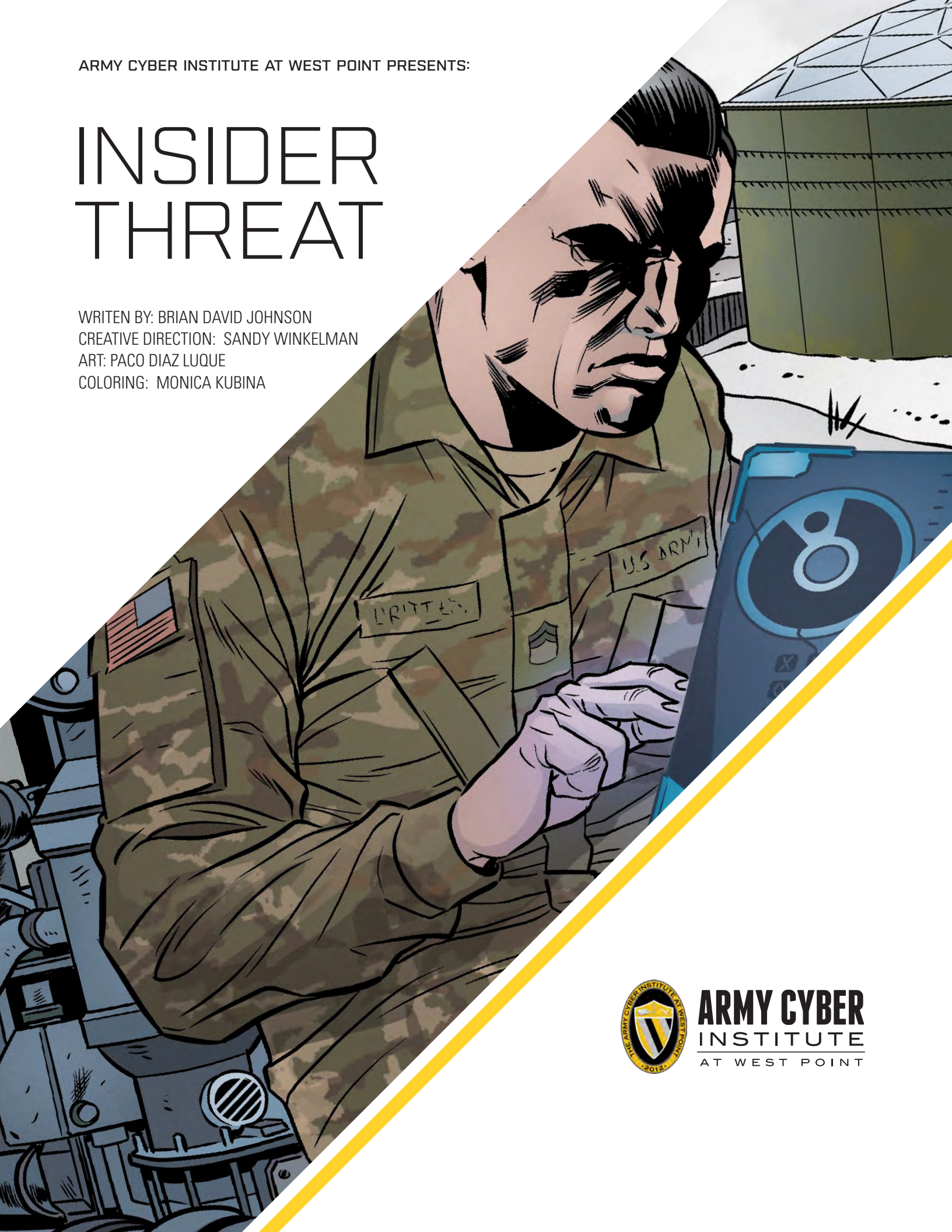
ARMY CYBER INSTITUTE AT WEST POINT PRESENTS:

INSIDER THREAT

WRITEN BY: BRIAN DAVID JOHNSON
CREATIVE DIRECTION: SANDY WINKELMAN
ART: PACO DIAZ LUQUE
COLORING: MONICA KUBINA



ARMY CYBER INSTITUTE AT WEST POINT

BUILDING A BETTER, STRONGER AND MORE SECURE FUTURE FOR OUR ARMED FORCES

Science Fiction Prototypes are science fiction stories based on future trends, technologies, economics, and cultural change. The story you are about to read is based on threatcasting research from the Army Cyber Institute at West Point and Arizona State University's Threatcasting Lab. Our story does not shy away from a dystopian vision of tomorrow. Exploring these dark regions inspires us to build a better, stronger, and more secure future for our Armed Forces.

Lt. Col. Natalie Vanatta
Academy Professor
U.S. Army Cyber Institute

INSIDER THREAT

"First, and foremost, we must recognize that human behavior is not always dictated by societal or cultural norms. Humans react or behave based upon their own individual personalities and life events. Thus, their actions are not generally predictable, and may be "surprising" or "shocking". Yet, while humans are complex and unpredictable, the stresses that they face each day will manifest in observable behaviors that are smaller indicators of potential future actions."

– Brad Millick, Ph.D.
Director, DoD Counter Insider Threat
Office of the Under Secretary of Defense for Intelligence

A concerned serviceman observes his counterpart acting erratically –plotting to cripple or contaminate the entire water system of a U.S. Army base. Suspicious behaviors observed over the course of a year point to a potential insider threat.

Insider threats are so dangerous because they are a betrayal of trust. Foundational to the U.S. military is the trust between service members. Erratic behavior doesn't automatically indicate a possible insider threat, nor should service members spend their days suspicious of their colleagues. In a time when technology has empowered soldiers to be more effective and efficient, these threats are increasingly hazardous. How can we create a culture of awareness and support to catch problems early and disrupt a possible insider threat before it ever exists?


THANKS FOR MEETING ME, LISA...I REALLY JUST NEED SOMEONE TO TALK THIS THROUGH WITH...
NO PROBLEM AT ALL JEFF...WHEN I GOT YOUR MESSAGE I COULD TELL SOMETHING WAS WRONG...WHAT'S UP?
THIS IS GOING TO SOUND CRAZY... BUT I THINK SOMETHING REALLY BAD IS ABOUT TO HAPPEN...I THINK SOMETHING'S UP WITH SSG RITTER.
WHAT DO YOU MEAN? I DON'T KNOW THAT NAME...
I REALLY DIDN'T EITHER... UNTIL ABOUT A YEAR AGO...
I ORIGINALLY MET RITTER AND HIS FAMILY AT MY OLDEST DAUGHTER JUDY'S SOCCER GAMES. NO BIG DEAL JUST USUAL PARENT STUFF... HE WAS ALWAYS FRIENDLY.. OFFERING ME A BEER.
TechCrunch 2022
THEN RITTER'S WIFE STOPPED COMING TO THE GAMES. WHICH WAS STRANGE AND HE STOPPED HELPING OUT THE COACHES... SOMEONE TOLD ME THEY WERE SPLITTING UP..THAT SHE HAD AN AFFAIR...
i void warranties
2:14 AM
MESSAGES
2am & 6 pack of beers again... is this a life?


I'D SEEN SOME ODD POSTS FROM HIM...BUT I DIDN'T REACH OUT OR SAY ANYTHING...YOU KNOW...I DIDN'T THINK IT WAS MY BUSINESS... I WANTED TO GIVE HIM HIS PRIVACY.
HOT CHOCOLATE $9
VIENNA $7
$8
THEN A FEW MONTHS LATER MY SQUAD WAS TRAINING FOR THE BEST RANGER COMPETITION AND WE NEEDED TO HAVE A MEDIC ON THE COURSE WHEN WE TRAINED.
WE DIDN'T TALK MUCH THEN EITHER. HE STILL SEEMED A LITTLE DISTRACTED BUT IF HE WAS GOING THROUGH A DIVORCE THAT'S UNDERSTANDABLE...LAST YEAR WE REALLY WANTED TO WIN SO WE HIT THE COURSE PRETTY HARD AND RITTER WAS THERE ALMOST EVERY TIME...
WELL, NONE OF THAT SOUNDS SO BAD...WHAT'S GOT YOU SO UPSET?
THAT'S JUST IT. DURING ONE PRACTICE I SAW RITTER DOING SOMETHING AND IT STUCK WITH ME...


I WAS TAKING A BREAK AND I DON'T THINK RITTER KNEW I WAS THERE. HE WAS ACTING STRANGE... WALKING BETWEEN THE WATER FOUNTAINS AND THE FIRE HYDRANT.
IT WAS LIKE HE WAS WALKING A PATTERN...
...AND I HAVE TO BE HONEST IT LOOKED KIND OF CRAZY.. LIKE THERE WAS SOMETHING WRONG WITH HIM.
WHEN I CALLED OUT TO HIM THE LOOK ON HIS FACE WAS LIKE HE WAS ON A DIFFERENT PLANET...
...BUT THEN HE SNAPPED BACK AND PRETENDED LIKE EVERY-THING WAS NORMAL.
BUT THAT WAS IT...I KNEW HE WAS PRETENDING. SO I REACHED OUT TO HIS CPT.
NAH... RITTER'S FINE... HE'S DISTRACTED... HE'S UPSET THAT HE DID NOT MAKE THE PROMOTION LIST LAST MONTH...


THEN JUST LAST DECEMBER I WAS DRIVING HOME FROM BASE AND I SAW RITTER BY HIMSELF WALKING THE RESERVOIR. HE WAS WALKING THAT SAME PATTERN WAY... WITH THE SAME LOOK ON HIS FACE.
NOW YESTERDAY I SAW THIS ABOUT THE HACK LAST MONTH ON THE LOCAL WATER AUTHORITY...
I LOOKED INTO IT AND THEY ARE THE CONTROL SYSTEMS THAT CONTROL THE WATER TO THE BASE...
IT CERTAINLY SOUNDS ODD... BUT WHAT ARE YOU THINKING... WHAT'S GOT YOU SO WORRIED?
U.S. ARMY
I'M WORRIED THAT RITTER MIGHT BE PLANNING OUT SOME KIND OF ATTACK ON THE BASE... SOMETHING WITH THE WATER... LIKE HE'S GOING TO DO SOMETHING TO HURT PEOPLE...
THAT'S A PRETTY BIG LEAP JEFF... HAVE YOU TALKED WITH OTHER PEOPLE TO CHECK IF THEY'VE SEEN ANYTHING? ARE YOU OK?
I'M FINE... WELL I'M NOT FINE... IT'S JUST THIS BAD FEELING AND I THINK I NEED TO SAY SOMETHING... TO DO SOMETHING ABOUT IT.

"It is imperative that when indicators of concerning behavior are observed, they be reported to appropriate officials. Informing the appropriate officials of concerning behavior facilitates professional assistance to those under stress and to mitigate any potential threat. It is incumbent on you to help protect our resources, operations, information, personnel, family and friends; use this novel to educate yourself and your team. Bottom line: trust your instincts and report questionable behavior."

– Brad Millick, Ph.D.
Director, DoD Counter Insider Threat
Office of the Under Secretary of Defense for Intelligence

AFTERWORD

An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems. Tackling insider threats requires a combination of techniques from the technical, the sociological, and the socio-technical domains. How organizations go about tackling this issue without creating a culture of distrust or suspicion is the crux of the problem.

In this story, behavior was the indicator of a potential insider threat. While these vary depending on the personality and motivation of a potentially malicious insider, there are common patterns that can be observed. Should Lisa have taken Jeff more seriously and launched an immediate investigation? What are some of the indicators in Ritter's behavior that could have been addressed early? If Jeff's interpretations of Ritter's behaviors turn out to be false, how should Lisa approach the situation without creating organizational trust issues?

An integrated effort to deter, understand, detect, and mitigate the risks from insider threats is critical. How should the U.S. military promote the reporting of suspicious activities without promoting an atmosphere of distrust within the organization?

First Edition: 2018