# THE DIR CYBERSECURITY INSIGHT

August FY2017 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

## Saved by the Bell!

Back to School. The phrase brings relief and fear to the minds of parents, teachers and students everywhere.

At the start of each school year, the Texas Department of Public Safety sends a reminder that drivers need to pay extra attention around school buses and should especially watch out for children who may be walking to or from school or waiting for buses. With increased traffic, comes an increased need for safe driving. For security professionals, the start of the school year brings reminders to parents and students about safe habits around their devices and Internet usage.

We remind parents and students to protect their laptops, tablets and mobile devices by regularly installing updates, security software and backing up their data often.

We remind parents and students to protect their information. Children are taught at a young age to share, yet ironically, we find ourselves stressing the limits of what they should share online. A Pew Research Center survey found that 94% of parents say they've talked with their teen about what is appropriate for them to share online -- but only 40% do so frequently.

We remind all users that things may not be as they appear. The email that seems to be from a friend or company may actually be a fake email intending to install malicious software or capture personal information.

We remind users to think before they post information online because there aren't any "takebacks" on the internet and you lose control of who sees the post or where it goes. Children are taught "stranger danger," yet most younger users don't see someone they meet online as a "stranger." Additionally, one study found that one-third of teens who met someone online followed up by meeting them in person.

We're all reminded that information security and safety is not limited to school hours, but rather is a continuing day-to-day educational process for all of us. So, is it 'Back to School' or 'Always in School'?

## CONTENTS

### Monthly Article

### Updates

## EVENTS

### Save the Date

- **Webinar: The State of Cloud Security** September 12 @ 9:00 a.m. (Email invite coming soon)
- **ISC2 Security Congress 201** September 25-27, Austin Link to Event Information
- **InfraGard National Members Alliance (INMA) Congress & Conference** September 24-28, Dallas Link to Event Information

# NSOC Update – What is Security Onion?

Security Onion is the open source tool kit in use by the Network Security Operations Center (NSOC) for network security monitoring (NSM). Onion software is free to use and the only cost is that of hardware and time. Each piece is stable and reliable. Onion adheres to the philosophy of the Linux OS its built on, like an old school erector set. If it lacks features you need, those can be bolted on with the right skillset. Like other Linux distros, the developer's imagination is the only limit.

Check out https://securityonion.net to get to know Security Onion. Doug Burks, Onion's primary developer, invites you to 'peel back the layers of your network.' Securityonion.net includes brief descriptions of Onion and lists out nine primary tools included with Onion. Onion can be deployed in minutes. It works reliably within a distributed architecture which is a collection of multiple Onion systems working together. You can build an interconnected stack that works together inspecting network traffic with open source software.

Securityonion.net shows the different types of data that Security Onion generates and processes. The site also exhibits images of the CapMe, Squil, Squert and ELSA interfaces that the analysts use during investigations.

Don't waste time developing your Security Onion without these important requirements. First, you need the right kind of network connection. Proper network monitoring cannot be accomplished without strategically connecting your Onion Sensor's monitoring interface to the physical route of bulk network traffic commonly found inside your perimeter firewall. Connect to either a tool port on a fiber aggregation switch or directly to a network tap. To monitor smaller network segments such as user or core datacenter VLANs a span port may also be configured on the switch that comprises these segments.

Second, you must have Security Onion Solution's Github Site located at https://github.com/Security-Onion-Solutions/security-onion. Specifically, the Github page is where you can read the hardware requirements, download Security Onion and check the integrity of your download. Before you begin installation read the first 7 articles on the right of the page under 'Getting Started'.

Snort is the focal point recommended for beginners. It compares each TCP/IP packet to its active rule set. When a packet breaks a rule, Snort alerts the Sguil database and adds an event to the Squert console. The analyst sees the alert or receives an email from Squert and begins investigating. Bro NIDS demands more time hunting for protocol abuses. It is recommended that absolute beginners leave packet capture disabled and focus on Snort. Onion generates a lot of alerts. Before dismissing Onion as one big false positive generator you must tune it to your needs. Read 'Managing Alerts' in the Github Wiki. Disable, suppress and threshold your rules. As the local administrator, know your network and shape the ruleset so actionable Indicators of Compromise (IoC) rise to the surface.

If you have any questions, contact Mac Cole ( mac.cole@dir.texas.gov).

# Services Updates

### SPECTRIM Update

We're making a few changes in the Risk and Incident Management areas, so stay tuned for updates after the start of the fiscal year! We will also offer training webinars after the changes go into effect.

***Please Note:*** *From September 1-15, the Risk Management module will not allow new risk assessments to be created. We apologize for any inconvenience this may cause.*

### Security Assessment Update

Good news! The coming biennium brought major changes in the cybersecurity realm – including assessments. To help agencies, DIR is able to provide more assessments at no cost to the agencies. We have 40 assessment slots available for each fiscal year in this biennium. Keep in mind that if you are an agency scheduled to go through a sunset review in the next two years, you will need a recent security assessment. If you are interested in an assessment, please contact dirsecurity@dir.texas.gov.

### UT Austin Offers Security Services

The UT-Austin Security Office has created and licenses several security tools for the enterprise – from incident management to credential management to risk assessments. More information can be found at https://security.utexas.edu/apps-services.

The UT Austin ISO also offers managed security services and assessment services to Texas agencies and institutions of higher education. Please feel free to contact security@utexas.edu if you would like any information about these services.

# IoT Security

During CompTIA's ChannelCon 2017 event, one of the hot topics was Internet of Things (IoT) Security. Simply put, an IoT device is anything that can be assigned an IP address with the ability to transfer data over a network. IoT devices can be anything from a heart monitor to a home thermostat to a tire pressure sensor in an automobile. Some of the most popular IoT devices are smarthome hubs (Amazon Echo), fitness trackers (Fitbit), and home security systems (Honeywell). These devices create an inter-related network of connectible computing devices that allow us to access, generate, and share data with ease. At the same time, these devices have also created a new security threat, targeted for malicious intent.

You may recall some time ago about the Mirai DDoS attack orchestrated by hackers to disrupt DNS service to companies like Netflix, Twitter, and AirBnB. They hijacked IoT security cameras, using default admin privileges and running unpatched operating systems, to take control of the devices and perpetrate the DDoS. Other security horror stories include the commandeering of internet-enabled refrigerators for spamming scandalous imagery, eavesdropping on private home conversations using baby monitors, and the complete takeover demonstration by security researchers of the 2014 Jeep Cherokee which led to a massive 1.4 million vehicle recall.

***The Problem*****:** So why is it so easy for hackers to take control of these devices? IoT Agenda gives us some very interesting answers. First, networking appliances, watches and similar devices are still a relatively new concept and security is not always considered a crucial component in the design. Second, the increasing popularity of providing users with a unique and ever-prevalent experience is a serious driving force in IoT device production. To remain competitive in a market of ever-changing consumer demand, companies need to get their devices out quickly. This often results in IoT devices being shipped with older and often unpatched software. Third, customers do not often change the default password of their IoT devices. If they do, they tend to choose a weak or inefficient password.

***Solutions:*** Wired, CSO Online and Bastille give the following recommendations:

**Create a separate network**. Since most IoT devices require Internet access to function, segment these devices into their own subnet, away from your primary network. Then, restrict access within their subnet by using local security policy tools and disabling null sessions to prevent anonymous sessions. Finally, monitor their subnet to identity potentially anomalous traffic and take appropriate action when it is detected.

**Ensure the latest firmware**. By keeping IoT devices up-to-date on firmware, you reduce the risk of a successful attack or compromise on these devices. Vulnerabilities will be patched as they are discovered, so make sure you to check for updates regularly. If it's possible to automate the process by setting up a schedule to check for updates, it's best to do so.

**Improve password usage**. Change out the default password on IoT devices immediately. Don't choose a common password and avoid using the same password for every device. If you're having trouble making up a good password, try passphrases and even password generators/managers.

**Limit or keep out IoTs from the workspace**. Make a Bring Your Own Device (BYOD) policy that does not permit the use of IoT devices at work; or if you have a Mobile Device Management system, create policies for IoT within that system. Doing so can at least minimize business risk while optimizing functionality and security. Make sure to have management approval beforehand and educate your users to ensure they understand and agree to the policy. Both are crucial!

**Don't connect unless it's needed**. As the number of IoT devices rise over the next several years, we must take a step back and really analyze these devices' functionality. Sure, a fridge or toaster *can* connect online. But is the online feature truly necessary for me to use the device for its intended purpose?

More information on IoT security can be found at the links below.

- http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security
- https://www.forbes.com/sites/gilpress/2017/03/20/6-hot-internet-of-things-iot-security-technologies/#5c96391e1b49
- https://krebsonsecurity.com/2017/08/new-bill-seeks-basic-iot-security-standards/
- https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/
- https://arstechnica.com/information-technology/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/
- https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/
- https://www.bastille.net/mission/

# Cybersecurity Coordinator Spotlight

## Cam Beasley

## Chief Information Security Officer

## University of Texas Austin

**Certifications?**

*CISSP, CIFI*

**Tell us about your educational and professional background. What agency do you work for? Tell us a little about it.**

I have a BS from UT Austin in Chemical Engineering, with a focus on Biomedical Engineering.

I have worked for UT Austin since 1996 and in the UT Austin Information Security Office since 1998.

**How did you get into the security field?**

I have had a natural curiosity for how computers worked since I got my first computer in the late 80's (I'm so old!). When I came to UT in '96 I started working at the High Performance Computer Center (now known as TACC – Texas Advanced Computing Center) supporting services for TENET – an entity focused on serving K-12 educators across the state. It was a lot of fun and from there I transitioned into a lone security role for UT Austin as a student in '98 before the Information Security Office was actually formed. The role (and the office) matured over time and today it is awesome to see the impact our function has on the university.

**How has information security has changed since you entered the field?**

I started out focusing on issues associated with students hosting media on local systems (violating copyright), using e-mail (then via MUTT or PINE) to harass each other, or launching attacks against campus resources. Things evolved into external entities scanning and attacking unpatched Windows systems -- then came fun events like CodeRED, Nimda, and SQLslammer.. Today, we have a much more diversified attack surface and a wider variety of attackers (state sponsored, hacktivists, organized crime, etc.).

**Who are your users/customers, and what is one of the most challenging areas for you?**

Students, Staff, Faculty at UT Austin are our primary customers.

We also serve the campuses within UT System, other municipalities across the state connected to UT's wide area network. We also work with DIR to offer security services to state agencies they serve. Lastly, we serve other higher education institutions across the country with products/tools we have created and extended to them.

**What do you like best about your job?**

I really enjoy the overall mission of serving a diverse population and working with a super talented team to make a difference that I alone could never achieve.

**What other career would you have liked to pursue?**

I had originally planned to become a research scientist in tissue engineering before I was lured away by the siren call of infosec.

**What has been the greatest challenge that you have faced, and how did you resolved it?**

Working to secure a very complex place like UT Austin, with a wide range of diverse opinions and needs and some of the brightest minds, has been a huge challenge. I wouldn't say it has been fully resolved, but we've made massive strides over the years in changing culture, business processes --- and improving the overall security posture of campus.

**What is something you are proud of?**

I am really honored to have helped form such a talented team of folks who are dedicated to securing the campus. Our team dynamic, communication and skill level is truly remarkable and I can't imagine working with a better group of folks.

**What are your top 3 life highlights?**
So far, they would have to be my marriage, my three children, and my connection to UT Austin.

**Where did you grow up?**
Dallas, Texas and moved to Austin as soon as I could.

**What are your hobbies?**
Brewing beer, woodworking, infosec.

**People would be surprised to know that you…**
I was a Dallas High-School All-Star in baseball and turned down a scholarship at a small Texas college to go to UT (because they have the best chemical engineering program, of course!).

**What is your favorite line from a movie?**
I've lost the bleeps, I lost the sweeps, and I lost the creeps. (Spaceballs)

**Do you have a favorite book you would recommend?**
None that I would recommend.

**What kind of music or podcasts do you enjoy?**
Early blues, early jazz, and electronica.

**If you could interview one person (dead or alive) who would it be?**
Nick Offerman. He's a great woodworker and I'd like to pick his brain – plus his straight-faced, dry humor cracks me up.

**Describe what you were like at age 10.**
A terror.

**What is one thing you couldn't live without?**
My family.

**What is your hidden talent?**
Seeing patterns in data??

**What is the best advice you have received?**
If you really want something and get told no – be persistent and keep trying.

**Give a word of advice for a new security professional.**
Develop a rational distrust of most things.