Hunt, Bourne and Ryan are Amateurs: *Using CTI to Save the World*

4OCT2023
Oregon Cyber Resilience Summit

MATT SINGLETON

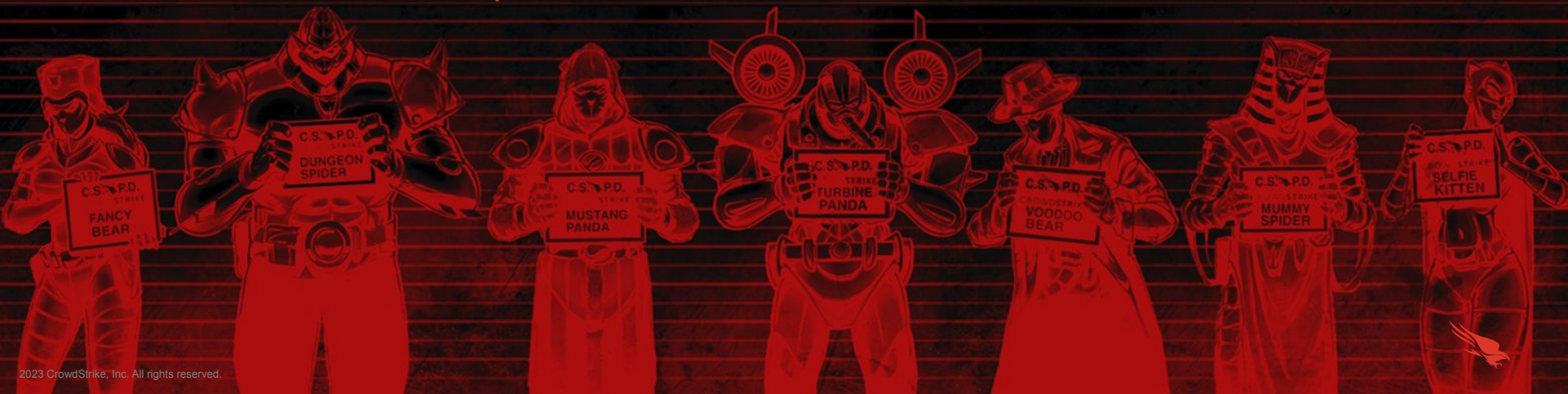
Executive Strategist

HIGHER ED | GOVERNMENT | CONSULTING

- **25+ years:** Innovating at the intersection of security, education & digital transformation
- **State Government:** Former Chief Information Security Officer for the State of Oklahoma; Chief Operations Officer for the state's IT division; State Chief Information Officer for Education
- **Higher Education:** Developed cybersecurity strategy and program for the University of Oklahoma system; Led innovation arm of OU IT; Professor of Cybersecurity
- **Education:** M.PS. – Applied Intelligence, specializing in Cyber Intel, Homeland Security & Counterterrorism from Georgetown University; B.A. – Administrative Leadership from the University Of Oklahoma
- **Thought Leadership:** Momentum, National Association of State Technology Directors; Hunt, Bourne and Ryan are Amateurs, Threatday

AGENDA

- Art of Intelligence
- Cyber Threat Intelligence
- Pre/Post-Pandemic Dynamics
- CTI Application



Art of Intelligence

“There are known knowns. There are things we know that we know. There are known unknowns. That is to say, there are things that we now know we don't know. But there are also unknown unknowns. There are things we do not know we don't know.”

– Secretary of Defense Donald Rumsfeld, 12 February 2002

CROWDSTRIKE

Rumsfeld's Quote

	Al-Qaeda Example	Violent Crime Example	Cybersecurity Example	Intelligence Action
There are known knowns	We know that al-Qaeda's intent is to commit more terrorist attacks against the U.S. and U.S. interests.	We know there is an increase in violent crime using guns within a community.	We know MS-NRPC has a critical vulnerability that could allow the compromise of all AD.	The information we know must be consistently monitored and verified (i.e., "standing requirements") to determine any changes in the status of the information we know.
There are known unknowns	We know that al-Qaeda has plans for future terrorist attacks, but the timing, method, and locations are unknown.	We know there is an increase in black market guns, but it is unknown who the supplier is, where the guns come from, or how the transactions are made.	We know other nations will try to influence US elections, but all strategies/tactics not yet known.	We know that we have intelligence gaps. Intelligence requirements, sources, and methods must be defined so that we may learn the currently unknown information.
There are unknown unknowns	If al-Qaeda has developed new alliances or new methods to commit attacks, these are unknown to us.	There are factors driving the increase in violence beyond the availability of guns; however, these other factors are unknown to us at the time.	Fraudsters will exploit eligibility programs during the pandemic; however, their targets and priorities are unknown to us.	Information must be collected from all sources and analyzed in an attempt to identify new threat information.

CROWDSTRIKE

What is Threat Intel?

Gartner defines threat intelligence as *“evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets.”*

Internal Threat Intelligence – What we have:

- Discovered,
- Experienced, or
- Developed.

External Threat Intelligence - What we get from external data sources:

- Subscription feeds,
- Proprietary reports,
- In-depth analysis on threat actors, their tactics, techniques and procedures (TTP), and
- Often industry-specific.

CROWDSTRIKE

Does Cyber Really Matter?

Cyber Meets Physical:

- Doxing
- Internet of Things (IoT)
- Smart Vehicles
- Social Media
- Security/Safety Systems
- Medical Systems

https://www.securitymagazine.com/articles/92518-the-need-for-cybersecurity-and-physical-security-convergence

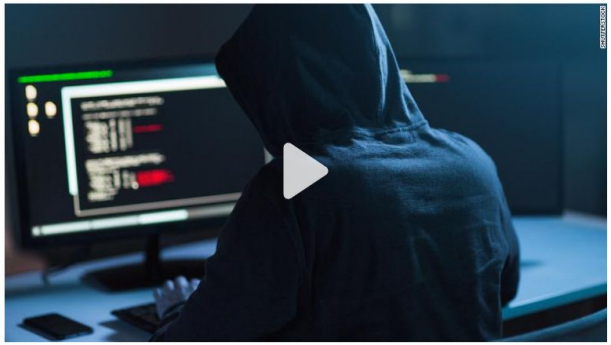
CROWDSTRIKE

High Stakes

CNN US Crime + Justice Energy + Environment Extreme Weather Space + Science LIVE TV Edition

Florida water treatment facility hack used a dormant remote access software, sheriff says

By Alex Marquardt, Eric Levenson and Amir Tal, CNN
Updated 5:03 PM ET, Wed February 10, 2021



Remote work leads to growing concerns over cybersecurity 02:24

More from CNN


Supreme Court wipes away ruling that said Trump violated...


Slain Capitol Police officer to lie in honor in US Capitol next...

Advertisement

(CNN) — A hacker who last week tried to poison a Florida city's water supply used a remote access software platform that had been dormant for months, Pinellas County Sheriff Bob Gualtieri told CNN on Tuesday.

The cyber-intruder got into Oldsmar's water treatment system twice on Friday -- at 8 a.m. and 1:30 p.m. -- through a dormant software called TeamViewer. The software hadn't been used in about six months but was still on the system.

"How they got in, whether it was through a password or through something else, I can't tell you that," said Gualtieri.

https://www.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html

The New York Times

Cyber Attack Suspected in German Woman's Death

Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital's computers. It could be the first fatality from a ransomware attack.

The ransomware attack involved servers at the University Hospital Düsseldorf on Sept. 10. Roland Weihrauch/dpa, via ZUMA Press

By Melissa Eddy and Nicole Perlroth

Sept. 18, 2020

BERLIN — The first known death from a cyberattack was reported Thursday after cybercriminals hit a hospital in Düsseldorf, Germany, with so-called ransomware, in which hackers encrypt data and hold it hostage until the victim pays a ransom.

https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

CROWDSTRIKE

Pre-Pandemic

THE OKLAHOMAN SUBSCRIBE NOW

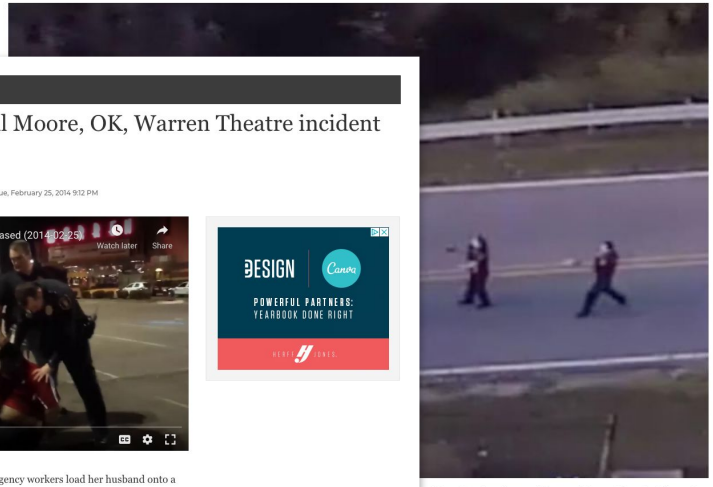
Hearing reset for Oklahoma woman in horse theft and animal cruelty case

BY JIM WILLIAMSON, AP
Published: Fri, March 9, 2012 12:00 AM

TEXARKANA, Ark. — A preli
County, Okla., District Court
five horses.

TULSA WORLD Timeline: The shooting of Terence Crutcher SHARE THIS

Sept. 19, 2016: Police release video of shooting



g the chatter heard from the police helicopter
uld be on something."

During an afternoon news conference, Tulsa
r or in his SUV.

THE OKLAHOMAN SUBSCRIBE NOW

Cellphone video in fatal Moore, OK, Warren Theatre incident is made public

by JENNIFER PALMER
Published: Tue, February 25, 2014 12:00 AM | Updated: Tue, February 25, 2014 9:12 PM

The panic in Nair Rodriguez's voice peaks as emergency workers load her husband onto a stretcher in the Warren Theatre parking lot.

Her hands are shaking, blurring the cellphone video she's shooting, and she's now screaming to her husband of 22 years, calling him "Papa."

"Papa! Is he OK? He doesn't move!"

"They've got him and they're going to take care of him," an officer responds.

"He doesn't move! You killed him! You killed him!"

Five law enforcement officers pinned Luis Rodriguez, 44, to the ground and handcuffed him

TIME WHY I BELIEVE MYANMAR'S PROTESTERS WILL SUCCEED' VIDEO NEWSLETTER SIGN IN

U.S.

Oklahoma Legislator Proposes Hoodie Ban

BY DENVER NICKS JANUARY 1, 2015 9:35 AM EST

Oklahoma could join a list of states where it is illegal to wear a hoodie in public, if a state senator's proposed bill goes through.

THE OKLAHOMAN SUBSCRIBE NOW

Former Norman City Councilwoman believes she was intended target of attack

by TIM WILLERT
Published: Sat, July 11, 2020 1:05 AM | Updated: Sat, July 11, 2020 1:21 AM

NORMAN — A woman who reported being raped June 27 said she recognized her attacker's voice when she listened to threatening messages left on the phone of her next-door neighbor, who at the time was a Norman City Council member.

The Oklahoma Bureau of Investigation is looking into the rape at the request of the Norman Police Department. At issue is whether the attack was meant for Alex Scott, a former council member and current Senate candidate.

https://time.com/3651529/oklahoma-hoodie-ban/
https://www.oklahoman.com/article/3937085/cellphone-video-in-fatal-moore-ok-warren-theatre-incident-is-made-public
https://tulsaworld.com/news/local/timeline-the-shooting-of-terence-crutcher/collection_187d7db2-8734-5f27-9e16-446f87b84208.html#3
https://www.oklahoman.com/article/3656072/hearing-reset-for-oklahoma-woman-in-horse-theft-and-animal-cruelty-case
https://www.oklahoman.com/article/5666549/woman-recognizes-attackers-voice-in-threatening-messages

CROWDSTRIKE

Post-Pandemic

back on my [redacted]
@brownbitterbish
Oklahoma County Commissioners are voting to restrict free speech TOMORROW MORNING 8/12 at 9AM. Check the resolution and areas they are restricting here: oklahomacounty.legistar.com/View.ashx?M=F&...
They are attempting to prevent the protests at the courthouse and Jail, particularly at the courthouse.
12:25 PM · Aug 11, 2020 · Twitter for Android

back on my [redacted]
@brownbitterbish
320 Robert S. Kerr
OKC, OK 73102

Blumert 405.713.1501
Carrie.Blumert@oklahomacounty.org

Maughan: 405.713.1502
Brian@oklahomacounty.org

Calvey: 405.713.1503
Kevin.Calvey@oklahomacounty.org
12:58 PM · Aug 11, 2020 · Twitter for And

back on my [redacted]
@brownbitterbish
Contact the ok county comm
relentless. There is no item
comment. If there is no pub
shouldn't be a vote. Raise h
@OkCountyMaughan @kev

back on my [redacted] @brownbitterbi
Oklahoma County Commissioners are vot
MORNING 8/12 at 9AM. Check the resolu
oklahomacounty.legistar.com/View.ashx?
They are attempting to prevent the prote
at the courthouse.

12:51 PM · Aug 11, 2020 · Twitter for Android

3

SATURDAY AT 10 AM – 1 PM
DRIVE FOR 45 ROLLING RALLY – TULSA
TCC Southeast

About Discu

Details
136 people
Saturday at
52–73°F Thun
TCC Southe
Public · Hos

Get your motor
gather to show
When
October 3rd · Sa
Instructions
Starting around
route from the m
campus at 61st a
drive route.
The attached ma
merge points.
You may choose

Kristi Cloud
November 18 at 10:28 PM ·
PLEASE PLEASE BRING EVERYONE YOU KNOW WHO SUPPORTS AND REMEMBER GIVE THEM CREDITS AND RELEASE THOSE TRYING TO DO THE NEXT RIGHT THING!!

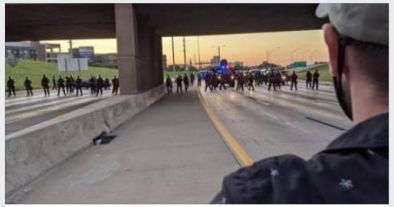
KILLING OKLAH
being ignored, ne
ALTHY MEALS F
TE FREE VIDEO
HOUT THE HOLI
STITT & O.D.O.C. RELEASE
es to save lives, Oklahoma
lp and Stand With - Power In
Martin Luther King Ave. Okc.,

Like · 1d

Riskline
@Riskline
UNITED STATES OF AMERICA: Protest against COVID-19 restrictions planned in Oklahoma City on 23 November | riskline.com
5:20 PM · Nov 19, 2020 · Riskline Updates

facebook Sign Up

Events
Events



AUG 29 March the Mural (OKC)
Public · Hosted by Informed-Voter.com

SATURDAY AT 5 PM – 7 PM
#TrumpPenceOutNow
Brookside Diner

About Discussion

Show Map

and Shartel

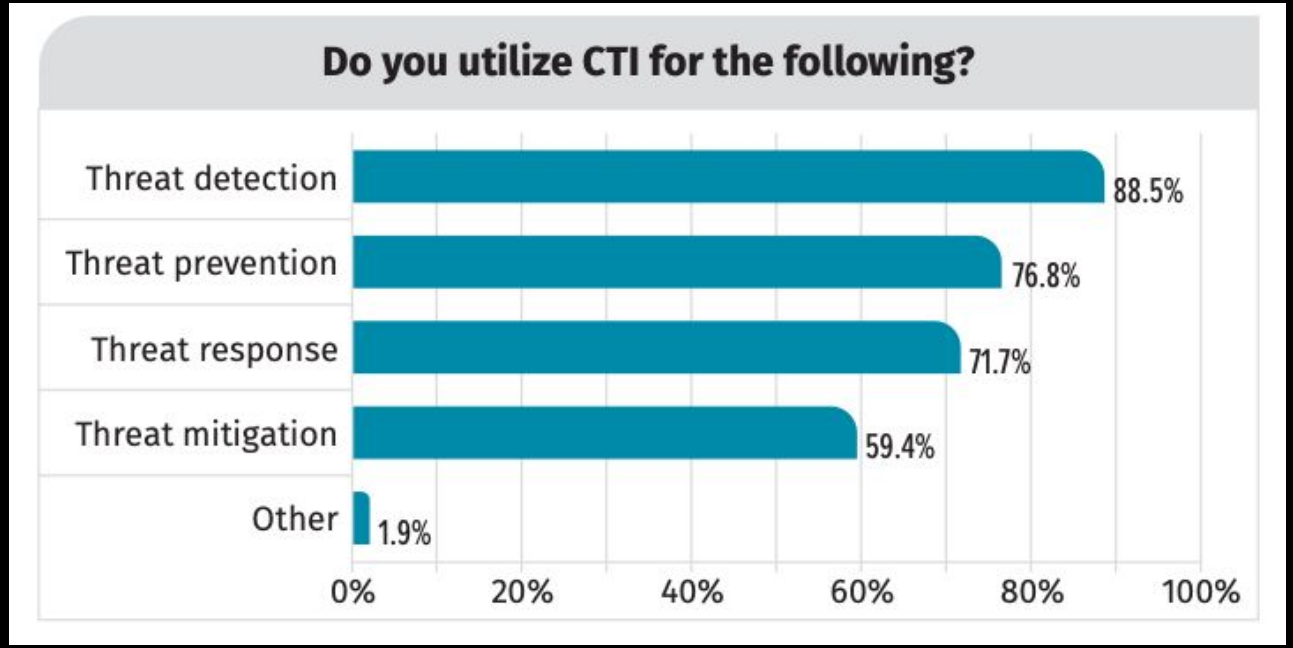
Host
Peaceful Rally - Tulsa
Nonprofit Organization

Midnight Rider ★★★ @Qanon76 · 1h
If you're going to Washington D.C. to be a part of history on January 6th, comment below and share what state you'll be representing.
Together We Win!!!
#YouMeWE

Peaced Off Patriot
@QonTwo
Replying to @Qanon76
Oklahoma will be there in force
2:33 PM · Dec 29, 2020 · Twitter for Android

CROWDSTRIKE

What is CTI Used For?



https://www.sans.org/reading-room/whitepapers/analyst/2020-cyber-threat-intelligence-cti-survey-39395

CROWDSTRIKE

What was “Other” in OK?

- Election Security
- Fraud
  - Unemployment Insurance
- Public Health/Safety
- OK-ISAC
  - Private Sector
  - State Agencies
  - Other States
  - K-12
  - Higher Ed
  - Municipalities
  - OK Information Fusion Center
  - Federal Agencies

CROWDSTRIKE

What Could “Other” Be?

- More Fraud:
  - Temporary Assistance for Needy Families (TANF)
  - Supplemental Nutrition Assistance Program (SNAP)
  - Special Supplemental Nutrition Program for Women, Infants and Children (WIC)
  - Workers Compensation
- Sentiment
- Counterintelligence
- Counterterrorism

CROWDSTRIKE

Matt.singleton@crowdstrike.com
www.linkedin.com/in/thematttman