LEARN. TRAIN. FIGHT.

Advancing InfoSec Operations Through Tradecraft Enhancement

CHIRON

CONTENTS

PART I:

AN INTRODUCTION TO TRADECRAFT

CONVERGING THEORY AND EXPERIENCE

There are two fundamental components of becoming a qualified InfoSec operations professional:

1. THEORY:

You're presented with information about the latest cyber threats and remediation tactics, you study those materials and then pass a written exam.

2. EXPERIENCE:

You put skills into action to discover challenges and overcome them, i.e., map networks, perform penetration testing, attempt to detect intrusions and build cybersecurity tools.

For individuals seeking to enter into the InfoSec workforce, certifications are proof of a theoretical understanding of security operations, which is crucial.

Certifications – a signifier of InfoSec acumen – are often supplemented and enhanced by live simulations in real-world environments. That takes skills derived from experience. And the fastest and most effective way to acquire those skills is through the cultivation of and attention to developing and perfecting the operator's tradecraft.

WHAT IS TRADECRAFT?

Tradecraft is the culmination of an individual's techniques, methods, tactics and technologies, which are applied toward achieving a certain objective.

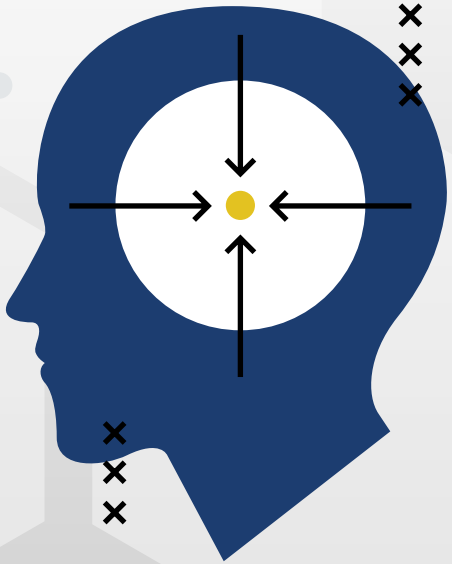
In InfoSec operations, training should improve or refine this repertoire of mission resources. This requires a four-step process:

1. EVALUATE:
Identify strengths and deficiencies and establish a benchmark for improvement.

2. TRAIN:
Emulate real-life scenarios that test skills and refine methodologies in the context of live adversarial situations.

3. VALIDATE:
Complete exercises to rate performance as it aligns with role functions.

4. SUSTAIN:
Student continues to develop skills to match adversarial threats, never lets sharpness atrophy.



Through this process, InfoSec professionals expeditiously gain real-world familiarity with the nuances of information security operations.

WHY IS TRADECRAFT ENHANCEMENT SO IMPORTANT?

Entry-level InfoSec operators may possess the necessary knowledge, but not the experience to effectively combat live threats.

And while baseline security training may be enough to keep amateur adversaries at bay, it's not the same as cultivating the experience-based skillsets that are needed to contend with the most seasoned cybercriminals.

We don't put soldiers into battle without running drills that train and validate their use of their equipment, and we should not expect new InfoSec recruits to excel at a task haven't actually practiced either.

This is the central problem tradecraft enhancement addresses in a short period of time.

PART II:

THE ADVERSARY IS STRONG. WE NEED TO BE STRONGER.

INFOSEC FACES GREATER ADVERSARIAL CHALLENGES

The Identify Theft Resource Center tallied more data breaches in 2016 than in any year prior. Tellingly:

- The private sector accounted for the majority of those breaches, with an average cost of $4 million per incident, according to IBM's security division.
- **Hacking and/or phishing was the most significant source of intrusion (55.5 percent).**
- The above percentage represents a 17 percent increase over 2015.

The findings of a major Data Breach Investigations Report by Verizon paint a similar picture, with malicious hacking topping the list of breach origins.

The report also found that 81 percent of the breaches and security incidents analyzed stemmed from stolen or compromised passwords. These intrusion tactics are inherently more challenging to detect and defend against.

Also, over the course of 2017, the application attack perimeter is expected to expand by 111 billion lines of code. This, paired with the increasing use of mobile and cloud in business and the rising tide of criminal hacking, is making information systems more difficult to defend.

THE SECURITY TALENT SHORTAGE IS REAL

To make matters worse, modern organizations lack the luxury of time. As criminal hackers become more adroit and advanced malware continues to proliferate, the world faces a global shortage of InfoSec professionals.

Today, there are an estimated 1 million global InfoSec vacancies - with 350,000 of those in the U.S. By 2021, the number of openings worldwide is expected to reach 3.5 million.

Meanwhile, 82 percent of IT staff members already believe that there are notable InfoSec shortfalls within their organization.

It begs the question: How can we possibly train enough mission-ready InfoSec professionals from the ground up, when we already have a talent deficit?

Like the threat actors themselves, we need to get stronger and more organized, and fast.

PART III:

TRADECRAFT AS THE X-FACTOR

TO CONTEND WITH NEW THREATS, IT TAKES AN ARMY

Already, we have the makings of one: the IT workforce.

One of the more compelling solutions to the InfoSec workforce shortage is the concept of cross-training IT professionals.

Specifically, organizations can handpick IT staff members within an organization who exhibit an aptitude for InfoSec operations, and then cultivate those skills. It's a simple idea, and one that goes against the notion that InfoSec talent must be plucked from a limited pool of pre-existing cybersecurity professionals.

This addresses two problems:

1. It significantly expands the inventory of InfoSec talent.
2. In doing so, it mitigates the cost of a skill that is in short supply and high demand.

MORE TRAINING IN LESS TIME WITH TRADECRAFT ENHANCEMENT

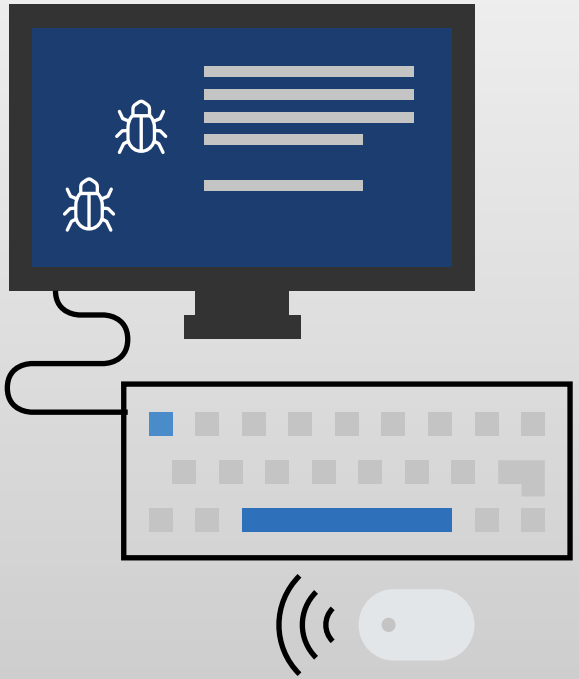
Given the state of IT security, the new InfoSec workforce cannot simply be "adequate." It needs to be agile, methodical and ready for anything, and it needs to get there fast.

This brings us to tradecraft enhancement.

Accelerating, customizing and continuously advancing the development of critical InfoSec skills by focusing on the most up-to-date defenses, detection and counter-intrusion tactics facilitates the improvement and maturation of an individual's and organization's tradecraft.

In the earliest stages of this training, students gain hands-on knowledge of commonly used operating systems. They'll also practice deep packet inspection, and conduct network forensics and cyber threat triage.

During this time the strengths and weakness of their tradecraft are evaluated, so they can move on to job task training.



CULTIVATING INFOSEC SPECIALISTS THROUGH ROLES-BASED TRAINING

Tradecraft enhancement is ideal for accelerating the development of job-ready skills because it relies on roles-based training and validation. What do we mean by that?

Think of physicians who focus on specific aspects of human health. While the various specialists may possess shared techniques and skills (called "core operations" in InfoSec tradecraft), an orthopedic surgeon will have a very different training regimen than a pulmonologist. A cardiovascular doctor will run different types medical simulations than an oncologist, and so on.

At Chiron, we divide role-based training into four job-functional areas:

1. **CYBER PROTECTION**
2. **CYBER THREAT EMULATION**
3. **DISCOVERY & COUNTER INFILTRATION**
4. **CYBERSECURITY DEVELOPER**

Each plays a critical role in developing mission-ready InfoSec professionals who have the expertise they need to perform real-world functions with proficiency.

TRAINING FOR THE MISSIONS AHEAD

There are some qualities of an InfoSec recruit that cannot be cultivated without the real-world, scenario-based training that underlies tradecraft. These include:

CIRCUMSPECTION:

An acute awareness of the many variables and risks involved in certain InfoSec operations.

CONTINGENCY:

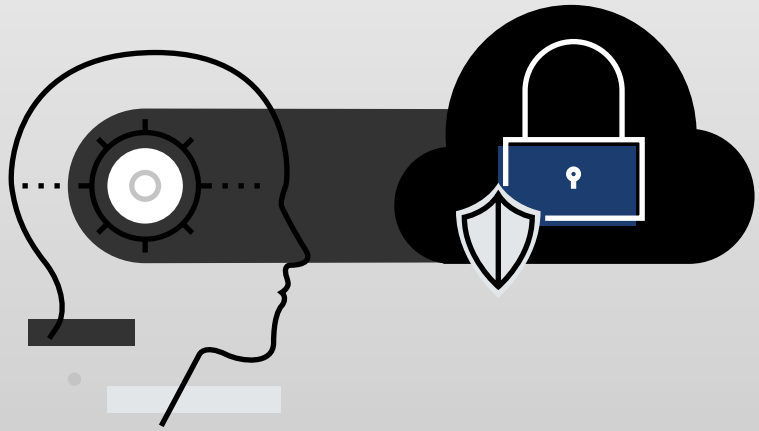
The ability to quickly and methodically adjust to sudden or unexpected changes in certain operations.

COMPETENCY:

Razor-sharp acumen in specialized, skills-based arenas in addition to comprehension of the facts.

Generally, these are traits that we expect to acquire through time spent on the job. With tradecraft enhancement, that experience is expedited through intensive, highly methodical training.

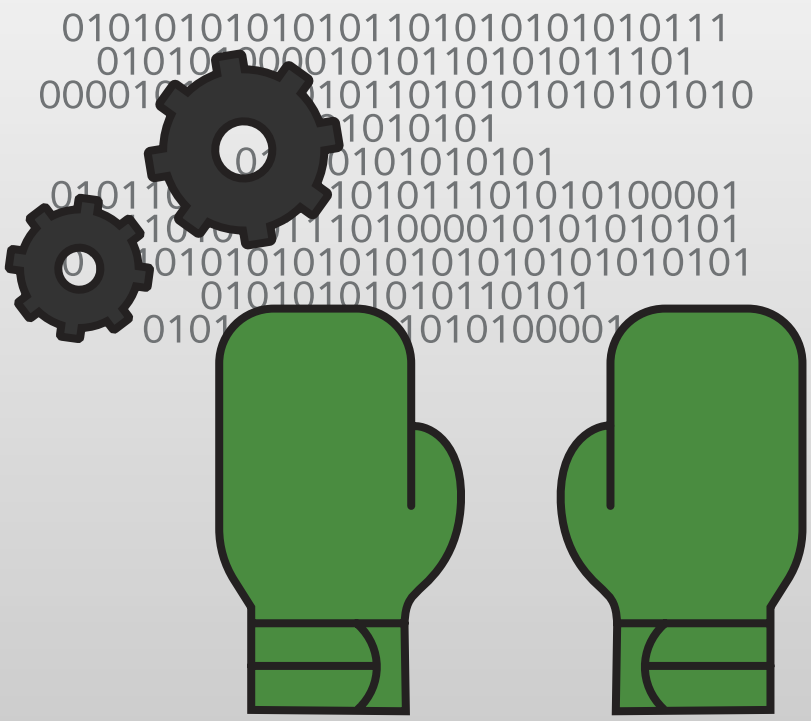
Tradecraft enhancement means students don't have to learn everything on the job - it boosts the skills they need to do their best work before they start.



LEARN THEORY, BUT TRAIN LIKE YOU FIGHT

Tradecraft enhancement is best summed up as:

"TRAIN LIKE YOU FIGHT."



Mastering theory, earning security certifications and running limited simulations exercises certainly have their place. But that's just learning.

Training, on the other hand, must happen through experience, with intensive, hands-on, real-world exercises that spare no detail or possibility.

Technology is always changing, and cybercriminals are constantly innovating. Only a tradecraft training methodology keeps you one step ahead of change, and an order of magnitude above the adversary.

SOURCES:

1. www.idtheftcenter.org/2016databreaches.html
2. www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
3. www-03.ibm.com/security/data-breach/
4. searchsecurity.techtarget.com/news/450412944/Nation-state-cyberattacks-rising-warns-former-NSA-director
5. www.marketwired.com/press-release/111-billion-lines-of-new-software-code-will-need-to-be-secured-in-2017-2190245.htm
6. www-01.ibm.com/software/data/bigdata/what-is-big-data.html
7. www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html
8. newsroom.intel.com/news-releases/global-study-reveals-businesses-countries-vulnerable-due-shortage-cybersecurity-talent/
9. www.scmagazine.com/35m-vacant-cybersecurity-roles-by-2021-cybersecurity-ventures-report/article/666895/

CHIRON

CORPORATE HEADQUARTERS

Chiron Technology Services, Inc.
7021 Columbia Gateway Dr. Suite 250
Columbia, MD 21046

Phone: 410.672.1522

GEORGIA REGIONAL TRAINING FACILITY

Chiron Technology Services, Inc.
3152 Perimeter Parkway
Augusta, GA 30909

Phone: 706.432.6127