, Konrad Miles, Paige Burke, Elizabeth Voeller, Brian Lebeck ■

RECOMMENDED READING

Suggested by **Larry Marks**, CISSP, CISA, CISM, CFE, PMP, CRVPM, CRISC, CGEIT, ITIL

Effective Cybersecurity: A Guide to Using Best Practices and Standards

By **William Stallings**

(Addison-Wesley Professional, 2018)

W

ILLIAM STALLINGS, in *Effective Cybersecurity: A Guide to Using Best*

Practices and Standards, defines his topic as “a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that are used to protect the cyberspace environment and organization and user’s assets.”

Stallings has written a comprehensive guide on implementing cybersecurity using best practices suggested by organizations like NIST and ISO. The coverage is thorough and detailed, written to help the average reader grasp the concepts. Each chapter ends with a small test of material covered. The reader then scores responses against answers available online.

While the book can be used as a reference in graduate school, Stallings’ material is applicable to the broad fields of information security and cybersecurity.

There are a few shortcomings in Stallings’ work. It is light on the current GDPR initiatives and NIST guides relevant to risk management. However, a reader will find a wealth of information that can be appreciated by a student or newly minted professional joining the cybersecurity field. *Effective Cybersecurity* provides the building blocks and the “blocking and tackling” practices that one needs to set up or improve a cybersecurity program. Bravo, William Stallings! ■



WHO DO YOU TRUST?



75%
of consumers surveyed said healthcare providers were most trustworthy with personal data

Source: AT Kearney, *Privacy and Personalization: The Paradox of Data in Consumer Marketing*

WHERE’S THE DATA?

93%

of firms surveyed store data in more than one environment

Source: Symantec, *Adapting to the New Reality of Cloud Threats*

<https://www.symantec.com/content/dam/symantec/docs/reports/cstr-adapting-to-new-reality-en.pdf>

READ. QUIZ. EARN.

Earn Two CPEs for Reading This Issue

Please note that (ISC)² submits CPEs for (ISC)²’s *InfoSecurity Professional* magazine on your behalf within five business days. This will automatically assign you two Group A CPEs.

Note: To access this members-only platform and quiz, you’ll need a Blue Sky account. If you don’t have an account, go to the Blue Sky homepage via the link and click on “Create User Profile” in the upper right-hand corner.

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&PCAT=7777&CAT=10831&Review=true

The author of Recommended Reading did not receive financial compensation from the book publisher, nor a free copy of this book. All opinions are his alone.

Image: iStock

■ ■ ■ (ISC)² CHAPTER SPOTLIGHT

Making Cybersecurity a Community Priority is (ISC)² Peru Chapter's Goal



Javier Romero, president, (ISC)² Peru Chapter, leading a monthly meeting.

“Elevar el nivel de conciencia de todos los líderes la sociedad peruana respecto a las ciber amenazas y despliegue tecnológico emergente.”

“To raise the level of awareness of all leaders in Peruvian society regarding cyber threats and emerging technological deployment.”

That is the vision of (ISC)² Peru Chapter. In order to realize that vision, the chapter aims to become the touchstone for its community's cybersecurity leaders. “We want the CISOs to see the chapter as the point of excellence to find knowledge, experiences, advice, and to analyze cases related to information security. Then, with this knowledge, we can advise our respective managers or consulting clients,” says chapter vice president Luis Mendoza.

(ISC)² Peru Chapter received its charter in October 2017 and has 20 members representing financial, consulting and infrastructure organizations. Monthly meetings focus on case studies from the data breach investigations conducted by Verizon, using them to discuss similar situations in their organizations and sharing solutions.

Cloud security is quickly becoming a key issue facing the cybersecurity community in Peru. “Our knowledge of the use of cloud services and the information security concerns is very poor,” Mendoza explains. “As a consequence, we need not only technical resources, but we need to know the regulation, laws and more detailed risks about this service and the consequences of its use.”

Through its work and cybersecurity advocacy, the objective of the chapter members is to provide leadership in security strategy throughout Peru. ■

(ISC)² PERU CHAPTER

Contact: Luis Mendoza, vice president, (ISC)² Peru Chapter

Email: board@isc2peruchapter.org

Q&A

Javier Romero

President, (ISC)² Peru Chapter

What do you see as the most important issues facing Peru's cybersecurity professionals?

I believe that professionals working for critical infrastructure, government and defense units must build realistic bridges with private and national intelligence organizations (both inside and outside their teams). In addition, professionals must be able to help the organizations realize their goals.



Foreign competitors who want to enter into the local cybersecurity services market have found a pool of local cybersecurity consultants (i.e., freelancers) with a very good curriculum who may not be selling their services at the best price.

We also must improve our professional status in the global arena. Foreign competitors who want to enter into the local cybersecurity services market have found a pool of local cybersecurity consultants (i.e., freelancers) with a very good curriculum who may not be selling their services at the best price. By undervaluing their skills, these talented cybersecurity professionals may be doing a disservice to the Peruvian technology market.

What has been the response from the business community to your chapter's efforts in raising awareness to cybersecurity needs?

The best! Our inaugural meeting was held in my business office. Our presentation so impressed one of the managers in the room that he offered the headquarters in one of Peru's largest banks to hold our monthly chapter meetings.

Since then (December 2017), our meetings have provided us a wonderful view of Lima and plenty of space for parking cars. While our members are committed to our mission, it is time for us to venture into the business schools to raise the awareness of the aspiring managers.

Where do you see the biggest need in your community for cybersecurity education: schools, business, government?

Need is the keyword here. Though government cannot provide total cybersecurity, its posture on cybersecurity has improved a lot in the last 20 years. But, in my opinion, government will never be able to protect the trade secrets, technology research and operations of key businesses. It doesn't matter how much money government spends on cybersecurity; businesses need to protect/defend/react/detect themselves. So, businesses: Heads up! You must invest in cybersecurity education.

What plans does the chapter have for 2020 to raise awareness and grow membership?

We will soon become an official nonprofit association registered in Peru. This will enable us to invoice members and participants in our case-of-use meetings and legally establish "agreements" with business schools and other organizations. From there, we will be able to increase our budget, which we can then use in marketing the organization to recruit new members.

What are some of the topics you are considering for your meetings?

As always, we expect to review both old and new cases of cyber breaches including the Amazon/Ethereum attack, the increasing attacks against Latin American banks, the attacks against SWIFT [the international banking network], as well as new malware tools, like VPNFilter. ■

TRAINING CAMP

WAKE UP AND JOIN THE 40,000+ CISSPs THAT CHOSE TRAINING CAMP TO GET CERTIFIED

WWW.TRAININGCAMP.COM

2017 & 2018 (ISC)² PARTNER OF THE YEAR

Remembering Where We Come From

by Tony Vizza

RECENTLY, I was presenting the findings of the (ISC)² Cybersecurity Workforce Study to a large group of cybersecurity professionals in Sydney, Australia. The results of the study are always a somber reminder of the significant skills gap that exists today and in the foreseeable future.

As I was presenting, I arrived at a set of statistics relating to what employers are looking for in new hires. In Australia, for example, 43% of employers want people with relevant cybersecurity work experience. It's a statistic that as an association, we proudly illustrate to show just how important our experience-based certifications truly are for professionals. Most other economies are within a few percentage points of this number.

As I started to illustrate and talk through this particular statistic, a heckler in the audience voiced a very clear sense of displeasure and exasperation. He openly challenged not the validity of the statistic itself, but rather, the notion that a cybersecurity student with no relevant work history could ever get hired if employers are predominantly looking for experienced candidates.

My response to him, verbatim, was: I entirely agree.

After the presentation, the heckler came up and apologized. Truth be told, I said to him that he had no reason to apologize. I explained that I too had once been a computer science student unable to find my first IT job. I remember applying for hundreds of jobs—jobs I knew I would be the best person for

(and in my desperation at the time, jobs that I was lucky *not* to land). Graduating from the top university in computer science mattered none. The handful of HR personnel who had the courtesy to contact me would simply advise that I “did not have enough experience.”

I understood where my heckler friend was coming from.

The point was hammered home a few days later when I was at an event launching the cybersecurity innovation node for the state of New South Wales. As I was speaking with a senior government official about the



cyber skills gap, she mentioned that she was aware of at least 10 recent vocational education graduates in cybersecurity who were unable to find employment, and she questioned whether the gap even existed.

As an industry, are we expecting too much from young women and men who want to join the field but often aren't considered due to their lack of experience?

As an industry, are we expecting too much from young women and men who want to join the field but often aren't considered due to their lack of experience? Are these young and impressionable people giving up on a cyber career because they can't find an employer willing to give them the opportunity, therefore leaving them to accept a run-of-the-mill IT job instead of one that aligns with their passion?

As an association of certified cybersecurity professionals, could we be doing more to champion the hiring of budding professionals in our workplaces? Could our organizations do more to support future certified professionals? Does your government offer programs to incentivize your business to recruit and train young men and women? Could you offer internships? Could you mentor students?

Sometimes we need to remember where we came from and the painful experiences we endured, and use that insight to see if we can do a better job for the next generation. ■



Tony Vizza is the Director of Cybersecurity Advocacy for (ISC)²'s Asia-Pacific region and is based in Sydney. He can be reached at tvizza@isc2.org.

Start tracking the vulnerabilities keeping you up at night

This exclusive, members-only resource aggregates, categorizes and prioritizes vulnerabilities affecting tens of thousands of products.

Create a customized feed filtered by the vendors, technologies and keywords that are relevant to your interests.

Visit: vulnerability.isc2.org

Free to (ISC)² members through the member portal, no new account required.



Achieve SecurityCertaintySM

Chain-of-Custody Security SolutionsSM



Global Consulting & Assessments
Incident Response & Remediation
Secure Technology Logistics
Managed Security Solutions
Secure Technology Asset Disposition

MCPc.com/Certainty



THE DATA PROTECTION COMPANY

THREAT

Is your security operation ready to launch such a program?

HUNTING

BY MATT GILLESPIE



IT COULD BE a blended attack as slick as a multichannel marketing campaign. Or a spontaneous crime of opportunity by a single disgruntled employee. It could even be an innocent configuration error.

When a threat exists, there will be indicators. The perennial challenge is to hunt for signs in the right places and to isolate the signal from the noise.

How best to find—and remove, where possible—such threats remains up for debate.

ILLUSTRATIONS BY TAYLOR CALLERY

Lance Cottrell, chief scientist at Ntrepid, approaches threat hunting less as a specific set of techniques than as a set of high-level goals. “From the 50,000-foot view, we’re trying to understand the threat landscape,” he says. “Write large, you are trying to figure out what the things are that are coming after you.”

The breadth of that mandate can make it difficult to define a threat hunting practice, or even to draw bright lines around where it borders with other security measures. For example, a specific threat identified through threat hunting may be investigated using existing general processes for incident analysis.

SEASONING THE ATTACK SURFACE



Threat hunting relies on both active and passive measures. Honeypot machines that no other system will ever legitimately connect to can be set up inside the firewall. This inward-looking measure can provide 100% confidence that every connection attempt is nefarious.

Another pre-positioning measure is salting production databases with false data to mark provenance. Hard to discern as illegitimate by outsiders, finding watermarked data in the wild can tell administrators that a specific data store in their environment has been breached.

Using such deception to detect wrongdoing has a much longer history than IT does. This salting practice harkens to fake “trap streets” inserted into maps so their creators could detect plagiarism of their work.

—Matt Gillespie

Likewise, threat hunting inputs run the gamut—from eavesdropped conversations among criminal gangs to analyses of server logs and user behavior. Some threats are malicious, while others are not. An organization’s concept of threat hunting should encompass this whole scope, even if its coverage is limited.

SETTING UP A THREAT HUNTING PRACTICE STARTS FROM THE TOP

Launching a formal program can be daunting. Even finding the right people to staff the practice is difficult, because of the breadth of skills involved.

“I think it requires quite a team effort, and I don’t think you’re going to find a unicorn that can handle the full gamut of what needs to be done in a threat hunting program,” says Tom Gorup, vice president of security and support operations at Alert Logic.

Before you even think about hiring a threat hunter, you need to get your culture in check. Once you do that, it opens a lot of doors, and then it’s about investment in time and tools.”



—Tom Gorup, vice president of security and support operations, Alert Logic

From server and network administrators to data scientists, aligning the organization toward threat hunting needs to come from upper management, enabled from top down.

“Before you even think about hiring a threat hunter, you need to get your culture in check. Once you do that, it opens a lot of doors, and then it’s about investment in time and tools,” Gorup suggests.

“If I were a CISO and the long-term strategy was to get threat hunting in place,” he continues, “I would want to be sure that all our basics were in place first. We’re able to centralize data, we have a good incident analysis process, we’re able to access information quickly and easily.”

As an open-ended, data-driven activity, threat hunting depends on access to information and collection methods that are designed with machine readability in mind, with characteristics such as key-value pairs and good parsing. Data silos must be broken down so that threat hunters

can draw on the information they need.

Data access also speaks to the cultural component of the process. For instance, a developing investigation might need access to specific log reports. The wealth of information they contain—from failed logins and lockouts to unusual data movement—can make them invaluable. Having the CEO and CISO sign off on the threat-hunting initiative can be the difference between threat hunters meeting with resistance versus cooperation when trying to get internal information.

In a world of limited resources, executive buy-in is critical to make threat hunting efficient enough to be sustainable. To extend that efficiency, it is also critical to operationalize the spoils of threat hunting so that teams can free themselves up to focus on novel issues.

Aamir Lakhani, a security strategist and researcher at Fortinet, identifies that requirement as a best practice. “The job of the threat hunter is really to get as many things off their plates as they can and make it as automated and

scripted as possible,” he says. In a job that requires looking at many places simultaneously, that efficiency is essential.

TARGETING INTERNAL THREATS, WHETHER MALICIOUS OR NOT

Alongside other security and IT practices, inward-facing threat hunting reveals truths that would otherwise remain hidden. A primary tool in this area is to use human intelligence gathered from human resources departments and direct observation to define typical behavior for specific user groups and to identify when users step outside those norms.

“We’re combining human psychology to define behavior and how that corresponds and interacts with IT,” Lakhani explains. “We had one customer’s employee where a few issues caught our eye. We saw that he wasn’t cashing paychecks, he was active on some really curious forum boards, and those things caught our attention in areas that we

A green-themed graphic for the ISC2 Community. It features a central dark green banner with the text "Join the new (ISC)2 Community!". Below the banner, there is a network of light green circles connected by lines, with several circles containing stylized human icons of diverse people. The background is a lighter shade of green with a subtle pattern of circles and lines.

Join the new
(ISC)²
Community!

With 15,000+ members, join the new (ISC)² Community where (ISC)² members, cyber experts and IT security professionals collaborate, share knowledge and best practices required to manage cyberthreats and risks in business today.

CONNECT. COLLABORATE. SHARE. DEVELOP.

community.isc2.org

They need to make friends with the right people, demonstrate the right competencies and knowledge and speak the right language, with the right kind of slang and the right behaviors. And technologically they need to look right; they can't be using their office-issued Windows desktop."



—Lance Cottrell, chief scientist, Ntrepid

wouldn't notice just doing pen testing or scans."

It turned out that the employee had signed an offer with a competitor and was trying to steal information. The indicators didn't paint a straight line to the threat, but they showed up as an aberration from expected behavior, which eventually led investigators to the truth.

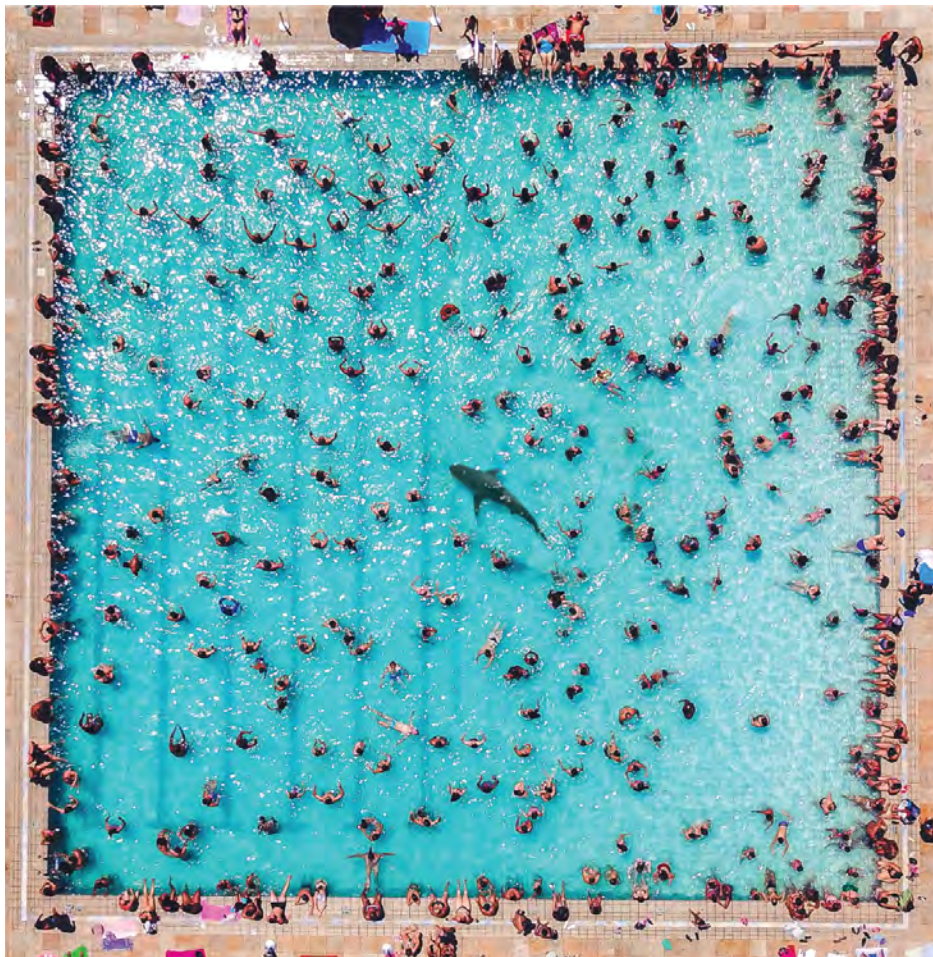
In addition, loyal employees can innocently create internal threats. For example, employees participating on discussion boards may inadvertently give out more information than they intend to. This is especially true if others on the board can determine where they work.

Lakhani explains, "They may be a leader in that community, and they're trying to do good answering questions on an Oracle system or an Apache system, but people can start putting together a profile on a given company." Helping potential attackers map out internal IT systems may be the last thing on such users' minds, but it shouldn't be.

By providing input into user-awareness training, a threat-hunting team could remediate the threat, closing the information loop by communicating back to the end users.

OBSERVING THREATS IN THEIR NATIVE HABITATS

Hunting outside the company for cyber threats is bound-



Cloud development is fun.
Cloud threats are not.
Rise above the noise of cloud-scale business with Reveal(x) Cloud, cloud-native network detection and response that helps you see and stop threats fast.

LEARN MORE:
www.extrahop.com/products/cloud/

 **ExtraHop**
Rise Above the Noise.

AI definitely has a broader place in the future, but it's far from being a magic bullet ... sometimes it seems like marketing teams have watched too many Terminator movies."



—Aamir Lakhani, security strategist and researcher, Fortinet

less in scope. Understanding the likely sources of threats and developing ways to monitor them can be an elaborate challenge in itself. For example, a defense contractor might study the priorities of foreign national research institutions in unfriendly countries. That information could suggest potential areas of interest where the country might level cyberattacks.

A threat hunter may also elect to participate directly in the forums and marketplaces frequented by threat actors of interest. That requires building a trusted false identity,

which is a complicated thing to do.

"They need to make friends with the right people, demonstrate the right competencies and knowledge and speak the right language, with the right kind of slang and the right behaviors," Cottrell says. "And technologically they need to look right; they can't be using their office-issued Windows desktop."

Once accepted into that community, threat hunters have access to conversations ranging from emerging new malware to specific targets and data being sought. In addition, looking at what's offered at a marketplace can reveal indicators of compromise, such as a customer list, credit card numbers or passwords that indicate a breach.

Most insights that turn up in external threat hunting are unclear, perhaps even valueless to a specific entity. Cottrell notes, "The advantage of an inward-looking approach is that all of the information you find is going to be relevant to your organization. ... If you are trying to hang out in hacker forums to look for threats, the vast majority of what

AGENTLESS DEVICE SECURITY

ARMIS

See every device, managed and unmanaged. Visit Armis at booth #111 to learn about better visibility and control.

www.armis.com

you're going to learn is probably not important to you.”

ANALYZING THE THREAT LANDSCAPE

Sometimes threats are unambiguous, such as a confirmed case of your purloined data on offer in a cyber souk or discussion of an upcoming DDoS attack. More often, they are detected in subtle patterns of events or behaviors, as with the example of the malicious employee digging up dirt for a competitor.

That example also reveals how broad the scope of information needed can be and how vague the indicators. Gorup remarks, “You’re dealing with a lot of ambiguity ... because you’re often dealing with an alert from your SIEM [security information and event management software] that doesn’t have a full picture for one reason or another.”

He cites the case of a large company that missed a pattern of such alerts. “They received [large numbers of alerts] from their endpoint solution that they marked as

ambiguous, and if they were looking at their data more in the aggregate, they would [have seen] an increase in these unknown-type alerts.”

That search for patterns brings data analytics and data analysis to the fore, and visualization tools play a valuable role. Visualization can also be used to create playbooks that describe patterns of notifications for specific incident types, presenting that data in a way that’s easy to consume.

In the analysis of future ambiguous events, those playbook records can be compared against emerging sets of notifications to help diagnose threats. “Data science plays a big part in that, because we want to be able to understand what’s abnormal when we’ve applied it against these particular use cases,” Gorup explains.

THE POTENTIAL FOR AI TO DEVELOP INSIGHTS

The emerging role of artificial intelligence (AI) stretches

AUTOMATE YOUR DATA MAPPING

Map business process and data usage to improve security and achieve compliance*

- Automate business process security analytics
- Eliminate costly data discovery
- Stay compliant with emerging data privacy laws


WWW.IORATLAS.COM

*Supports GDPR Article 30, PCI 1.1.3, HIPAA Security Rule 45: 164.308/310, CCPA and others

the boundaries of what's possible with modeling and statistical methods. Detecting patterns and anomalies in the context of threat hunting is broadly similar to the use of AI by mainstream antivirus solutions. Indeed, malware detection based on files' behaviors has become more capable in recent years, as detection models have become more sophisticated.

On the other hand, Lakhani suggests a judicious perspective on the outer limits of present technology. "If you're tracking expenses and expense behavior, the right machine learning models can definitely say, 'Hey, this type of expense is very odd for this user.'"

He is cautious about generalizing that success too far, though. The broad use of AI to detect patterns in alerts and behaviors, while promising, is in its infancy. "AI definitely has a broader place in the future, but it's far from being a magic bullet ... sometimes it seems like marketing teams have watched too many Terminator movies."

On the current state of analyzing live threats using AI, Cottrell says: "You may be surprised how much of it is manual. Say you've infiltrated a criminal cyber souk; there aren't tens of thousands of big data dumps per day going into these things. So, you may be wanting to follow up every time someone says they have a new big chunk of data."

That's a role for manual involvement and relationship building. The prospect of removing humans from their primary role in the threat-hunting kill chain is still a long way off. Security decision makers are well advised to enable them with the authority, tools and data to help make them successful. ■

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



Galvanize

IT security, risk management,
compliance, and audit software.

One powerful platform to drive productivity and insight into your
IT risk and compliance posture.

Visit wegalvanize.com to learn more.

A NEW PRESCRIPTION FOR SECURITY AND IT'S FREE.

Introducing Qualys
Global IT Asset
Inventory[®]

CREATE YOUR ACCOUNT AT
[QUALYS.COM/INVENTORY](https://qualys.com/inventory)





How MITRE's methodology to find threats and embed counter-measures might work in your organization

BY NARESH KURADA, CISSP

THREAT MODELING is gaining even more attention with today's dynamic threat environment. The sophistication of threat actors and development of advanced tactics, techniques and procedures (TTPs) has put a brighter spotlight on the process of finding vulnerabilities by incorporating the attacker's point of view.

There are several threat modeling approaches and techniques to consider. Often, these can be classified as *asset-centric*, *system-centric*, *people-centric* or *risk-centric*. For instance, Microsoft's STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege) is system-centric, while PASTA (Process for Attack Simulation and Threat Analysis) is risk-centric.

ILLUSTRATION BY ENRICO VARRASSO

Regardless of the model, the primary objectives remain the same—identify threats and embed countermeasures at the outset and, preferably, during design. However, threat modeling for each of these approaches may not be comprehensive enough and could also be difficult to apply. More importantly, there are no formal frameworks to holistically identify threats from adversarial tactics. And there is often an overreliance on the experience and expertise of security practitioners, software developers and systems engineers.

This was true until MITRE developed the Adversarial Tactics, Techniques and Common Knowledge framework, better known as ATT&CK. The even better news is that MITRE ATT&CK can also be used to holistically identify threats emanating from adversarial tactics or techniques to the widely used STRIDE approach. The system-centric STRIDE approach for threat modeling is usually leveraged during secure software and system development, or as an extension to DevSecOps.

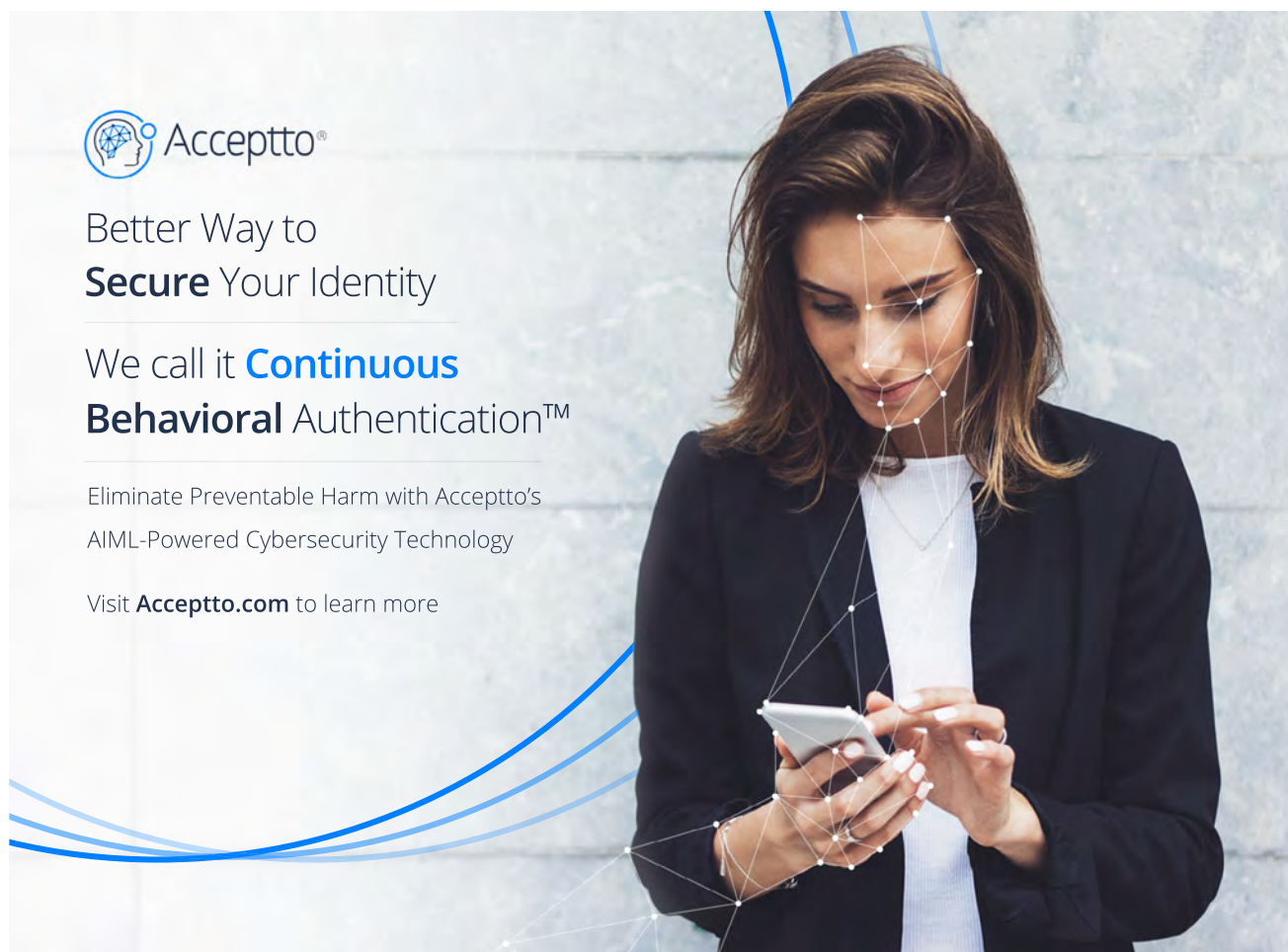
Here's what you need to know before diving in.


THREAT MODELING FUNDAMENTALS

The underlying premise of threat modeling, as an extension of reliability engineering, is that a system will always have an undefined vulnerability that could potentially be exploited through a sequence of steps or in a certain scenario. Simply put: A system will always have an undefined flaw waiting to be exploited.

Simply put: A system will always have an undefined flaw waiting to be exploited.

Consequently, threat modeling is a systematic process to elicit potential threats and anticipate the exploitability of vulnerabilities. Some of the earliest works on threat



 Acceptto®

Better Way to
Secure Your Identity

We call it **Continuous**
Behavioral Authentication™

Eliminate Preventable Harm with Acceptto's
AIML-Powered Cybersecurity Technology

Visit **Acceptto.com** to learn more

FIGURE 1: SAMPLE OF MITRE ATT&CK MATRIX FOR ENTERPRISES*

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInIt DLLs	Bypass User Account Control	Credential Dumping
Replication Through Removable Media	Control Panel Items	AppInIt DLLs	Application Shimming	Clear Command History	Credentials in Files
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry
Spearphishing Link	Execution Through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access
Spearphishing via Service	Execution Through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Hijacking	DCShadow	Keychain

modeling include the use of attack trees (https://www.researchgate.net/publication/234738557_Threat_Modeling_Using_Attack_Trees) (as an extension of fault tree analysis) and numerous other academic pursuits as derivatives of mathematical stochastic processes.

Most threat modeling approaches have four components:

- Actor or adversary
- System or subject
- Vulnerability
- Attack technique or method

Of the four, the attack techniques are largely similar and offer opportunities for attack pattern recognition. Ironically, the taxonomy related to attack techniques has not been formalized and linked back to the actor in the context of a system.

Also, in the context of inputs to threat modeling, the processes to maintain and report on vulnerabilities has

matured over the years, and numerous publicly available vulnerability databases have evolved. For instance, the NIST National Vulnerability Database (NVD) offers a good source of known vulnerabilities across various technologies.

Also, security researchers have made deliberate attempts to capture and map out tactics as patterns used by adversaries. Lockheed Martin's Cyber Kill Chain is one such approach and describes the adversarial tactics as a seven-step process. These steps are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. While both the NVD and the Cyber Kill Chain offer valuable input, neither is holistic enough for effective threat modeling. The Cyber Kill Chain is a high-level adversarial framework of tactics, while vulnerability databases are too low-level.

This is where the MITRE ATT&CK framework fits— to fill the gap and provide a succinct set of tactics with an appropriate depth and taxonomy of techniques.

*The complete MITRE ATT&CK matrix can be found online at <https://mitre-attack.github.io/attack-navigator/enterprise/>.

DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	EXFILTRATION	IMPACT
Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation

In spirit, ATT&CK is similar to the Cyber Kill Chain, yet more defined with depth and actively updated (similar to how NVD is actively updated).

A DEEPER DIVE INTO MITRE ATT&CK

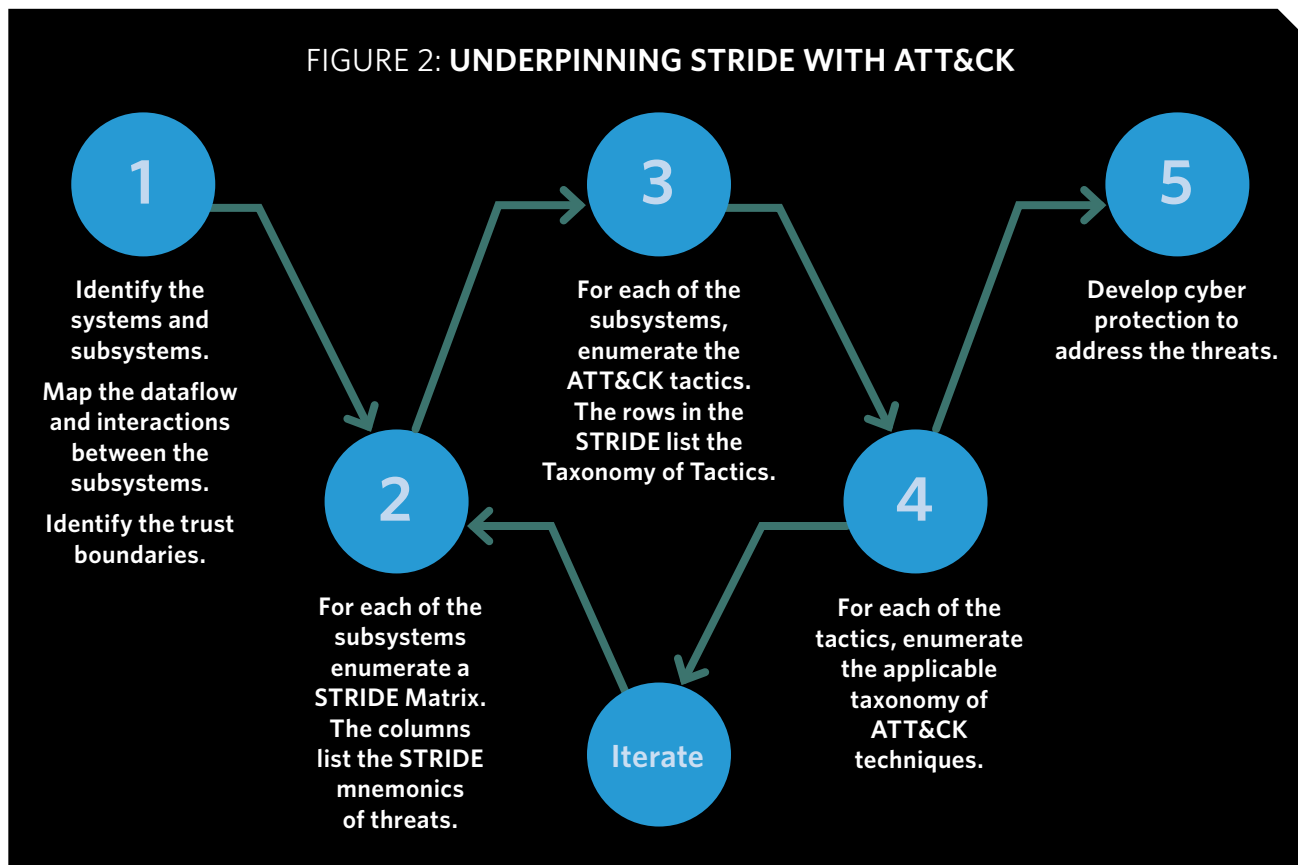
The MITRE organization recognized the disparity in articulating the adversarial view of an attack lifecycle and created ATT&CK (<https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philoso->

phy.pdf). An attacker's target platforms and the techniques and tactics detailed in ATT&CK is a community-driven knowledge base maintained and updated by MITRE.

In spirit, ATT&CK is similar to the Cyber Kill Chain, yet more defined with depth and actively updated (similar to how NVD is actively updated). At a high level, ATT&CK is organized as a matrix of adversarial patterns, capturing the progressive tactics (and intent) of cyber adversary behavior along with the corresponding techniques.

A sample of the MITRE ATT&CK matrix is illustrated in Figure 1, above. What differentiates ATT&CK from the Cyber Kill Chain is the depth of the techniques and the curated taxonomy of those techniques. Also, the organization of the matrix presents use cases for cyber defense and protection. Some of the use cases for cyber defense are gap assessments in security operations based on specific exposure to threats and elicit opportunities for improving the protection.

FIGURE 2: UNDERPINNING STRIDE WITH ATT&CK



ATT&CK also presents as a plug-in or a second layer to other frameworks that lack the adversarial tactics and techniques. More specifically, it can be used as a second layer for STRIDE, which is often used to drive threat modeling in secure software development.

A DEEPER DIVE INTO MICROSOFT STRIDE THREAT MODELING

STRIDE is a popular system-centric threat modeling technique used to elicit threats in systems and the software development lifecycle (SDL) along the dimensions or mnemonics of spoofing, tampering, repudiation, information disclosure, denial-of-service and elevation of privilege.

The primary steps needed to apply STRIDE require:

- Identifying processes, data stores and dataflows.
- Establishing trust boundaries between systems and subsystems (such as data flow diagrams).

Subsequently, each of the systems or subsystems are systematically analyzed against each of the components of STRIDE, as well as the desired outcome to protect

authenticity, integrity, non-repudiation, confidentiality, availability and authorization.

STRIDE is a robust process for high-level threat modeling. It also offers the right amount of “shift left” (development of security countermeasures at the outset) required of security in SDL and as an extension to DevOps during design and Agile development—as opposed to a later stage (such as a software release).

What STRIDE doesn’t do, however, is account for how adversaries intend to exploit a system. What is their plan of attack? For instance, STRIDE doesn’t factor in the intent of the tactics, from “initial access” to “lateral movement,” or to maintain “persistence” within a system or subsystem.

Similarly, within each tactic, the taxonomy of techniques used to exploit vulnerabilities is not defined at the level required for modern advanced TTPs. All these factors are required for developing strong cyber protections during SDL. Also, the depth and breadth of threat modeling becomes an even more critical security concern in DevOps because of modern Agile-based development that includes continuous integration and development (CI/CD), as well

as infrastructure and security developed as code.

Let's also not forget the thoroughness of security needed to derive and develop the foundations for a golden image (blueprint of security countermeasures). The golden image must be in lockstep with the high-security risks of shorter release cycles (days or hours as opposed to months) in continuous integration/continuous delivery processes with automated security testing during development.

UNDERPINNING STRIDE WITH ATT&CK

Given all we've covered, the application of ATT&CK in the STRIDE process is a natural fit. This combined process for threat modeling is illustrated in Figure 2, p. 32.

Like STRIDE, the first step is to identify the systems, subsystems and more, then map out the dataflows and interactions between them and the trust boundaries.

Second, for each of the subsystems, enumerate a STRIDE matrix listing the mnemonics. Third, the 12

ATT&CK tactics are tallied. Enumerated tactics are:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact


Each of these tactics is progressively sophisticated and, accordingly, the defense (protection) for each of them becomes more complicated.

In Step 4, for each of the tactics within each of the STRIDE mnemonics, the applicable techniques are

eSENTIRE

Complete visibility. Rapid response.

eSentire Managed Detection and Response™ (MDR) protects against cyberattacks that traditional security technologies can miss.

-  We detect, analyze, interpret, classify, isolate and report on suspicious and malicious activity on your endpoints and network.
-  Our high-touch, turn-key service is designed to ensure your organization assumes the minimal amount of risk possible.
-  We reduce the time to response and recover so your organization can return to a known state of good without disruption to your business.

www.eSentire.com
© 2019 eSentire, Inc. All rights reserved.

WANT TO LEARN MORE?

Listen to the (ISC)² Think Tank webcast *The Power of 2: How Automated Threat Hunting & the ATT&CK Framework from MITRE Can Work Together*

FEATURING:

Brandon Dunlap, Moderator

Jason Bevis, BlackBerry Cylance - VP Global Threat Hunting & International Services

Alex Holden, Hold Security, LLC - CISO

Douglas "Chip" Wagner, IBM - Security Analytics Leader, North America

Link: <https://www.brighttalk.com/webcast/5385/366122/the-power-of-2-how-automated-threat-hunting-att-ck-can-work-together>

evaluated. For instance, for the STRIDE mnemonic of spoofing, the 12 tactics are evaluated for ATT&CK threat techniques that could result in spoofing against authenticity. In other words, Steps 2 through 4 are a process of elimination. In the fifth and final step, this process is

iterated against all subsystems to enumerate all the threats and ascertain defenses.

BETTER TOGETHER

The ATT&CK matrix offers a rich taxonomy of adversarial tactics with a curated enumeration of adversarial techniques readily available for various use cases. ATT&CK can be used as a tool to systematically evaluate adversarial tactics and techniques that are lacking in the STRIDE threat modeling process widely used during SDL. The result is an overall improvement in the effectiveness and efficacy of threat modeling. ■

NARESH KURADA, CISSP, is director of security consulting at *Avanade* (a joint venture between Accenture and Microsoft). In the past 15 years, he has specialized in cybersecurity risk management on a variety of computing environments in financial services, power and utilities, and telecom industries.



WALLIX
CYBERSECURITY SIMPLIFIED

IS YOUR DIGITAL FUTURE SECURE?

Visit us at **stand 107** to find out how WALLIX's innovative solutions can help you secure your digital future

Live demos all day!

Meet us on the IoT track!

Adapt your cybersecurity and manufacturing approach to the explosive growth of Industrial IoT

October 30th • 11am - 12pm

Northern E4

WWW.WALLIX.COM

The Authority to Operate (ATO) on AWS Program accelerates independent software vendors (ISV) through multiple security and compliance certifications and authorizations, such as FedRAMP, ISO-27k, PCI, DoD SRG, IRAP, GDPR, and many more.

The ATO on AWS Program consists of varying resources that help expedite the authorization process. Program participants are afforded access to both technical Security Automation and Orchestration (SAO) capabilities as well as direct engagement with highly qualified AWS compliance specialists. Whether you are just beginning your cloud journey or are a cloud veteran, the Program will provide you the necessary guidance and expertise to better migrate, manage and secure your customers' most highly regulated workloads on AWS.

WHAT DOES THE ATO ON AWS PROGRAM INCLUDE?

Training in the AWS Security Automation and Orchestration (SAO) methodology, enabling program participants to:

- Constrain, track and publish continuous risk treatments (CRT) and configurations
- Configure and assimilate DevOps routines (e.g. continuous integration (CI) and continuous delivery (CD)) into a "Type Accredited" architecture
- Leverage the "Type Accreditations" to meet and exceed common security frameworks through the use of security as code practices (e.g. Risk Management Framework (RMF), FedRAMP and DoD CC SRG control baselines, PCI-DSS, IRS 1075, etc).

Access to a detailed and customized action plan providing a blueprint to achieve your security and compliance goals, optimizing your cloud workloads and improving your ability to meet your most demanding customers' requirements.

PROGRAM DETAILS AND BENEFITS

Direct engagement

Qualified AWS compliance specialists will provide mentorship and guidance throughout the process, from initial planning to authorization/certification. Introductions to expert consulting partners trained in the SAO framework can also be leveraged to deploy and/or manage and support the system throughout its lifecycle.

Guidance, templates, tools, and partner solutions

Reusable artifacts, tools, and pre-built templates that ISVs use to build and optimize DevOps, SecOps, CI/CD, and CRT using proven techniques from AWS Security Automation and Orchestration (SAO). Additionally, we have partnered with multiple solution providers who provide products and tools that help simplify and accelerate compliance authorization and management.

Training

Learn best practices to meet security and compliance requirements for solutions on AWS while maintaining a secure and compliant environment effectively and efficiently over time.

Qualified Managed Service Providers for Compliant Workloads

We work with proven AWS Managed Service Providers (MSP) to help them build and support environments that meet specific compliance and regulatory standards. These MSPs are good options for ISVs who prefer to minimize and simplify their area of responsibility by offloading hosting and compliance management.

To learn more about the ATO on AWS Program, contact our ATO on AWS Team.

atoonaws@amazon.com

Connect with us

- facebook.com/amazonwebservices
- twitter.com/AWS_Gov
- youtube.com/user/amazonwebservices
- aws.amazon.com/blogs/publicsector
- aws.amazon.com/blogs/apn

Jump Start Your Cloud Journey!

- Accelerate business growth by unlocking additional revenue opportunities.
- Enhance credibility through defined, secure and compliant cloud capabilities.
- Build a robust go-to-market strategy with AWS.
- Differentiate your practice through security certification as a competitive edge in the market.
- Become eligible for advanced resources, programs, tools, and support.

For more information see

aws.amazon.com/partners/ato/

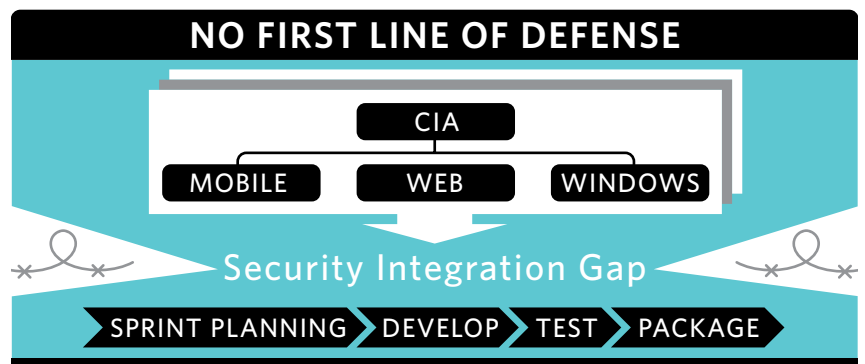
LET'S WORK TOGETHER

An (ISC)² member details a software security integration system that eliminates that '50-page security policy' for developers

BY MICHAEL BERGMAN, CISSP

UNLESS YOUR ORGANIZATION is gifted with resources, your software development teams do not have a dedicated first-line-of-defense function that integrates controls and makes it easier for developers to secure the products they build.

Instead developers, particularly those using Agile for project management, typically are handed a 50-page security policy document and told to "implement that along with your functional requirements, all within your two-week sprint cycle." The result is frustrated developers who usually do not understand cybersecurity well enough to extract security requirements from that massive policy document, let alone write code that correctly meets those requirements.



This lack of control integration, lack of understanding, and inconsistent or incorrect control implementation of security requirements is referred to as the security integration gap.

Symptoms of a security integration gap include:

- 50-page documents sitting idle on developers' desks.
- Slowdown in project management.
- Developers openly frustrated by security requirements.
- Incorrectly implemented security controls.

INFOGRAPHICS BY ROBERT PIZZO

Failing to narrow and eventually eliminate such a gap not only stifles software development, it puts an entire company at greater risk of legal challenges and market failures when products get released late and/or with exploitable vulnerabilities.

Standing on the sidelines, or throwing resources at the issue without a clear plan, is not the proper response to this common business problem. Instead, information security teams need a structured and repeatable way to integrate the security policy and strategic direction of the organization into the software development process and help developers implement it in their code.

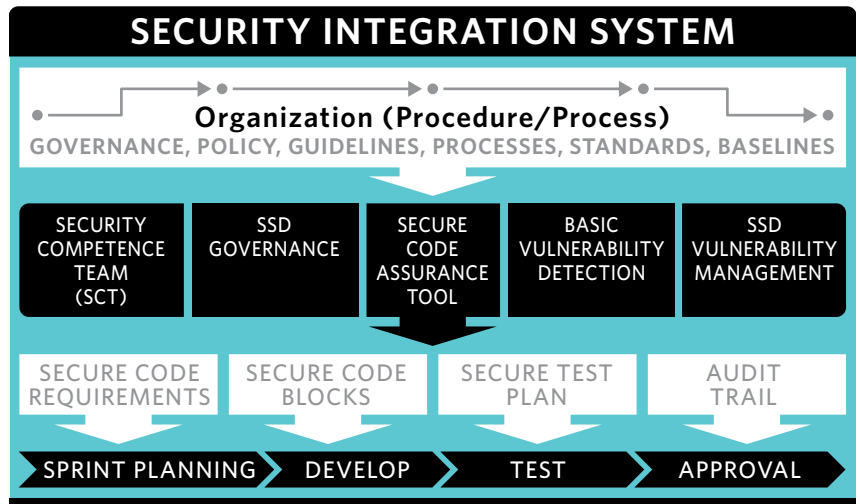
An integrated software security system uses a host of resources including OWASP, COBIT and ISO to build a system of proven, effective and essential tools and technical and administrative controls that secure your software development.

What does the software security integration system do?

It vertically cuts through all three lines of defense. First, by decomposing security policy into a security control system. Second, by making sure controls are integrated. And finally, by providing code-level guidance ensuring controls are correctly implemented.

Three domains within SSD

There are three domains to consider when securing software development (SSD).



- Secure software development process.
- Secure code development.
- Continuous improvement.

To integrate security into these three SSD domains, organizations must determine their IT risk exposure and then wed security policy with the organization's strategic direction in a way that promotes software development without killing its responsiveness to market.

No one-size-fits-all when building such a system

Each organization implements its software development process differently, using different development languages, technologies and methodologies. Information security teams cannot build a silver bullet system to secure all of these.

Instead, what information security can do is develop an integration system around the aforementioned three areas within the software development process. The following are suggestions for how this can be done for each of the three domains.

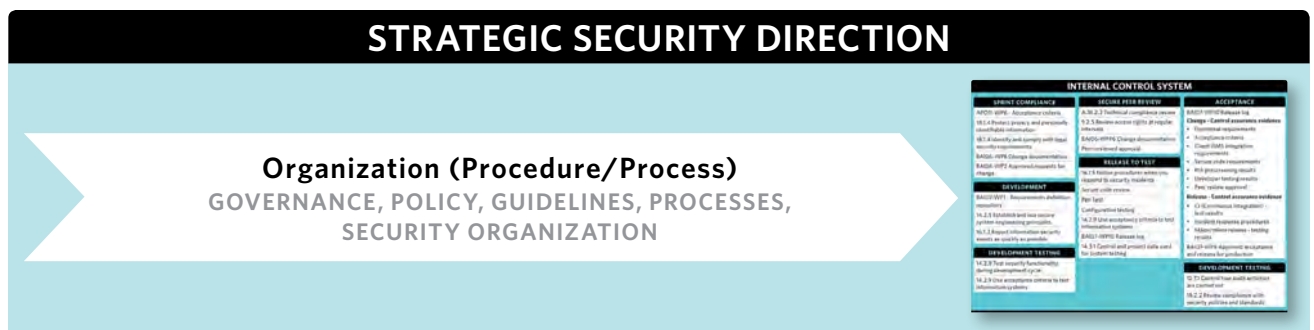
THE SECURE SOFTWARE DEVELOPMENT PROCESS

This domain focuses on SSD governance, which consists of three separate elements:

- SSD internal control system.
- Planned compliance and assurance effort.
- Written procedures.

SSD internal control system

This element manages IT risk by clearly defining what the organization expects from software develop-



INTERNAL CONTROL SYSTEM

SPRINT COMPLIANCE

APO11-WP6 - Acceptance criteria
 18.1.4 Protect privacy and personally identifiable information
 18.1.4 Identify and comply with legal security requirements
 BAI06-WP6 Change documentation
 BAI06-WP2 Approved requests for change

DEVELOPMENT

BAI02-WP1 - Requirements definition repository
 14.2.5 Establish and use secure system engineering principles
 16.1.2 Report information security events as quickly as possible

DEVELOPMENT TESTING

14.2.8 Test security functionality during development cycle
 14.2.9 Use acceptance criteria to test information systems

SECURE PEER REVIEW

A.18.2.3 Technical compliance review
 9.2.5 Review access rights at regular intervals
 BAI06-WPP6 Change documentation
 Peer-reviewed approval

RELEASE TO TEST

16.1.5 Follow procedures when you respond to security incidents
 Secure code review
 Pen test
 Configuration testing
 14.2.9 Use acceptance criteria to test information systems
 BAI07-WP10 Release log
 14.3.1 Control and protect data used for system testing

ACCEPTANCE

BAI07-WP10 Release log
Change - Control assurance evidence

- Functional requirements
- Acceptance criteria
- Client ISMS integration requirements
- Secure code requirements
- PIA prescreening results
- Developer testing results
- Peer review approval

Release - Control assurance evidence

- CI (Continuous Integration) - test results
- Incident response procedures
- Major/minor release - testing results

BAI07-WP8 Approved acceptance and release for production

DEVELOPMENT TESTING

12.7.1 Control how audit activities are carried out
 18.2.2 Review compliance with security policies and standards

ment in terms of security.

To create the SSD internal control system, we use internal security policies, COBIT and ISO 27002 to define the security controls required to secure our software development process.

Above is an example of what an SSD internal control system will look like and represents the security

controls mapped to example software development phases.

Planned compliance and assurance

This element involves designing security controls into the software development process where compliance to the controls has the least impact on market responsiveness.

Written procedures

Here we guide the development teams toward compliance and list the tasks they must perform to comply to the security controls set in the SSD internal control system.

Software development methodologies focus on rapid response to market; therefore, it's important that a software development process reflects this responsiveness requirement.

To help information security teams define a process sensitive to the importance of market responsiveness, I've documented a series of articles (<https://bit.ly/2kxqddC>) about building trust and maximizing value delivery of the Agile software development process.

SECURITY ROLES AND COMPONENTS



DEVELOPING SECURE CODE

Ensure secure code requirements are understood and correctly implemented at all stages of the software development process

SECURE CODE ASSURANCE TOOL

Define secure code requirements and provide code-level guidance and verification toward meeting these

BASIC VULNERABILITY DETECTION

Improve development team's basic vulnerability detection and prevention capabilities

SECURE CODE DEVELOPMENT

Both standard secure code and architectural requirements need to be considered when developing secure software. These considerations need to be relevant and available early in the development process—as well as

implemented across all development teams.

Standard secure code requirements ensure code cannot be exploited, such as by SQL injection or directory transversal attacks. Architectural security requirements ensure the software can be securely

deployed into the organization's environment and list, for example, the approved authentication mechanism to use. This domain holds two components: secure coding and basic vulnerability detection. Both are wrapped in the secure code assurance tool, which is aimed at making sure security requirements are defined, understood and implemented correctly.

Secure code assurance tool (SCAT)

The secure code assurance tool is an OWASP piece of software written in MVC C# with a MySQL database.

What does the tool do?

The secure code assurance tool (SCAT) is used by in-house and third-party development teams



Don't let it be you!

Secure every email. Protect every user.

• Talk to our experts • See a product demo • Enter to win a Nintendo Switch

.....
Speaker session | Defending impossible risk vectors: Human frailty, curiosity, and people-centric risks

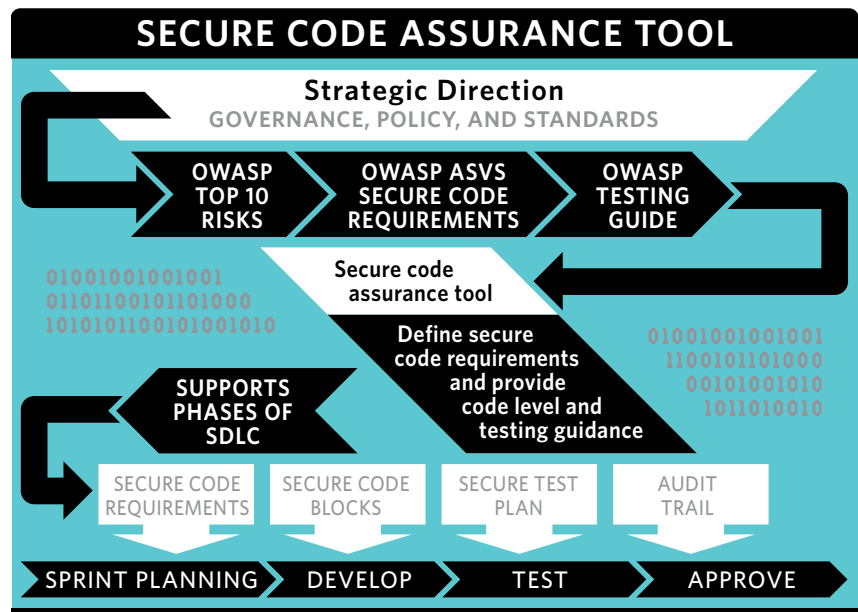
Monday, October 28th at 11:00 AM,
Room: Northern E3

Visit Egress
at booth #217

www.egress.com

to build, verify and assure secure software.

- **Build:** SCAT uses code-level guidance to clearly instruct developers on how to correctly implement security requirements.
- **Verify:** SCAT uses a combination of ZAP basic scans and security test plans to verify correct implementation of security requirements.
- **Assure:** SCAT centrally stores and publishes successful test results as an audit trail. It provides evidence, traceable through requirements, of a secure development process.



BASIC VULNERABILITY DETECTION

Improve development team's basic vulnerability detection and prevention capabilities

The idea behind the tool is to use “hacker tools” to give developers an insight into the world of a hacker.

The basic vulnerability detection component is a free, open source application called OWASP ZAP. This tool is installed on the developer's machine to perform basic vulnerability scans of the developer's code on localhost before committing it to the source code repository. The idea behind the tool is to use “hacker tools” to give developers an insight into the world of a hacker.

Working together with SCAT, which generates secure code requirements, it helps requirements and helps developers understand and

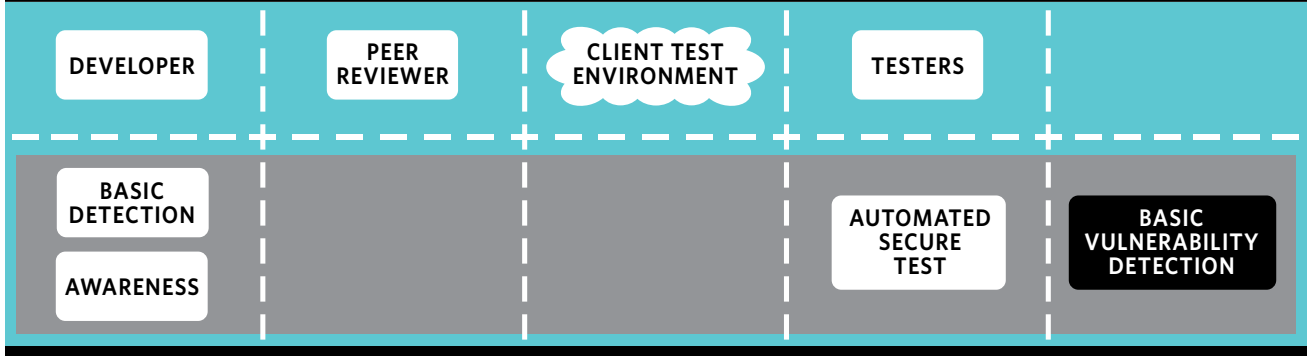
OWASP SECURITY INTEGRATION SYSTEM'S SCAT

For a more detailed look at the secure code assurance tool (SCAT), you can check out OWASP project documentation at https://www.owasp.org/index.php?title=OWASP_Security_Integration_System. This tool helps information security teams:

1. **ENABLE** developers to generate security requirements before development begins (https://www.owasp.org/index.php?title=OWASP_Security_Integration_System#Sprint_planning_phase).
2. **ENSURE** consistent and correct implementation of security requirements across all teams (https://www.owasp.org/index.php?title=OWASP_Security_Integration_System#Development_phase).
3. **GUIDE** the secure testing process (https://www.owasp.org/index.php?title=OWASP_Security_Integration_System#Testing_phase).
4. **STREAMLINE** the approval and audit process (https://www.owasp.org/index.php?title=OWASP_Security_Integration_System#Approval_phase).
5. **ENABLE** risk managers to prioritize, plan and monitor mitigation efforts (https://www.owasp.org/index.php?title=OWASP_Security_Integration_System#Risk_management).

—Michael Bergman

WHICH DEVELOPMENT TEAM ROLES USE THIS COMPONENT?

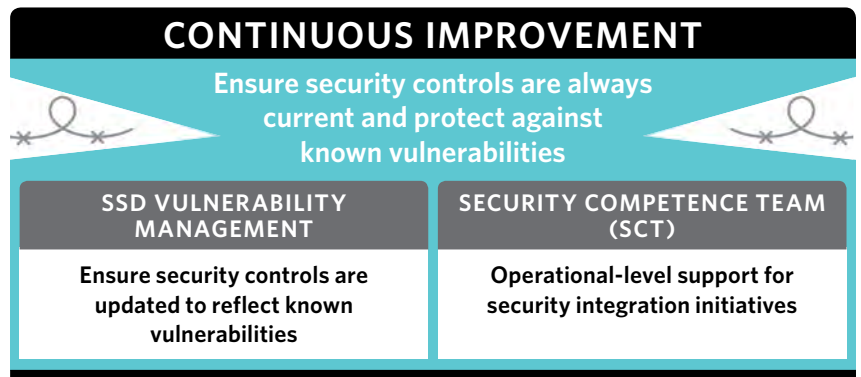


implement these.

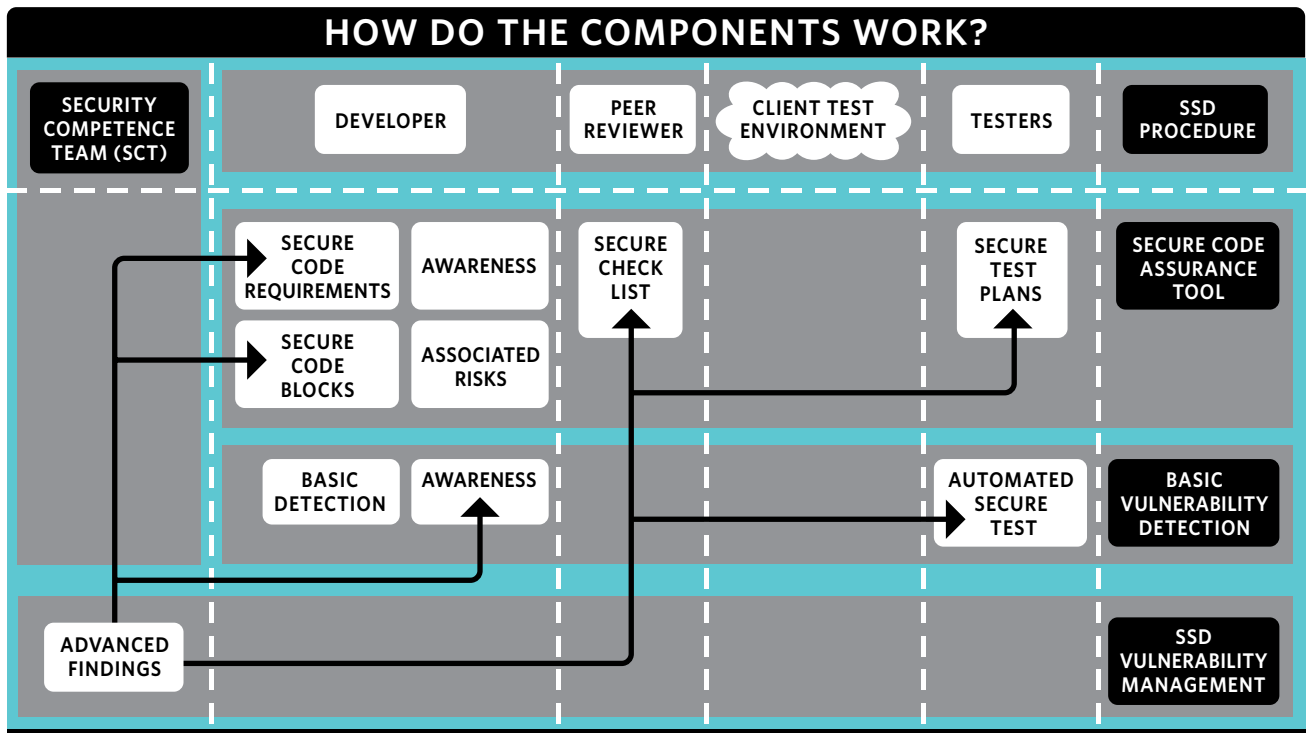
OWASP ZAP performs basic vulnerability scans to verify the developer's understanding and control implementation. The two tools build on each other to ensure a consistent and repeatable level of security.

OWASP ZAP allows the developer to enter into a fix-and-rescan loop to test the effect code-level changes have on fixing their own vulnerabilities. This loop will increase their level

CONTINUOUS IMPROVEMENT



HOW DO THE COMPONENTS WORK?



of awareness, improve their basic vulnerability detection and result in a better quality of code reaching peer reviewer after check-in.

CONTINUOUS IMPROVEMENT

Red teams use pen testing and other advanced detection capabilities to ensure our security controls protect against known vulnerabilities. The continuous improvement domain holds two components: SSD vulnerability management (VM) and security competence team.

SSD VULNERABILITY MANAGEMENT

Ensure security controls are updated to reflect known vulnerabilities

This component uses advanced detection capabilities like pen tests, code reviews and environment configuration tools like Nessus to detect more complex vulnerabilities. This element, supported by VM procedure, will guide the proper processing of the advanced teams' findings. Together, these two elements build on each other, ensuring all controls are updated to protect against known vulnerabilities.

SECURITY COMPETENCE TEAM (SCT)

Operational-level support for security integration initiatives

The team is made up of an interdisciplinary group of security champions selected from the Agile software development teams. This team is the human glue that binds together all these components across all domains.

The team's functions include:

When done properly and done well, the result should be more secure products both in development and in markets.

- Receiving and processing pen test report findings.
- Answering secure code questions.
- Updating the secure building blocks library.
- Updating the secure test scripts library.
- Managing the automation of security tests.

These activities ensure that complex vulnerabilities are detected and correctly processed to update all security controls. This, in turn, ensures that once a vulnerability is found and processed it will not reoccur when a different developer makes the same mistake in the following sprint, or two-week plan of work.

CONCLUSION

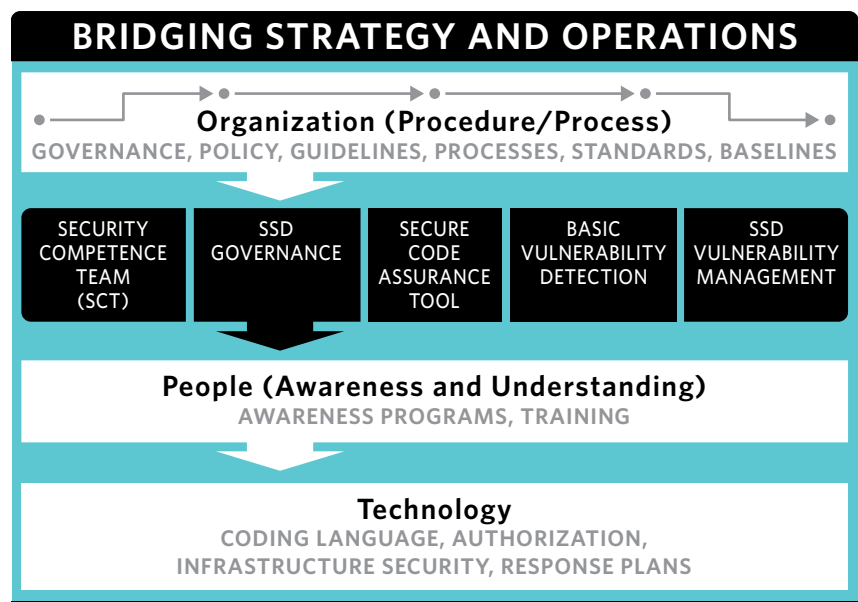
This software security integration system relies on proven, effective and essential tools, along with technical and administrative controls required

for secure software development.

The components build on each other to bridge the gap between strategic direction and operational-level software development teams. The functionality vertically cuts through all three lines of defense by first decomposing security policy into a security control system, then making sure controls are integrated and, finally, providing code-level guidance ensuring controls are correctly implemented.

When done properly and done well, the result should be more secure products both in development and in markets. ■

MICHAEL BERGMAN, CISSP, CCSP, CRISC, was born in Cape Town, South Africa, but has called a good few countries across a couple of continents home. He has a passionate interest in protecting and controlling software development activities, managing its IT risk and making security an inherent part of software development.



Is it Time We Made Time to Do More?

by Pat Craven

If there were 25 hours in a day, what would you do with that extra hour?

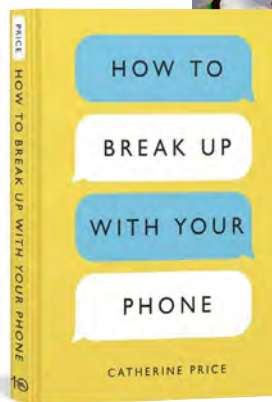
That is the opening question we will pose to teenagers as part of our new cyber safety program called Vita Unplugged. This is very different from any of our other efforts or anything else we have seen any organization teaching today. It is not the traditional 45-minute, PowerPoint-style lecture to upper-grade students. Instead, it is a four-week, curriculum-based program that focuses on helping students (and adults) develop a better screen/life balance.

Let's be real: There is no way we are going to convince teenagers to give up their phones and drop off the social media grid. But can we get them to cut back? Can we help them avoid the distractions of messages and endless scrolling? While we can't create a 25th hour in a day, we can help them gain an hour of their lives back. If they are on their devices just an hour less per day, they will be safer and more productive.

At the core of the curriculum is the book by Catherine Price (<http://www.catherine-price.com>), *How to Break Up with Your Phone* (<https://phonebreakup.com/>).

Through the book and other resources, articles and videos, the students will explore the reasons they spend so much time on devices and then learn what they can do to regain control over their phones and their lives. As part of the course, the students will be challenged to go offline for 24 hours to help them discover life (vita) unplugged.

We are thrilled to pilot the program this fall and do a larger launch in 2020. *How to Break Up with Your Phone* has already been published in 26 countries and is available in 18 different languages. Our goal is to be able to provide the program



on a global basis.

Speaking of global, a year ago, I promised that your Center for Cyber Safety and Education was committed to doing a better job of providing you—our volunteers, members and supporters—with with more innovative programs in multiple languages. I am proud to tell you we are keeping that promise and delivering more.

On our website, www.IAmCyberSafe.org, you will now find most of our Safe and Secure Online materials for parents, senior citizens and children in more than 20 languages! This is all thanks to more than 300 (ISC)² members who have volunteered countless hours to the project. And we aren't done. If you don't see your language on the site, please reach out to us at center@isc2.org and volunteer to help truly make it a safer cyber world.

Also, be on the lookout for the release of our new apps featuring Garfield. Thanks to the students and faculty at ECPI University (<https://www.ecpi.edu/>), we are converting our award-winning Garfield's Cyber Safety Adventures cartoons into fun and interactive apps.

Thank you for your continued support of our effort to make it a safer cyber world for everyone. ■



Pat Craven is the director of the Center for Cyber Safety and Education and can be reached at pccraven@isc2.org.

Image: iStock

Advice on Wiping Machines and Choosing Between SHA-1 and SHA-2

The (ISC)² Community has more than 23,000 cybersecurity professionals connecting, sharing knowledge and offering solutions in the online forum. Note that the questions and responses may have been edited for clarity and brevity.

QUESTION:

Is it overkill to wipe a machine after a successful phishing attempt?

Scans from two different AV products plus a rootkit scan came up empty on the user's machine. I play a paranoia card. (The user didn't report

the compromise AT ALL. We found out when another event occurred). The help desk is pushing back with "Wipe, re-image and restore is gonna take us forever! There was nothing found on the machine so gonna ignore your recommendation."

I would appreciate your thoughts on "wipe or don't wipe?"

—Submitted by d46j48fx

SELECTED REPLIES:

Wipe. If anybody has any suspicions, wipe. That said, the help desk is right to complain about MTTR [mean time to repair]. Users have jobs to do, and incident response prevents them from getting their work done. Instead of fighting for downtime, fight for tools, techniques and procedures that quickly and securely get the user back to normal.

—Submitted by denbesten



Identity and Access Management

PRIVILEGED ACCESS MANAGER

IDENTITY MANAGER

PASSWORD MANAGER



SECURITY CONGRESS

October 28-30
Orlando, FL

Attend a Demo at Booth 411

Get a Personalized Water Bottle



hitachi-id.com

HITACHI
Inspire the Next

I'm going to be a bit harsher here. The help desk does not get to make decisions of a security matter when it could mean damage to the whole organization. Their job is to ensure smooth operations, and if that means re-imaging a machine, then that's exactly what they do.

—Submitted by MikeGlassman

I am a fan of doing an entire clean re-image from a known clean source and restoring from known clean backups if you're dealing with a sophisticated threat or if you don't know who you are dealing with in terms of means and motivation. The evil-doers are very insidious and unless your management has a huge

appetite for risk, just to save staffers some time, I would flatten the infected systems and start from a known clean fresh start.

—Submitted by Frank_Mayer

In my opinion, wiping is overkill if you're utilizing images, dealing with end-user systems, aren't protecting sensitive data and have proper controls in place—in which case completely isolating a system from the rest of your network should suffice, since you may need it for investigations.

—Submitted by Shannon

Find this complete thread here
([https://community.isc2.org/t5/Tech-Talk/Is-it-overkill-to-wipe-a-](https://community.isc2.org/t5/Tech-Talk/Is-it-overkill-to-wipe-a-machine-after-successful-phishing/td-p/26322/page/2)

[machine-after-successful-phishing/td-p/26322/page/2](https://community.isc2.org/t5/Tech-Talk/Is-it-overkill-to-wipe-a-machine-after-successful-phishing/td-p/26322/page/2)).

QUESTION:

Is moving from SHA-1 to SHA-2 enough?

As SHA-2 shares the same algorithm as SHA-1, aren't the hash lengths subject to the same type of attacks? One would think that the industry would want to move to SHA-3 and avoid a repeat of the SHA-1 fiasco. Am I wrong? Am I reading too much into it?

—Submitted by clyoneer

SELECTED REPLIES:

SHA-2 is designed to provide protection against hash collision attacks but

Stop by Booth 117

Cybersecurity & Information Resilience

Protecting your people, information and reputation

Give us a call
1 800 862 4977
or visit us on the web
bsigroup.com/iso-iec-27001-us/



bsi.

"In the end, our job is to make it too expensive for an attacker to target our systems."

—wimremes

does not improve resistance against brute force or dictionary-based attacks so the answer will depend on what you are using SHA* for and what your overall threat model looks like. If hash collisions are relevant to your threat model, migrating from SHA-1 to SHA-2 might be suffi-

cient. If other attack types are more relevant, maybe you want to move to something else. In the end, our job is to make it too expensive for an attacker to target our systems. If using SHA-2 satisfies that need at an acceptable cost, it is good enough.

—Submitted by wimremes

Since I am not a crypto-geek, I leave it to others to interpret. However, the search results from the CVE database (<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=%22SHA-2%22>) and the National Vulnerabilities Database (https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=-SHA-2&search_ty...) may help inform the discussion.

—Submitted by CraginS

Find this complete thread here
<https://community.isc2.org/t5/Tech-Talk/SHA-2-Vulnerability/m-p/25746#M1571>.



ISHPI is a globally recognized leader in CMMI Maturity Level 5 Cyber-Secure Software Development and the winner of the 2013 Government Information Security Leadership Award for secure software lifecycle practices as well as a past IEEE Computer Society Software Process Achievement Award winner.

We work in concert with other defenders of the Homeland to fortify national preparedness, agility, strength and advantage in the cyber domain – a readiness state we refer to as a Holistic CyberStance. Using our integrated Holistic service solutions, we weave the armor and forge the weapons that enable our clients to maintain a dominating Holistic CyberStance – always ready to Anticipate, Defend, Exploit and Attack in the Cyber domain.

Our Information Operations, Advanced Information Services, CSISR Engineering & Technical Services, and Training & Consulting business units work in unison to provide experienced people, proven processes, technology, advice and leadership to enable full spectrum Cyber capability.

INFORMATION OPERATIONS



ADVANCED INFORMATION SERVICES



CSISR ENGINEERING & TECHNICAL



HEALTH CARE IT SERVICES



TRAINING & CONSULTING



WWW.ISHPI.NET



CMMI DEV/5
Exp. 2020-02-09 / Appraisal #28477



WORKING A SAFE AND SECURE CYBER WORLD





CENTER FOR **CYBER SAFETY AND EDUCATION™**

- Take Your Kids to Work Day
- Adopt a School
- Employee Volunteer Program
- Digital Health and Wellness Program
- College Scholarships

STAND OUT WITH YOUR CORPORATE SOCIAL RESPONSIBILITY PROGRAM

- Improve public image
- Increase media coverage
- Boost employee engagement
- Attract and retain investors

**IAMCYBERSAFE.ORG
CENTER@ISC2.ORG**

Visit CSA at
Booth #110

CSA EMEA Congress 2019



The Cloud Security Alliance is proud to host the 2019 EMEA Congress in the home of our new European Headquarters: Berlin, Germany. This multi-day conference will feature trainings, educational sessions and networking opportunities for cloud security professionals. Attendees, representing both end-user and industry viewpoints, will experience a unique mixture of compelling presentations and topical discussions on research, development, practice and requirements related to cloud security.

This year marks the ten-year anniversary of CSA. From inception, the CSA has been dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment throughout the world. The CSA EMEA Congress is our time to reflect on the lessons learned by enterprises and providers as cloud has become the dominant IT system in the market. We will also explore new frontiers that are accelerating change in information security, such as artificial intelligence, blockchain and IoT. Join us in celebrating this milestone year at the CSA EMEA Congress as we bring key thought leaders to the main stage and look ahead to the next ten years of cloud security.

November 2019
Mon, 18th - Thu, 21st

Hotel Adlon Kempinski
Berlin Germany

