NAVIGATING A SECURITY WASTELAND

Cloud Security

Volume 3

August 2018

CYBRARY

ThreatConnect™

CYBRARY

Adam Vincent, CEO & Co-Founder of ThreatConnect, takes a deep dive with Cybrary to discuss how “Managing your enterprise security organization like a small business” is pivotal when it comes to application and cloud security.

WHAT CHALLENGES DO YOU SEE COMPANIES FACING IN TRYING TO SECURE THEIR DATA?

What does “their” even mean anymore? Look at things like GDPR with data processors and data controllers. It is not simple to know what data requires security and at what level these days - questions like where it came from, who sees it, and what they can do with it are all questions that are difficult for companies to answer.

Recently I wrote a blog post on the topic which goes into depth on exactly what data ThreatConnect gets from our customers, what we do with it, and conveys the importance of our protecting it. With that said, it’s not just about the confusion and proliferation of data, the problem is bigger - security is dealing with an exponential increase in all things digital.

More sensors, more devices, more cloud computing, more automation, more complexity, more reliance. With more of everything, no wonder we are feeling the pressure of more risk.

DO THEY HAVE A HOLISTIC STRATEGY?

Understanding what is happening is definitely a top goal, but next is deciding what to do about it.

In order to protect their data, companies must first understand what threats they are up against, the effectiveness of their existing security controls - people and technologies against those controls, and ultimately what risk they are willing to accept. Most companies have pieces of this, but not all, and definitely do not have a holistic risk-based approach for how they are building and managing their security program.

In order to understand risk, the security organization must connect with stakeholders in the business and find ways to communicate about risk.

DO THEY HAVE THE ABILITY TO MANAGE SECURITY EFFECTIVELY?

Holistic understanding is difficult to do across all aspects of the security program immediately, especially with a lack of process and process measurement. Instead, you must

ThreatConnect™

start by looking at just a single part of the strategy. The people, technologies, process must be brought together based on the goals and strategy. Next comes automating parts or all of the process and providing a streamlined way for people to participate in the end to end workflows.

Next, is to measure the process against the process' objectives and make improvements. Because security and risk mitigation should always be balanced against value to the business, cost of the specific process vs. risk mitigation should be conveyed frequently to management as part of the discussion on effectiveness.

HOW WOULD YOU RECOMMEND THEY OVERCOME THESE CHALLENGES?

- Develop a strategy for your security organization that connects to the business stakeholders to understand and minimize risk. Socialize your strategy and top priorities to management and clearly state objectives that incorporate a business-focused approach to security and reducing enterprise risk while minimizing expense.

"WITH MORE OF EVERYTHING, NO WONDER WE ARE FEELING THE PRESSURE OF MORE RISK."

ADAM VINCENT

CEO & CO-FOUNDER, THREATCONNECT

ADAM VINCENT

ThreatConnect™

CEO & CO-FOUNDER, THREATCONNECT

Adam is an information security expert and is currently the CEO and a founder at ThreatConnect, Inc. He possesses over a decade of experience in programming, network security, penetration testing, cryptography design & cryptanalysis, identity and access control, and a detailed expertise in information security. The culmination of this knowledge has led to the company's creation of ThreatConnect, the first-of-its-kind threat intelligence platform. He currently serves as an advisor to multiple security-focused organizations and has provided consultation to numerous businesses ranging from start-ups to governments, Fortune 500 organizations, and top financial institutions. Adam holds an MS in computer science with graduate certifications in computer security and information assurance from George Washington University. Vincent lives in Arlington, VA with his wife, four children, and dog.

- Look at one of the objectives of your overall strategy: Increase effectiveness of phishing email analysis by 50%. Architect your people, process, and technologies for the process. Leverage a security platform like ThreatConnect to put analytics, orchestration, and workflow around the end to end process.
- Determine what parts of the process must be manual and what can be automated. Ensure that stakeholders have provided feedback on the overall workflow that they have been doing prior to technically enabling the process, so that the new approach is better than what they were previously doing.
- Create metrics for time and cost across all major parts of the process. These metrics will be used later to measure the efficacy of the overall process and deliver insights to various stakeholders on the process' effectiveness.
- Build a simple dashboard that measures the most basic metrics of the process and make it available for all to see that have a part in that process. Share the heck out of the dashboard and your results. Highlight the value of the process as number of emails that have been detected as phishing, what parts of the organization were the threat targets, the time on average it takes to process a phish email, and the current cost of the process. You could also get advanced here and talk about the business and possible risk mitigation, but this is an advanced move and would recommend that you not go there until the basics are accomplished.
- Rinse and repeat for other processes.
- Now you can start to think about taking the processes you have made measurable and creating strategic views for them. So for example, you might have a single dashboard for your CISO that shows the phishing process, incident response process, and vulnerability process side by side with some quantitative measurement that takes efficiencies and risk mitigated from each process and sums it for an enterprise view.
- Doing the right thing is #1 - protect the data as if it is yours. Be transparent - here is our blog post on data and analytics.

"DOING THE RIGHT THING IS #1-PROTECT THE DATA AS IF IT IS YOURS. BE TRANSPARENT."

- Policies and Governance are going to be critical to provide protections against abuse.

DO THEY SEEM TO HAVE THE RESOURCES NECESSARY TO PROTECT THEMSELVES AGAINST CYBER ATTACKS?

Most organizations are ill-prepared to stop an advanced cyber attack. Even large, well resourced organizations have a challenge in that they have lots of silos of excellence, covering a lot of different attack surfaces, and too many products. Meanwhile, the threat is highly focused, motivated, and can move quickly and assuredly towards the weakest link in the security program, which allows it to come in via the seams between people, process, and technology.

IF NOT, WHY DON'T THEY HAVE THOSE RESOURCES? WHAT SEEMS TO BE THE CHALLENGE THERE?

As stated before, resources isn't even the right first step, it's having a strategy and building a measurable and improvement focused security organization. Because security organizations have been operating for a long time without many aspects of a "business offering" for securing their organization, they have a long way to go before even knowing what their biggest resource needs are and how they would map to enterprise risk and risk mitigation. This goes back to the age old problem of security professionals being overly enamored with "the problem" and their lack of business skills to approach management with clearly defined business goals. What we need to do is start with the business goal and work backwards.

HOW CAN PROFESSIONALS GET INVOLVED IN YOUR FIELD AND WHAT TYPE OF BACKGROUND DO YOU RECOMMEND THEY ESTABLISH IN ORDER TO LAUNCH A CAREER IN CYBER SECURITY?

If things continue to go in the direction they are heading with the digital revolution, we

need the equivalent of the cyber security Sales & Marketing industry for security. If you think about sales and marketing, they are the lifeblood of the company. They are responsible for the face of the company, and are involved in all aspects of the company's efforts to sell their services or products, and in keeping customers happy longer term. Now think about the size of sales and marketing teams at most companies, the value they create, and the understood ROI of what they produce. There is a direct correlation to sales and marketing and the company's overall value. As cyber risk continues to grow, so does the need for more resources - people, technologies, processes.

I make the analogy to sales and marketing because at the end of the day I want organizations to think the same way about risk to their revenue generation as they do about revenue generation itself. People, technologies, process must be brought together based on the goals and strategy. Then comes automating parts or all of the process and providing a streamlined way for people to participate in the end to end workflows. Next is to measure the process against the process' objectives and improve. Because security and risk mitigation should always be balanced against value to the business, cost of the specific process vs. risk mitigated should be conveyed frequently to management as part of the discussion on effectiveness.

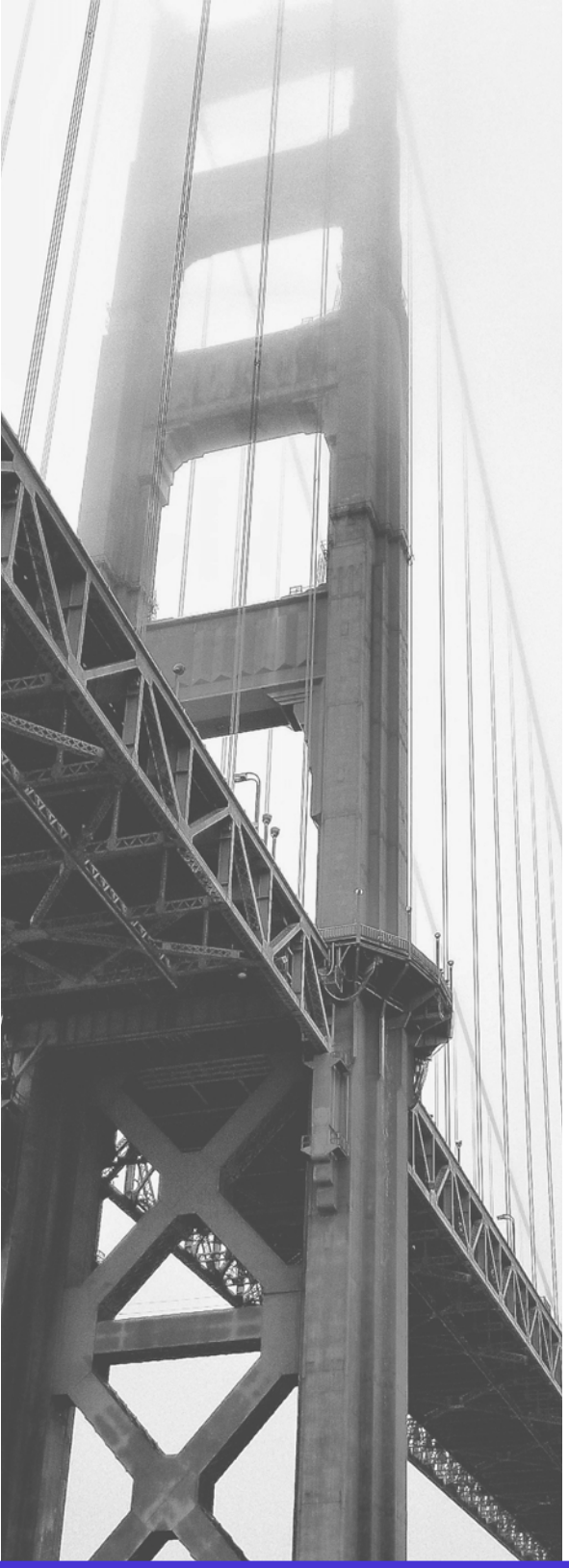
WHAT ARE THE TOP FIVE MOST IMPORTANT COURSES/ASSESSMENTS NEW HIRES NEED TO BREAK INTO THE FIELD?

- Certifications and required experience are another issue affecting the cyber workforce. According to employment data analytics company BurningGlass' Cybersecurity Jobs, 2015 report, CISSP certification is what many companies use to set the bar for their cyber workforce. In 2014, there were nearly 50,000 postings which required a CISSP. Interestingly, they say that this is three-quarters of all the people who hold that certification in the United States, and presume that most of them already have jobs. There is also a requirement for 5 years of work experience to receive your CISSP. Although this data is about 2 years old, I would imagine that this is still the case. Burning glass also states, "The fastest increases in demand for cybersecurity workers are in industries managing increasing volumes of consumer data such as Finance (+137% over the last five years), Health Care (+121%), and Retail Trade (+89%)." And further, "Some 84% of cybersecurity postings specify at least a bachelor's degree, and 83% require at least three years of experience. Because of the high education and experience requirements for these roles, skills gaps cannot easily be resolved through short-term solutions. Employers and training providers must work together to cultivate a talent pipeline for these critical roles."

- I'm a supporter of CISSP and other similar certifications, but do not feel that they are the end-all be-all, or should be critical for the hiring of all security staff members. Instead, I think there needs to be more willingness to hire/train what I call the cyber security "blue collar" workforce that works for people that have CISSP's, years of experience, and college degrees.

"AS CYBER RISK CONTINUES TO GROW, SO DOES THE NEED FOR MORE RESOURCES - PEOPLE, TECHNOLOGIES, PROCESSES."

ADAM VINCENT, CEO & CO-FOUNDER ThreatConnect



- Hiring someone with a CISSP to cover down on those email phishes that are being evaluated with a simple process of looking at the header, doing some enrichment, reading, and follow up on content from the body, and analyzing any attachments via an AMA is not a process requiring a CISSP. Technical enablement of the process also allows the process and guidance for the person to change dynamically. Think about a Verizon call center - as new phones are added, as trends are discovered, as things change, so do the scripts the people that answer the phones follow. This allows people to be used dynamically and to keep the need to hire highly skilled and educated labor to a minimum.

HOW DID YOU GET STARTED IN YOUR FIELD AND WHAT HAVE YOU FOUND TO BE HELPFUL FACTORS IN YOUR OWN SUCCESS?

- I have always had an affinity for computers and the possibilities that computing brings to all things.
- I started my career as a IT administrator for a small company while in high school. It was a great opportunity to learn a lot of basics. I upgraded computers, troubleshooted device and networking issues, and helped manage enterprise business systems.
- I then went to college for computer science and worked at a local juice company doing the same type of work that I did in High School. Here I learned about control systems and how computers loaded with sticky juice remnants had the awesome power to control machinery on a factory floor. I had two realizations here 1.) the connection was made between computers and the physical world and 2.) old rancid juice is very disgusting.
- I became really interested in the idea that everything in the juice company was controlled by a computer and I wasn't confident that there

wasn't a way to manipulate those computers in a malicious way. This wasn't my job, and I was just an intern, so no way to bring it up, but it got me thinking.

- I started setting up firewalls in my dorm room where I was learning everything I could about how they worked.
- I met a guy one day when I was an RA and he was moving his daughter into the dorm. He worked at MITRE and said he did security stuff. I told him about my firewalls and he told me to keep in touch.
- ….The rest is history

WHERE DO YOU SEE THE FUTURE OF WEB APPLICATION/CLOUD SECURITY GOING IN THE NEXT YEAR? IN THE NEXT FIVE?

The reality of web apps and cloud has been here for awhile. The realization that we are now relying on it seems to be just occurring. In the next year, more organizations are going to stop what they are doing outside of their own controlled IT and investigate the risk that they are exposing to their organizations by using these external services.

Then they will likely go back to using them, because the business value will outweigh the risk and the risk will be minimized through trust of the service providers. In the next 5 years, we will see much more rigor placed around how we "create trust" of these services and determine whether they are actually worthy of that trust. There will be more issues with them along the way which will scare people, but ultimately, I think that people will have a hard time moving away from them.

"IN THE NEXT YEAR, MORE ORGANIZATIONS ARE GOING TO STOP WHAT THEY ARE DOING OUTSIDE OF THEIR OWN CONTROLLED I.T. AND INVESTIGATE THE RISK."

ADAM VINCENT

CEO & CO-FOUNDER, THREATCONNECT

ThreatConnect™

KATHIE MILEY

COO, CYBRARY

Kathie has 25 years of experience in the information technology and security field and is currently serving as the Chief Operating Officer of Cybrary. Kathie has held a variety of leadership roles in the information security and cyber industry including positions at Invincea, RiskAnalytics, Predictive Systems, Verizon Enterprise Solutions (MCI, NetSec, CyberTrust and Terremark divisions). Kathie's expertise includes Enterprise Governance Risk and Compliance, Security Policy Assessment and Development, Global Managed Security, Physical Security and Advisory, Cyber Threat and Intelligence, Vulnerability and Patch Management, Identity and Access Management, Security and Network Architecture, and IT Security Training and Enablement. Kathie previously served as a board member of the ISSA-DC Chapter and is a member of industry security organizations including ISACA, ISSA, HIMSS, and others. Kathie currently maintains her CSX and held certifications for HIPAA Security Expert (CHSE) and Certified HIPAA Privacy Expert (CHPE).

CYBRARY

CYBRARY

Kathie Miley, COO of Cybrary, discusses the challenges she sees for Cybrary users and gives recommendations to combat these challenges when it comes to cloud security and protecting your data.

WHAT CHALLENGES DO YOU SEE CYBRARY USERS FACING IN TRYING TO SECURE THEIR DATA?

Application, infrastructure attacks, and insider threats- which come in all shapes and sizes - are on a dramatic increase. Phishing, malware, ransomware, misuse, social engineering - and the list goes on. Distributed Denial of Service (DDoS) attacks certainly represent one of the biggest threats to businesses. Voluminous bandwidth saturation, and under the radar application attacks are the predominant ones we hear about in the news. These attacks can happen whether managed internally or by a cloud provider. Throw in IoT, and attackers have endless vulnerabilities to exploit. Basically, these attacks can cause disruption in vital services, or a complete shutdown.

HOW DO YOU RECOMMEND THEY OVERCOME THESE CHALLENGES?

Make sure your program includes a detection, protection and prevention methodology. Building a wall - aka perimeter security - isn't enough. User behavior, third parties, network traffic, secure coding, logging, and eradication of adversaries need to be monitored and managed, which all play into a layered approach. Policies and procedures also need to be implemented to ensure the program is operating as planned.

Ultimately, security can't be done by a single person, department, or company. Even if your employees practice security "perfectly", your program can't be successful alone. There are still needs for third-party support - like in the event of a DDoS. As they say, it takes a village.

ThreatConnect™

DO THEY SEEM TO HAVE THE RESOURCES NECESSARY TO PROTECT THEMSELVES AGAINST CYBER ATTACKS?

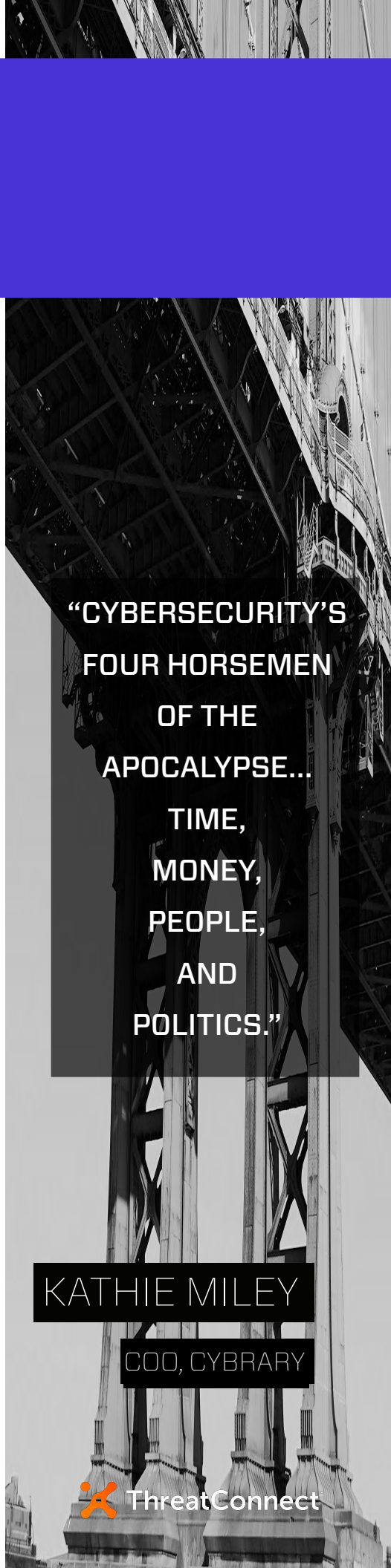
Most companies do not have the resources. As mentioned previously, a combination of internal resources and third-party providers are necessary. Further, with the myriad of attack vectors, there aren't enough resources in any company to completely protect against cyber attacks. A successful cyber attack really isn't a matter of if or when, it has already happened - Some just don't know it yet. In the end, security is a life raft riddled with holes, and as you find the punctures, you patch them. The goal is to make the best damn life raft you can, and have a plan for patching so you can be ready to plug the holes.

IF NOT, WHY DON'T THEY HAVE THOSE RESOURCES? WHAT SEEMS TO BE THE CHALLENGE THERE?

Cybersecurity's four horsemen of the Apocalypse.....time, money, people and politics.

HOW CAN PROFESSIONALS GET INVOLVED IN YOUR FIELD AND WHAT TYPE OF BACKGROUND DO YOU RECOMMEND THEY ESTABLISH IN ORDER TO LAUNCH A CAREER IN CYBER SECURITY?

People are the most menacing component of the four horsemen. We are facing a shortage of 3m cyber professionals. We have done a disservice to the world by portraying an image of cyber professionals as being in a secret society where only the elite can join. That perhaps may have been the case - but it certainly isn't now. Cybrary was created to address talent shortage, in order to make training available to anyone in the world and to create millions of new cyber professionals. You only need a browser to start.



WHAT ARE THE TOP FIVE MOST IMPORTANT COURSES/ASSESSMENTS NEW HIRES NEED TO BREAK INTO THE FIELD?

High cost of training and/or not knowing where to begin, historically are the barriers to entry into cybersecurity. In our 2018 Declassified Report, we found that security professionals come from all types of backgrounds including IT, marketing, healthcare, and even straight out of high school. But everyone needs continuous learning.

What one needs to know is HOW to get started, and this begins with a career path. Not unlike doctors and lawyers, cyber has dozens of specialities. Cybrary provides comprehensive guides to become an expert in one or more specialized area, such as a SOC Analyst, Pen Tester, and/or InfoSec Engineer for example. Whether you have absolutely no experience, or are looking to advance in your domain - we have a curriculum for you. These include courses, hands on experiential labs, CTF challenges, practice exams, and mentors to personally coach you to success.

HOW DID YOU GET STARTED IN YOUR FIELD AND WHAT HAVE YOU FOUND TO BE HELPFUL FACTORS IN YOUR OWN SUCCESS?

I started as an office manager in an IT Services company, and worked my way up the ladder. I spent 9 yrs in ITS but moved into security the moment I met Chris O'Ferrell while working at Predictive Systems (formerly Global Integrity). Chris was an amazing hacker, an exceptional leader at the company, and he became my first true mentor. I was incredibly eager to learn, and extremely tenacious, so Chris took me under his wing, and invested his personal time to guide me, which launched my career in cyber. Since then I have had two mentors who changed my life and my career - Jay Zimmet (who I met when I was at NetSec/MCI) and David Keasey (who I worked for when I was at Verizon-CyberTrust & Terramark). Without them, I wouldn't be where I am today.

I am often asked this question, specifically as it pertains to being a woman leader in cyber. I have boiled it down to three things - in this order:

1. Positive attitude with a passion to succeed
2. Commitment to learning something new every single day, and most importantly...
3. Having amazing mentors

WHERE DO YOU SEE THE FUTURE OF WEB APPLICATION/CLOUD SECURITY GOING IN THE NEXT YEAR? IN THE NEXT FIVE?

The Software Defined Perimeter (SDP) is a strong architecture for application and cloud security. Using Zero-trust as a foundation, SDP focuses on restricting access to authorized users on a case-by-case basis. The high level overview is ensuring the source and destination connection are validated and then only permitted if access was preauthorized and granted to the user. This model is great because it can even extend to IoT devices. While accomplishing the security objectives, you achieve reduced attack surface and unified security. Cyxtera and OPAQ Networks offer fantastic solutions for enterprise/government and small/medium sized businesses respectively. Cyxtera will be offering SDP as a service.

"EXPERTS ACROSS THE WORLD HAVE AND ARE
THE THREATS WE FACE SHOULD A.I. GO ROUGE
POSSESS SELF LEARNING, WITH THE ABILITY TO

KATHIE MILEY, COO CYBRARY

Further out, as technology advances, AI will become increasingly important. Unfortunately, this pertains to unethical use as well. Experts across the world have and are vigorously warning humanity of the threats we face should AI go rogue or be used with malicious intent. AI possess self learning, with the ability to strategize, and achieve objectives - like "don't let anyone access this application". This will challenge AI and initiate self discovery, furthering dominance. And now we are learning more about Evolutionary algorithms which makes AI progression unimaginable.

HOW DO YOU PROVIDE PROTECTION AGAINST NETWORK THREATS AND VULNERABILITIES IN THE CLOUD?

Using logical access controls, the goal is to restrict access to resources on a need-to-know basis. Employees in the shipping department should not have access to payroll data, so at a high level - employing network segmentation with access controls can help mitigate that risk.

Further, in an infrastructure-as-a-service model the responsibility to secure their data in the cloud resides with the business vs. the cloud provider. Unless there is an explicit agreement between the business and cloud provider, the data will not be covered under guaranteed protections or SLAs, nor will the stability of the application. The cloud provider assumably did not architect and/or write the code for your application(s). As such, they have no ability to attest to the security of the application. However, the cloud provider will provide security protections at the physical and hardware layers (servers, storage, networking, and virtualization). If you want them to manage more, you are looking at Platform-as-a-Service options, or Software-as-a-Service if they are available for your application.

Data exists in use, in transit or at rest. For all states of data, businesses can and should use encryption. Ideally, the keys should be managed by a third-party proxy or kept on a separate server, and have a managed refresh schedule with an offsite backup. And given the importance of access controls, the cloud provider should not have access to the keys.

VIGOROUSLY WARNING HUMANITY OF
OR USED WITH MALICIOUS INTENT. AI
STRATEGIZE."

ThreatConnect Inc.®, the pioneer in threat intelligence platforms, arms organizations with a powerful defense against cyber threats and the confidence to make strategic business decisions. Built on the industry's only extensible security platform, ThreatConnect provides a suite of products designed to meet the threat intelligence aggregation, analysis, automation, and orchestration needs of security teams at any maturity level. More than 1,600 companies and agencies worldwide use the ThreatConnect platform to integrate their security technologies, teams, and processes with relevant threat intelligence resulting in reduced detection and response time for enhanced asset protection.

CONTACT:

ThreatConnect, Inc.
sales@threatconnect.com
www.threatconnect.com
3865 Wilson Blvd.
Suite 550
Arlington, VA 22203

CYBRARY

Cybrary is a crowdsourced cyber security and IT career development platform. Its ecosystem of people, companies, content, and technologies converge to create an ever-growing catalog of online courses and experiential tools that provide IT and cyber security learning opportunities to anyone, anywhere, anytime. Cybrary has received industry recognition since its 2015 founding, often being named as an innovator and pioneer in cyber and IT development. This year Cybrary was listed as #164 on the Cybersecurity Ventures' Top 500 World's Hottest and Most Innovative Companies to watch in 2018.

CONTACT:

Cybrary, Inc.
bizdev@cybrary.it
www.cybrary.it
7833 Walker Drive
Suite 510
Greenbelt, MD 20770