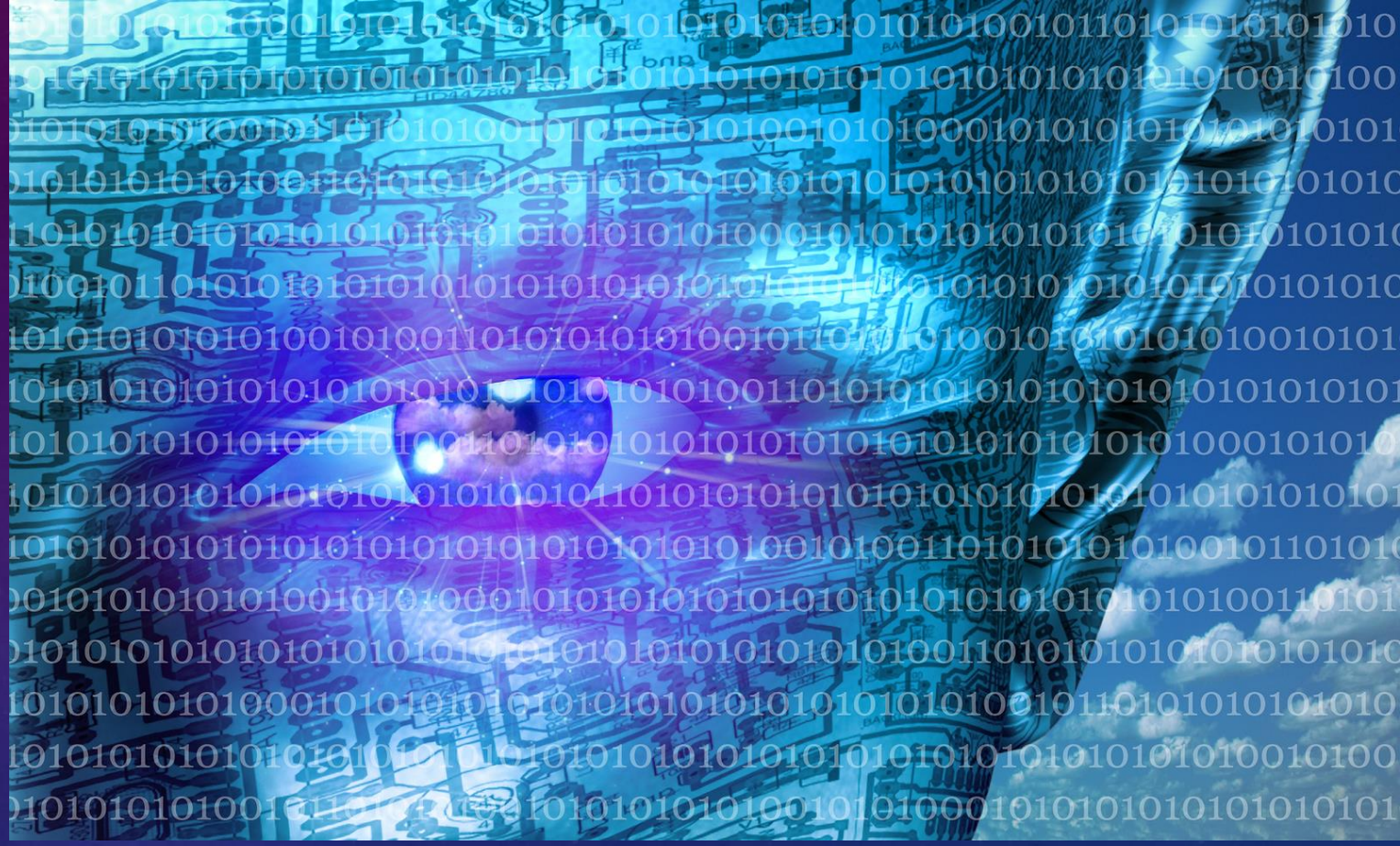


DARKTRACE

DARK TRACE

IST 623 – INFORMATION SECURITY

Yodit Ayalew
Arun Ojha
Ronen Reouveni
Leticia Spencer

PRESENTATION TOPICS

HISTORY OF SECURITY THREATS

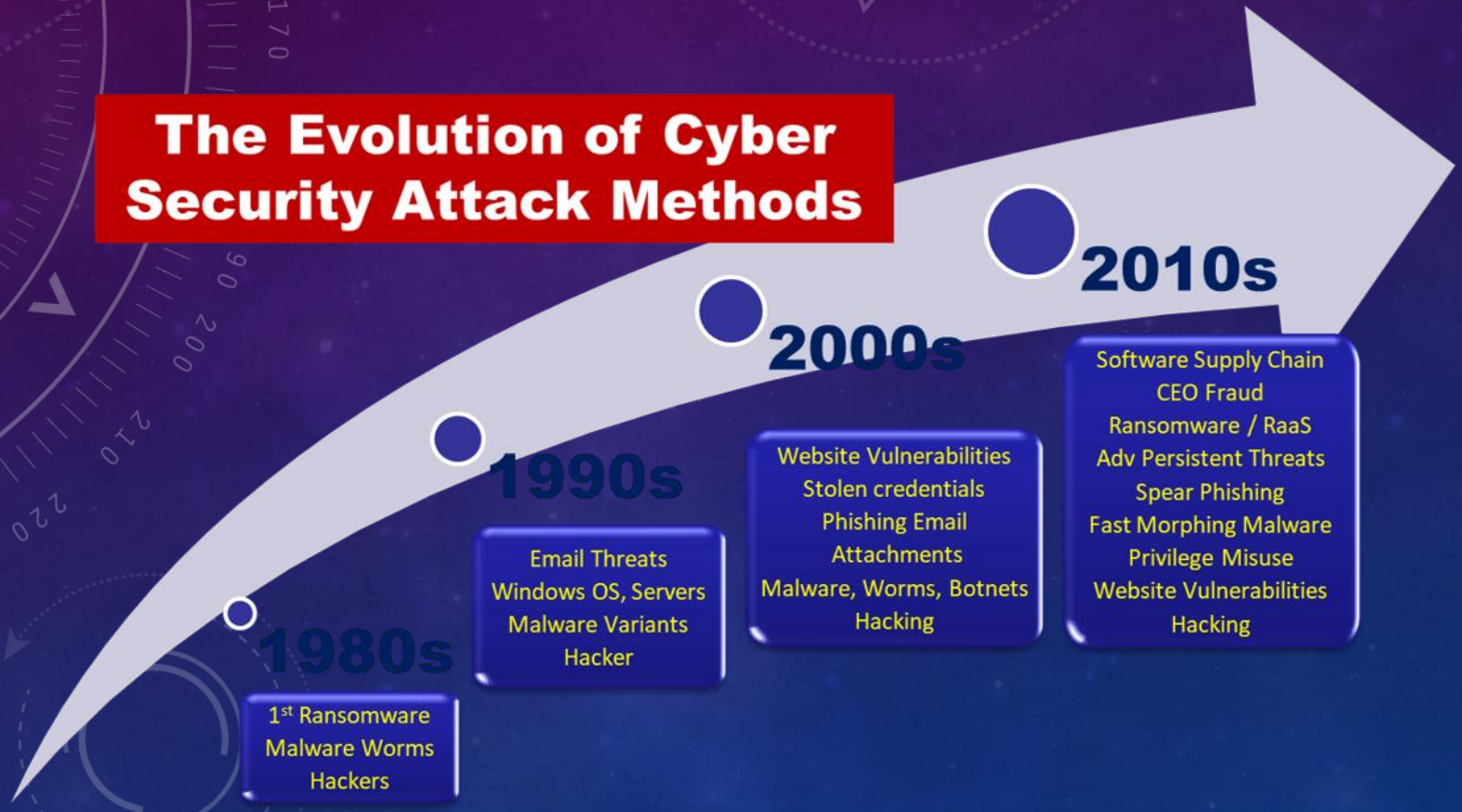
DARK TRACE & SIEM

WHAT KIND OF THREATS DARK TRACE FINDS ?

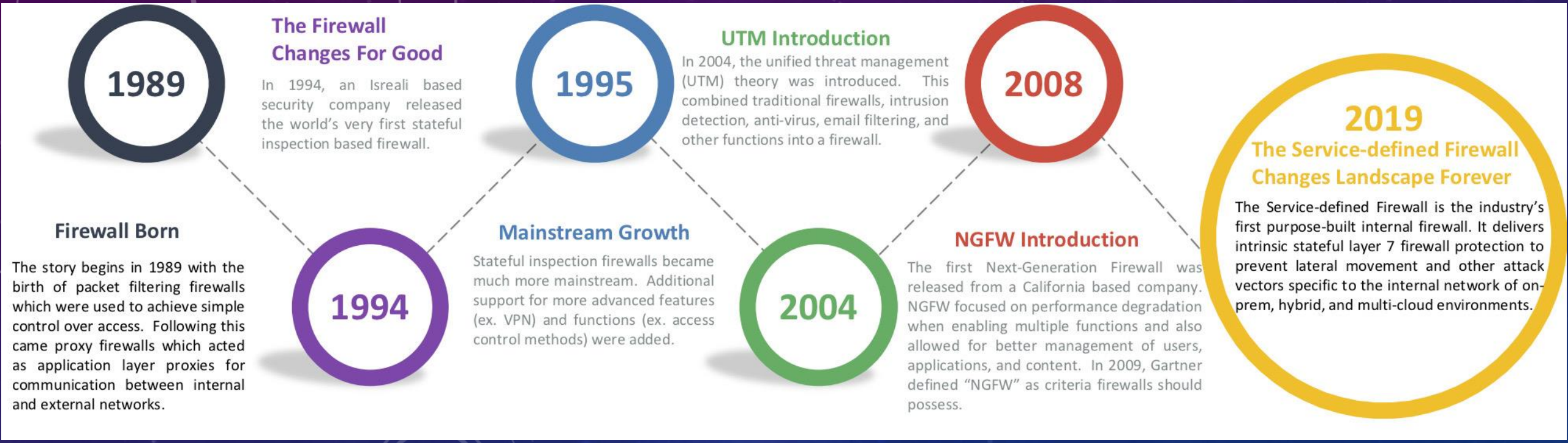
WHO USES IT ? HOW DO THEY DETECT THREAT ?

DOES DARK TRACE METHODS WORK?

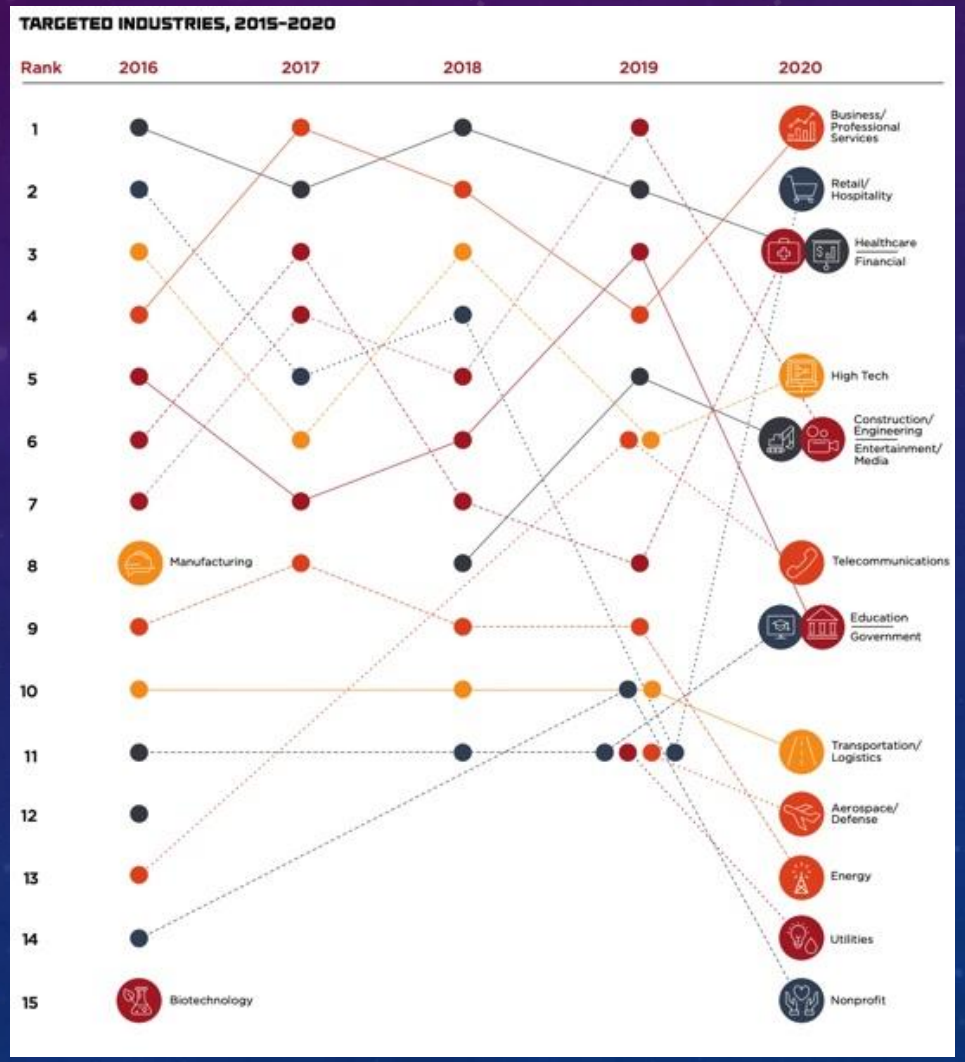
HISTORY OF SECURITY THREATS



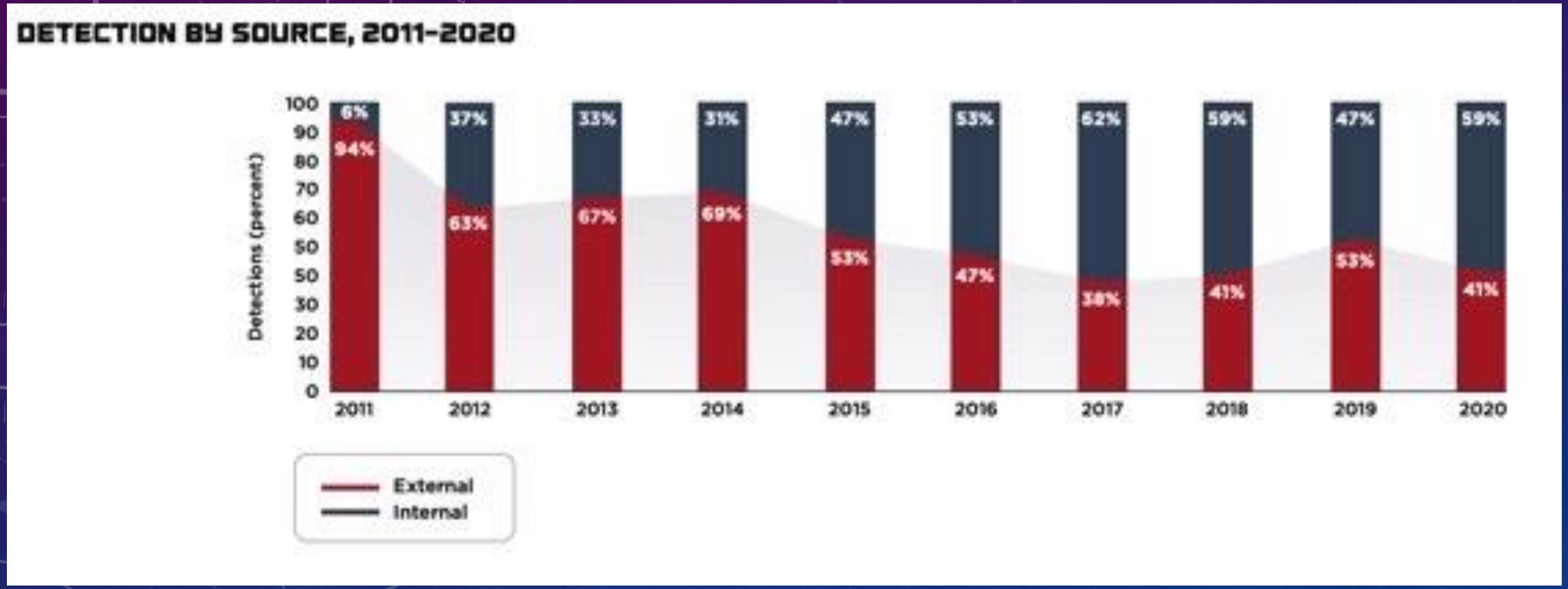
HISTORY OF SECURITY THREATS



M-TRENDS 2021
FIREEYE MANDIANT SERVICES SPECIAL REPORT

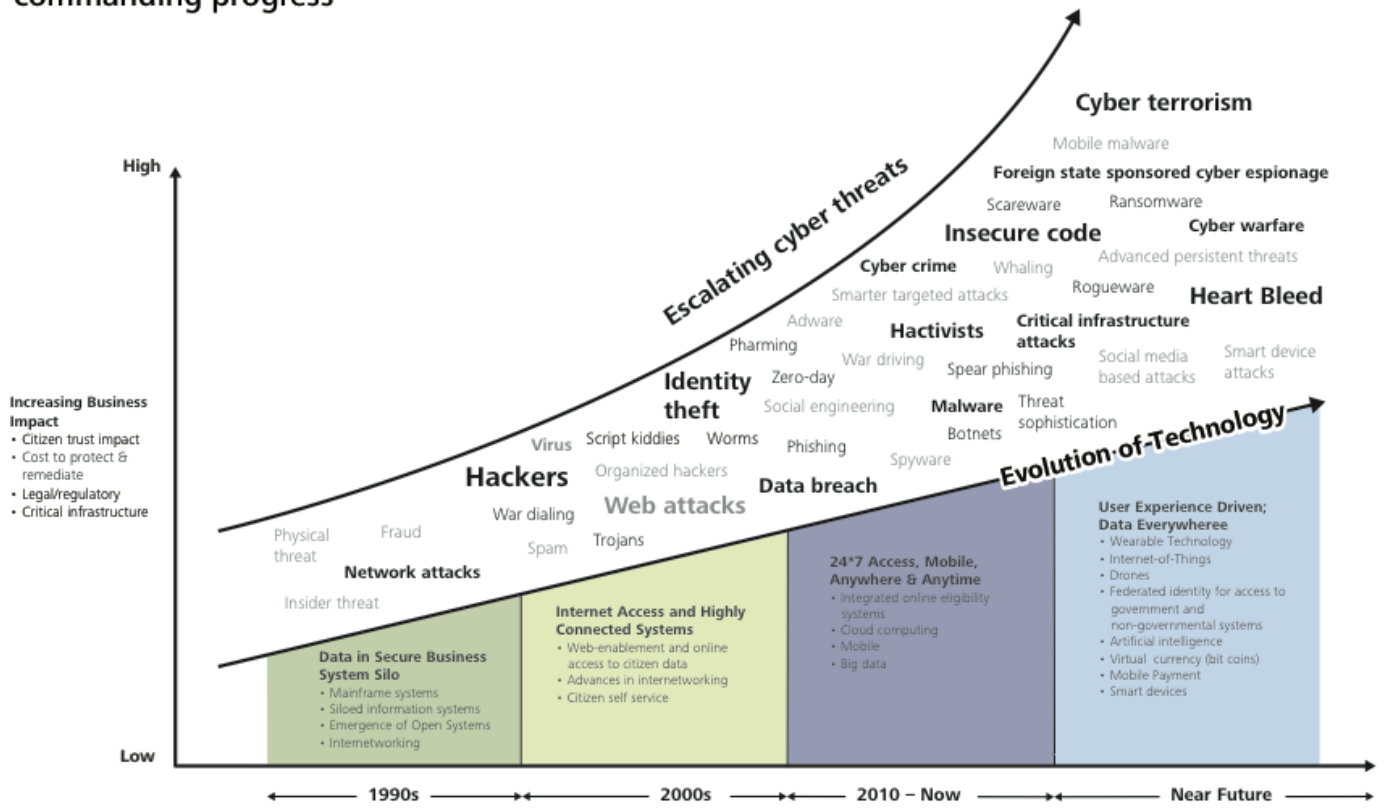


SOURCE DETECTION OF SECURITY THREATS

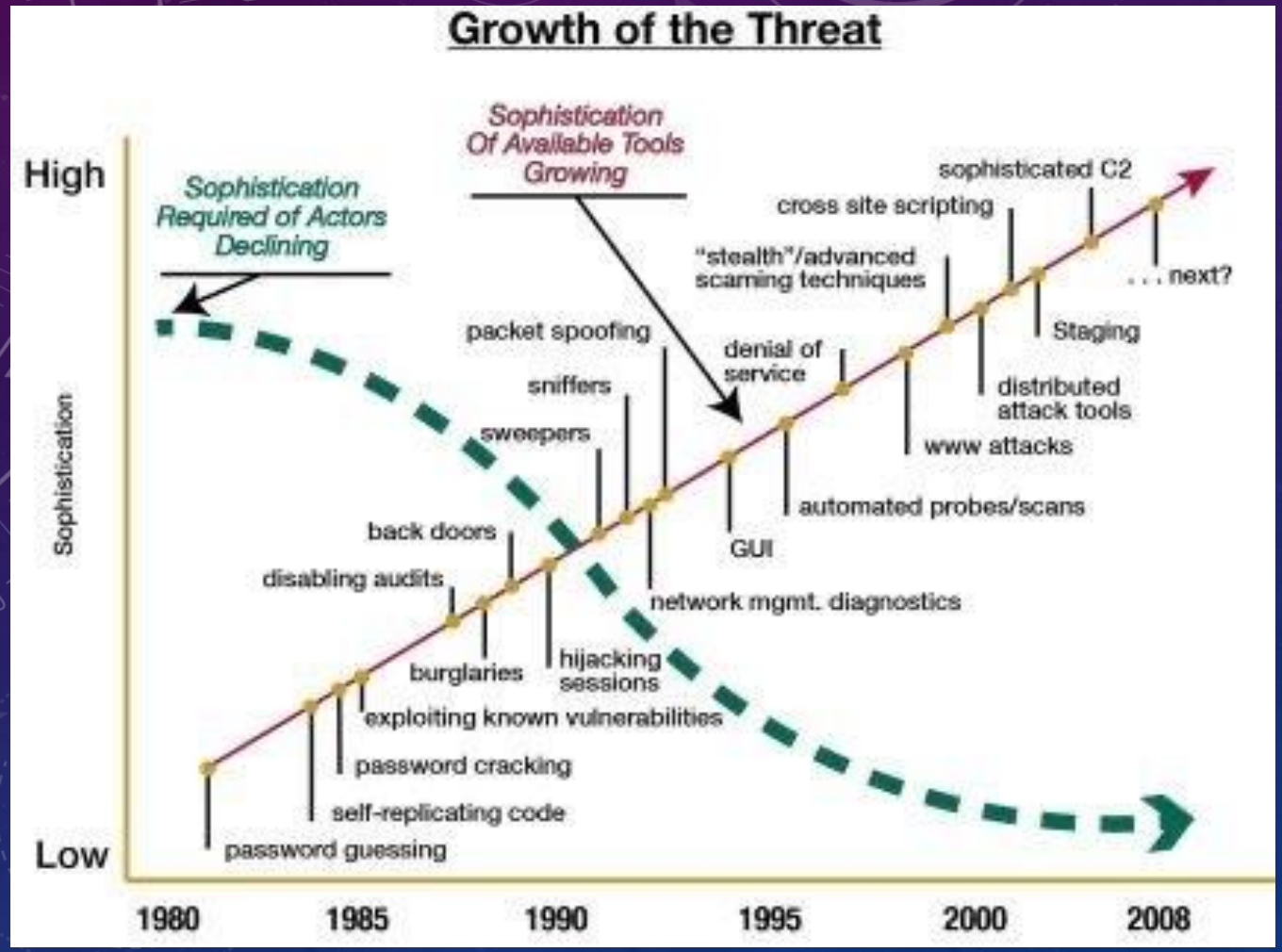


HISTORY OF SECURITY THREATS

Figure 29: Evolving technology and rapidly escalating cyber threats call for a deliberate approach to make commanding progress



HISTORY OF SECURITY THREATS



DARK TRACE & SIEM

Who is Dark Trace ?

- Darktrace was founded in Cambridge in 2013. out of a collaboration of cyber experts from various government intelligence backgrounds and mathematicians who were experts in machine learning

- The company’s product vision is to provide autonomous security (closed-loop solution) that offers autonomous detection, investigation, and response.

- Darktrace’s product portfolio is inspired by the biological immune system. That is effective in anomaly detection and serves as a weapon to discover and combat cyber threats that may have successfully bypassed traditional cybersecurity products.

SIEM & DARK TRACE OVERVIEW

SIEM

SIEM IS A SECURITY SOLUTION THAT HELPS ORGANIZATIONS RECOGNIZE POTENTIAL SECURITY THREATS AND VULNERABILITIES BEFORE THEY HAVE A CHANCE TO DISRUPT BUSINESS OPERATIONS. IT CONTAINS FOLLOWING MAJOR COMPONENTS:

- LOG MANAGEMENT
- EVENT CORRELATION ANALYTICS
- INCIDENT MONITORING AND SECURITY ALERTS
- COMPLIANCE MANAGEMENT AND REPORTING

DARK TRACE

Darktrace pioneered an approach that learns the normal behavior of users, based on unsupervised Machine Learning, and detects outlier activity (like the biological immune system). DARK TRACE offers following services in its portfolio:

- Enterprise Immune System
- Darktrace Antigena
- Cyber AI Analyst

Can DARK TRACE replace SIEM ?

While SIEMs simply aggregate information and may add a rules-based analysis layer, Darktrace Cyber AI continuously analyzes traffic to form a deep understanding of behavior that lets it intelligently detect and respond to even the most subtle anomalies. Because these approaches are so different at their core, the term ‘replace’ is not accurate.

DOES DARK TRACE WORK WITH SIEM ?

- DARKTRACE CAN WORK WITH A SIEM AND ENHANCE ITS VALUE. HOWEVER, ORGANIZATIONS THAT HAVE NOT INVESTED IN A SIEM AND DO NOT NEED TO GATHER LARGE VOLUMES OF HISTORIC LOGS INTO A DATABASE OFTEN FIND THAT DARKTRACE SATISFIES THEIR NEED FOR UNIFIED RISK REDUCTION AND REAL-TIME CYBER DEFENSE
- DARKTRACE IS COMPATIBLE WITH ALL MAJOR SIEMS THAT SUPPORT THE INDUSTRY STANDARD COMMON EVENT FORMAT (CEF) AND LOG EVENT EXTENDED FORMAT (LEEF) INCLUDING SPLUNK, QRADAR, ARCSIGHT, AND LOGRHYTHM.
- DARKTRACE CAN BE CONFIGURED TO FIT INTO SIEM DASHBOARDS, SO ALERTS FROM THREATS DETECTED BY THE DARKTRACE CYBER AI PLATFORM CAN BE SENT TO SECURITY TEAMS VIA THE SIEM

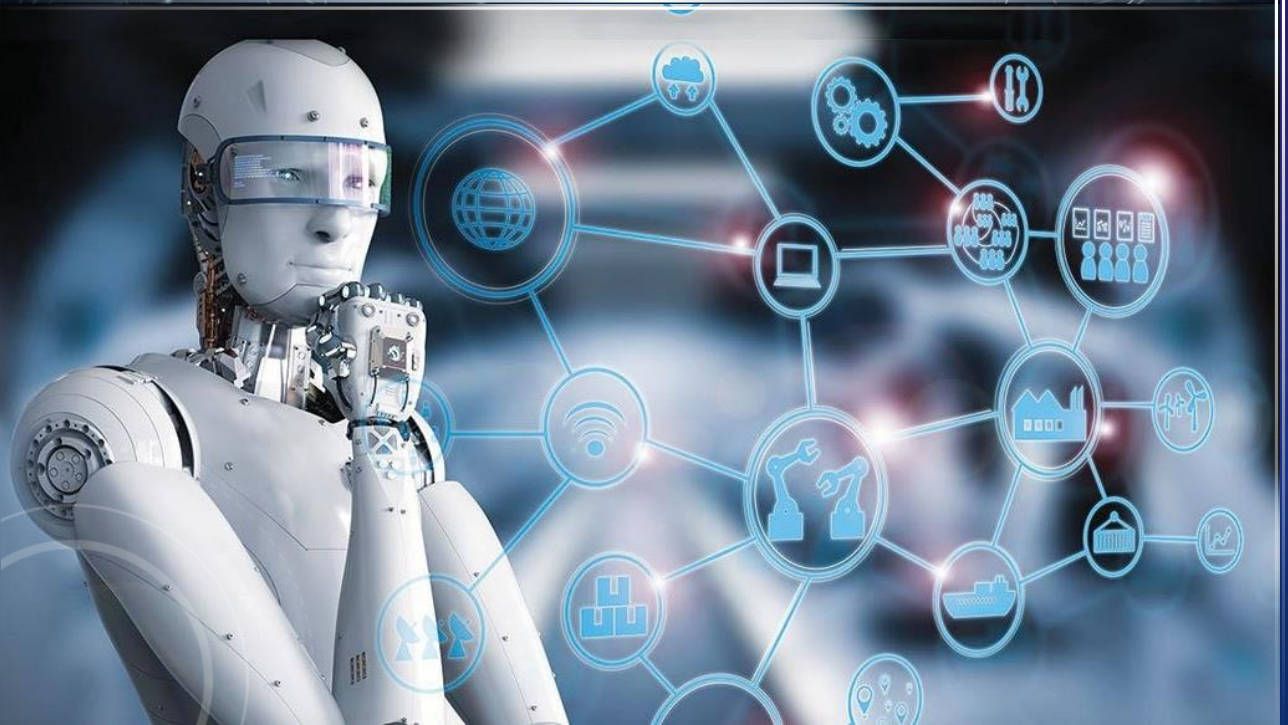
DARK TRACE APPROACH

STAGE 1 : LEARN

THE MACHINE USES AN ALGORITHM TO OBSERVE THE TRAFFIC WITHIN YOUR ENVIRONMENT AND STARTS TO CREATE A PATTERN OF LIFE (I.E., WHAT IS NORMAL BEHAVIOR).

BY LISTENING TO ALL TRAFFIC WITHIN YOUR NETWORK, IOT, OT AND CLOUD ENVIRONMENTS, DARKTRACE CAN CREATE AN ACCURATE PICTURE OF NORMAL. AS MORE TIME PASSES AND MORE DATA IS CONSUMED, THE MACHINE BECOMES MORE EFFECTIVE AND ACCURATE.

DARK TRACE APPROACH

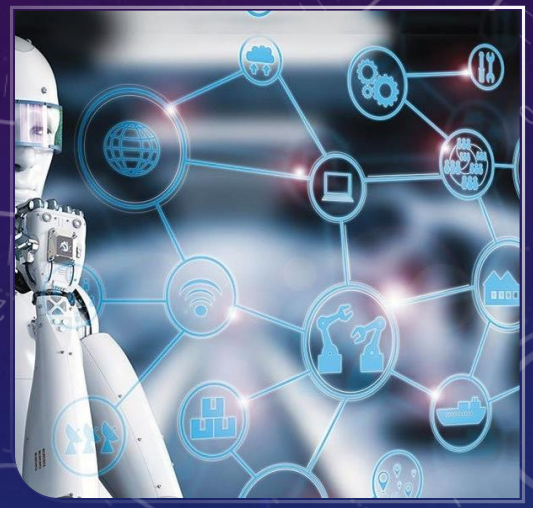


STAGE 2 : DETECT

THROUGH THE CONSUMPTION OF DATA, THE MACHINE BEGINS TO UNDERSTAND CONNECTIONS AT A VERY INTUITIVE LEVEL. BY MODELING THE NORMAL BEHAVIOR OF EACH DEVICE AND USER, DARKTRACE CAN DETECT ABNORMAL BEHAVIOR.

USING A COMPLEX MATHEMATICAL FORMULA, KNOWN AS THE RECURSIVE BAYESIAN MODEL, DARKTRACE CAN ACCURATELY DETERMINE MALICIOUS BEHAVIOR, WITHOUT PRIOR KNOWLEDGE OR SIGNATURE RECOGNITION. THIS MEANS THAT DARKTRACE CAN DETECT ADVANCED ATTACKS LIKE SPEAR PHISHING, RANSOMWARE AND INSIDER THREATS. WITH UNSUPERVISED MACHINE LEARNING, YOU CAN DETECT ABNORMAL PATTERNS WITHOUT RULES AND SIGNATURES.

DARK TRACE APPROACH

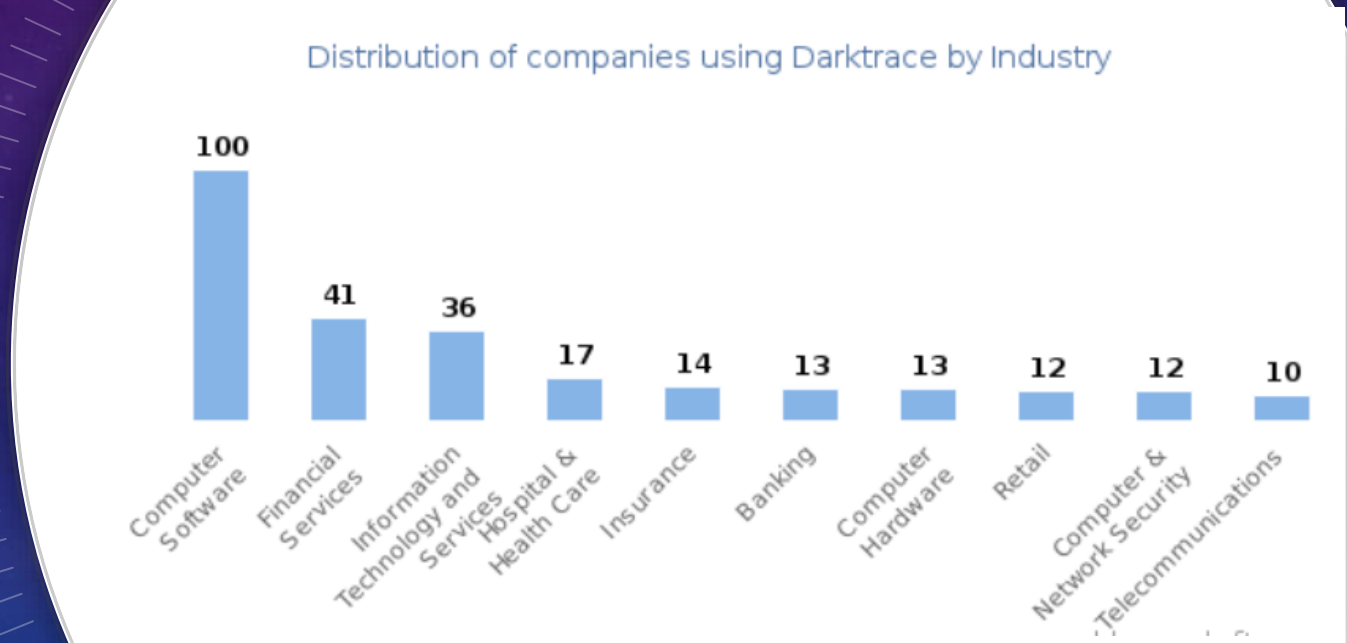


STAGE 3 : RESPOND

ONCE AN ACTIVITY REACHES A CERTAIN THREAT LEVEL, DARKTRACE'S ANTI-GENA SOLUTION CAN AUTONOMOUSLY RESPOND AND CONTAIN THE THREAT BEFORE IT HAS THE DESIRED IMPACT ON THE ORGANIZATION.

WITH SURGICAL PRECISION, ANY ACTIVITY THAT IS PERCEIVED AS HIGHLY MALICIOUS IS CONTAINED AND A MESSAGE IS SENT TO THE SECURITY TEAM TO INVESTIGATE AND RESOLVE.

WHO USES DARKTRACE



WHO USES DARKTRACE

DARKTRACE HAS ABOUT 5,600 CUSTOMERS, BOTH PRIVATE AND GOVERNMENT.

THAT IS UP 42% FROM LAST YEAR. THEY ARE GROWING EXTREMELY FAST.

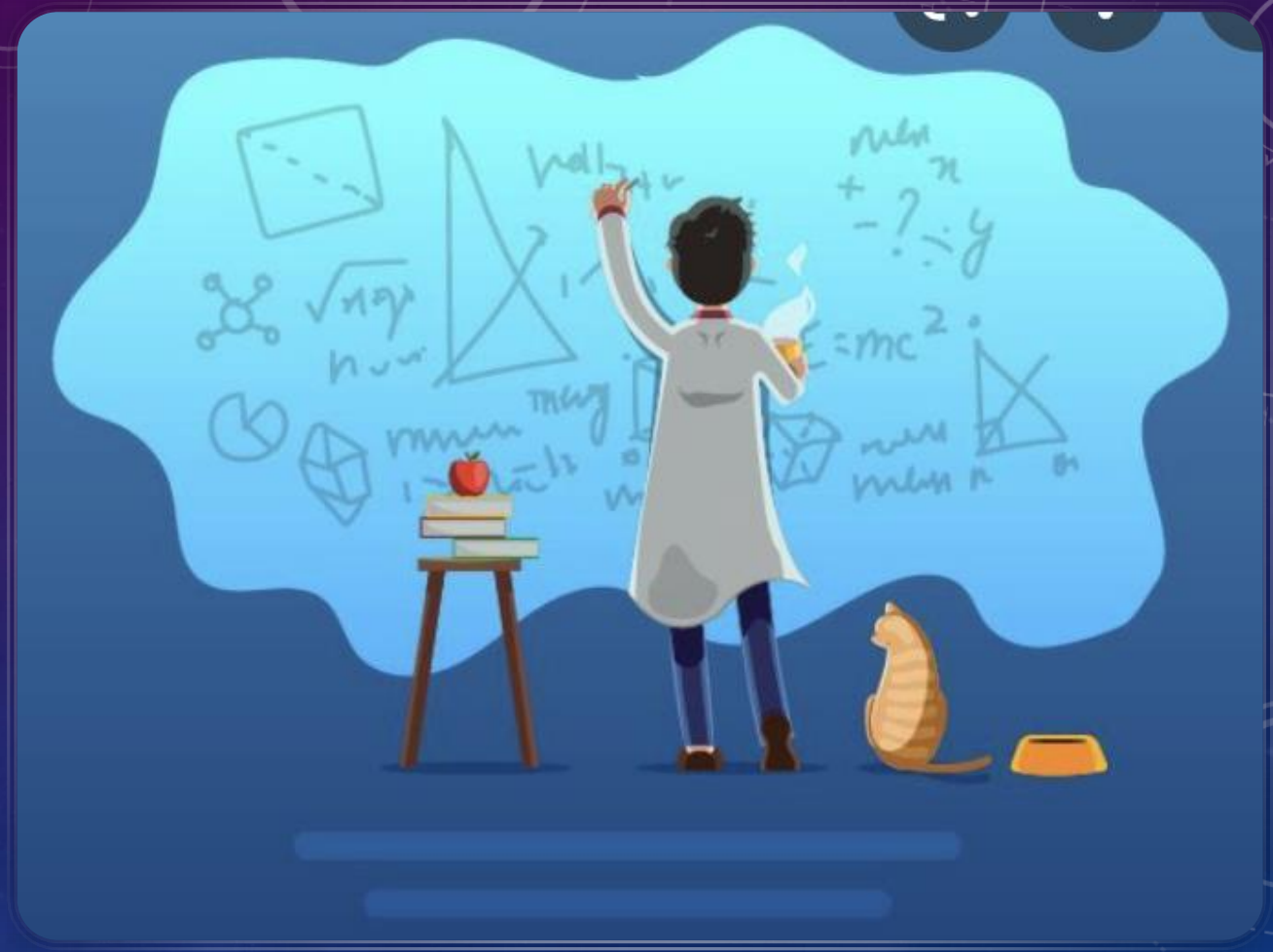
Bandwidth	Description	12 MONTHS
30-day Trial	Free Proof of Value (POV)	$0
Small	Up to 300 Mbps of average bandwidth. 200 Hosts	$30,000
Medium	Up to 2 Gbps average bandwidth. 1000 Hosts	**$60,000**
Large	Up to 5Gbps average bandwidth. 10,000 hosts	$100,000

DARKTRACE AND SOLAR WINDS

- The solar winds breach was one of the largest and most profound in the past few years. Many government arms were breached.

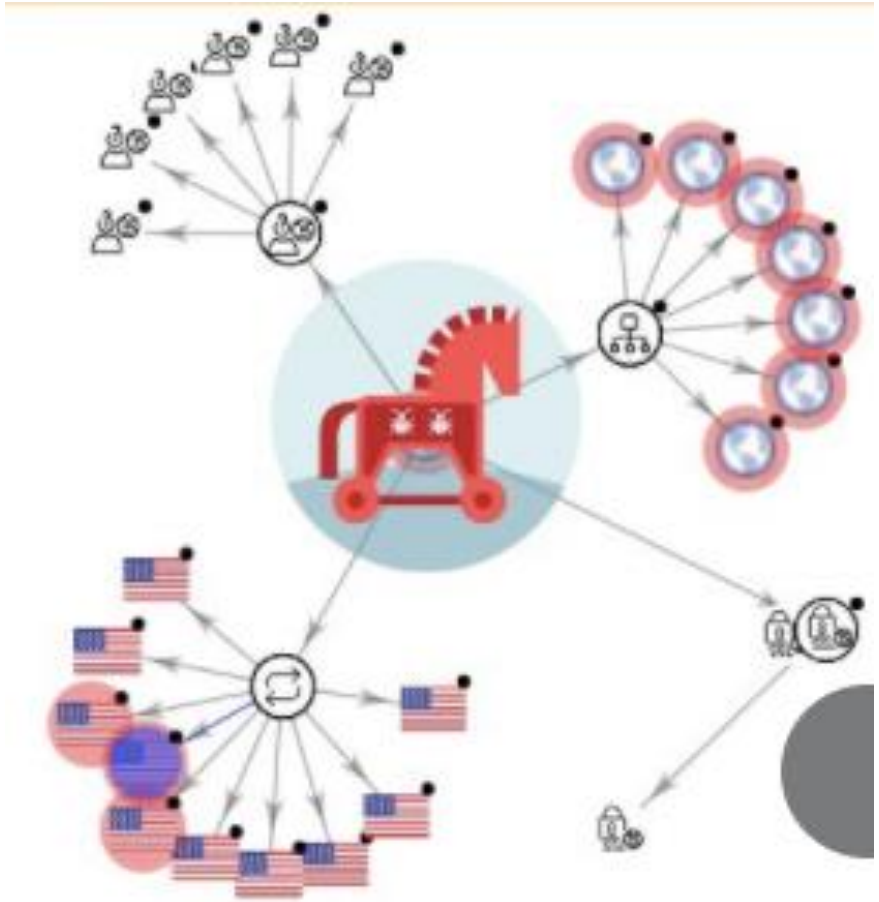
- As discussed above, Darktrace is unique in that it recognizes threats that are new. It does not need to have seen the attack before in order to recognize it, unlike traditional systems.

- A large part of Darktrace marketing is their proof of concepts demonstrations.



SOLAR WINDS CONTINUED

IN THE GOVERNMENT DEMONSTRATION, THE ORION MALWARE WHICH CAUSED THE SOLARWINDS BREACH WAS DETECTED IN REAL TIME. DARKTRACE WAS ABLE TO RECOGNIZE THAT THERE WAS A BREACH. IT THEORETICALLY COULD HAVE STOPPED THE BREACH.



WHERE DOES DARKTRACE EXCEL

Darktrace claims:

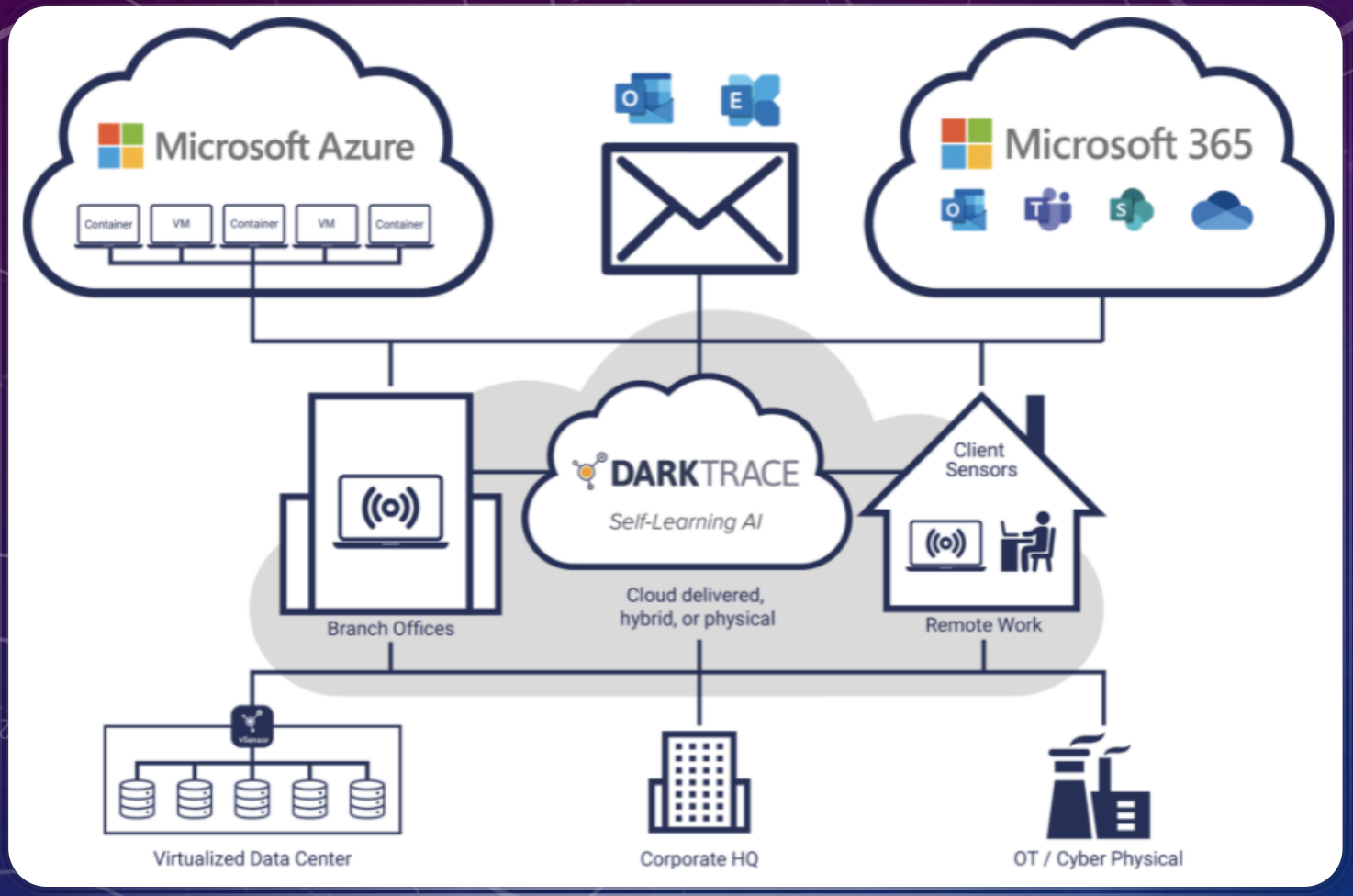
"This autonomous decision-making gives humans precious time to catch up with fast-moving incidents, and focus on higher-value, strategic work."

IT IS SELF LEARNING, IN THAT IT IS CLUSTERING USERS AND DEVICES INTO SIMILAR GROUPS AND THEN MONITORS FOR ANOMILIES. THEY CLAIM THAT THE SYSTEM REQUIRES NO PREPROCESSING OF DATA. MEANING THEY ARE ABLE TO 'THRIVE' IN COMPLEXITY. WITH THIS TYPE OF AI, THE MORE DATA, THE BETTER RESULTS. THIS MEANS AS THE COMPANY EXPANDS, THEIR DEFENSE SYSTEMS WILL NATURALLY IMPROVE.

DARKTRACE AND MICROSOFT

WE EXPLAINED BEFORE THAT DARKTRACE DOES NOT REPLACE SEIM SYSTEMS, IT ONLY ROUNDS THEM OUT. MICROSOFT HAS PARTNERED WITH DARKTRACE. IN DOING SO, THEY ARE CREATING A SECURITY ECOSYSTEM WHERE MICROSOFT IS THE BASE WITH DARKTRACE COVERING THE AUTONOMOUS RESPONSE AND 'NOVEL' CYBER THREAT DETECTION.

DARKTRACE AND MICROSOFT CONTINUED



DARKTRACE IS USED ON ALMOST ALL MICROSOFT 365 PRODUCTS. IT IS ALSO IMPLEMENTED ON DATA CENTERS HOSTED ON AZURE. DARKTRACE IS USED ACROSS THE ENTIRE MICROSOFT ENTERPRISE.

DOES DARK TRACE METHODS WORK? TRUE STORIES OF HACK ATTEMPTS AND HOW DARK TRACE CACHED AND RESOLVED THE ISSUE

STORY ONE

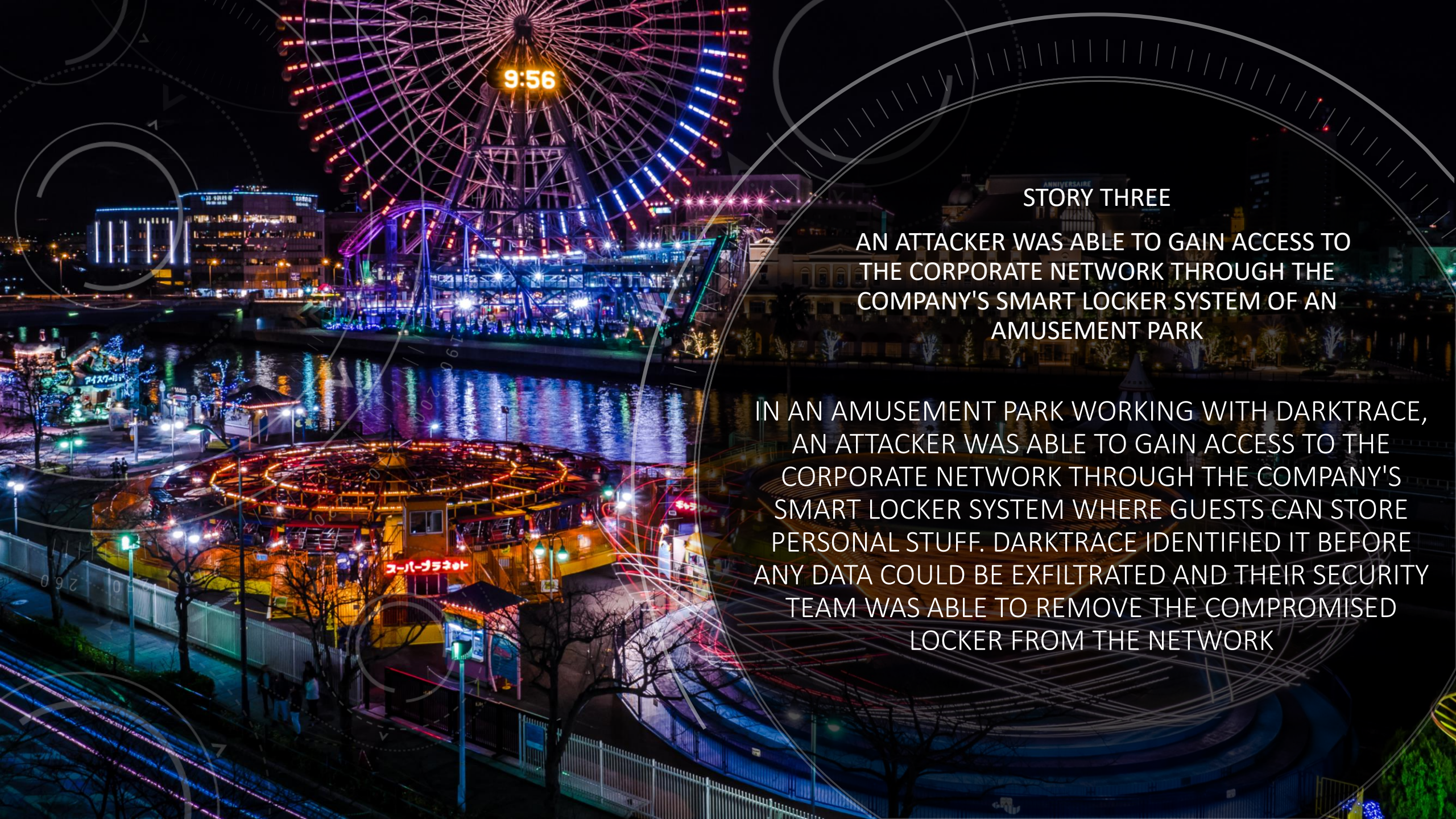
CASINO WAS HACKED THROUGH ITS INTERNET-ENABLED FISH TANK

THE "VERY LARGE" FISH TANK HAD AN IOT-CONNECTED THERMOSTAT TO MEASURE THE WATER TEMPERATURE THEY FORGOT TO TELL THE I.T AND SECURITY DEPARTMENTS ABOUT THIS NEW IOT DEVICE CONNECTED TO THE FISH TANK, ATTACKERS SCANNED THE NETWORK AND WERE ABLE TO BREAK IN THROUGH THIS THERMOSTAT. THEN THEY SEARCHED ACROSS, AND THEY TRIED TO FIND THE HIGH-ROLLERS DATABASE BECAUSE THAT'S WHAT WAS OF VALUE TO THEM, AND THEY WERE ABLE TO FIND SOME OF THAT TRY TO PULL IT BACK ACROSS THE NETWORK AND STEAL THE DATA AND MOVE IT UP TO A CLOUD, DARKTRACE WAS ABLE TO SPOT THE ACTIVITY BECAUSE IT WASN'T USUAL BEHAVIOR. NORMALLY, THE THERMOSTAT WOULDN'T LOOK FOR THE HIGH-ROLLER DATABASE AND SO THEY WERE ABLE TO SPOT IT AND STOP IT RIGHT IN ITS TRACKS

STORY TWO

USING THE COMPANY'S COMPUTER SERVERS AND PROCESSING POWER TO MINE BITCOIN

AN EMPLOYEE OF A LARGE BANK WAS SURREPTITIOUSLY USING THE COMPANY'S COMPUTER SERVERS AND PROCESSING POWER TO MINE BITCOIN. HIS JOB WAS TO LOAD NEW SERVERS INTO THE COMPUTER ROOM, OCCASIONALLY HE WOULD JUST TAKE ONE OF THESE SERVERS AND HIDE IT UNDER THE FLOORBOARDS IN THE DATA CENTER AND EVENTUALLY HE PUT ENOUGH SERVERS TOGETHER THAT HE STARTED RUNNING HIS OWN BITCOIN MINING OPERATION
THIS WAS DOING SOMETHING DIFFERENT THAN ALL THE OTHER SERVERS IN THE DATA CENTER, SO DARKTRACE'S ARTIFICIAL INTELLIGENCE WAS ABLE TO SPOT IT AND STOP IT RIGHT AWAY.



STORY THREE

AN ATTACKER WAS ABLE TO GAIN ACCESS TO THE CORPORATE NETWORK THROUGH THE COMPANY'S SMART LOCKER SYSTEM OF AN AMUSEMENT PARK

IN AN AMUSEMENT PARK WORKING WITH DARKTRACE, AN ATTACKER WAS ABLE TO GAIN ACCESS TO THE CORPORATE NETWORK THROUGH THE COMPANY'S SMART LOCKER SYSTEM WHERE GUESTS CAN STORE PERSONAL STUFF. DARKTRACE IDENTIFIED IT BEFORE ANY DATA COULD BE EXFILTRATED AND THEIR SECURITY TEAM WAS ABLE TO REMOVE THE COMPROMISED LOCKER FROM THE NETWORK

WHAT DO CUSTOMERS LIKE MOST ABOUT DARKTRACE? WHAT WORKED FOR THEM?

- ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY, ADVANCED MACHINE LEARNING CAPABILITIES, ENTERPRISE IMMUNE SYSTEM, ANTIGENA NETWORK, AND ANTIGENA EMAIL FEATURES ARE THE BEST.
- THE WAY THE SOLUTION DETECTS THE THREAT OVER THE NETWORK BEFORE IT SPREADS IS VERY GOOD. IT NOTIFIES YOU OF WHAT THE THREAT IS EXACTLY DOING AND GIVES YOU ALL THE DETAILS ABOUT THE EXECUTION OF THAT APPLICATION THAT HAD CREATED THE THREAT OVER YOUR NETWORK.
- THE PRODUCT OFFERS A VERY GOOD USER INTERFACE AND THE NETWORK VISIBILITY VERY GOOD.
- THE MOST VALUABLE FEATURE OF THIS SOLUTION IS THAT IT DOES NOT REQUIRE HUMAN INTERVENTION TO ELIMINATE A THREAT. ITS UNSUPERVISED MACHINE LEARNING HAS REDUCED TEAM'S EFFORTS A LOT.
- ITS ABILITY TO IDENTIFY MALICIOUS CONNECTED IPS FROM OUTSIDE AND THE ATTACKS THAT GET THROUGH TO THE INSIDE IS VALUABLE
- THE DYNAMIC THREAT DASHBOARD IS VERY NICE, IT LISTS ALL THREATS AND RATES THEM, AND THEN YOU CAN CHOOSE WHETHER TO INVESTIGATE FURTHER.
- THE ALERTS ARE MEANINGFUL. THE EVENT ROLLS UP INTO MEANINGFUL AND ACTIONABLE ALERTS RATHER THAN JUST BEING NOISE.

SAMPLE DARKTRACE REVIEWS

FEBRUARY 09, 2021

DarkTrace is great for small to medium size businesses

Share

Verified User
Analyst in Information Technology
Public Safety Company, 201-500 employees

Score 10 out of 10 · Vetted Review · Verified User · Review Source

Use Cases and Deployment Scope

We needed a better insight into network security threats that might be in our organization. DarkTrace provides an invaluable service of not only giving us the ability to dig deep into possible network intrusions but also has a weekly summary of possible network security issues. One of the main reasons we chose DarkTrace was that they provided the weekly report put together by a security professional. We review this weekly report and take action as needed.

FEBRUARY 09, 2021

DarkTrace is great for small to medium size businesses

Share

Verified User
Analyst in Information Technology
Public Safety Company, 201-500 employees

Score 10 out of 10 · Vetted Review · Verified User · Review Source

Use Cases and Deployment Scope

We needed a better insight into network security threats that might be in our organization. DarkTrace provides an invaluable service of not only giving us the ability to dig deep into possible network intrusions but also has a weekly summary of possible network security issues. One of the main reasons we chose DarkTrace was that they provided the weekly report put together by a security professional. We review this weekly report and take action as needed.

FEBRUARY 19, 2020

Good tool but a LOT of false positives

Share

Verified User
Professional in Information Technology
Primary/Secondary Education Company, 1001-5000 employees

Score 7 out of 10 · Vetted Review · Verified User · Review Source

Use Cases and Deployment Scope

I worked with Darktrace in a couple of organizations (from 300 to 1000+ users). Darktrace is a beneficial product to keep track of lateral network traffic inside of the organization. It augments the firewall, which looks at the traffic moving in and out of the company's LAN. Darktrace utilizes SPAN ports on switches to get the traffic, that's the only configuration needed outside of the Darktrace appliance, making installation relatively easy. If organization has multiple locations, either multiple Darktrace units will be required, or the network must be configured to forward SPAN traffic. Darktrace does provide beneficial insights into network activity inside the network, such as the use of obsolete protocols, DLP breaches, etc.

JANUARY 12, 2018

Why I didn't pick Darktrace

Share

Matt Frederickson
Director of Information Technology
Council Rock School District (Education Management, 1001-5000 employees)

Score 2 out of 10 · Vetted Review · Verified User · Review Source

Use Cases and Deployment Scope

Brought it in to act as an intelligence gatherer for network traffic - specifically to look for anomalies and help identify potential threats and suspicious activity. I installed it at the network core, so it was able to view all traffic (well, mostly all traffic - we had a few issues with some of the VLANs and my switches are configured for fault tolerance, which it also had an issue with) moving from inside to outside.

QUESTIONS?

References
https://www.cyberseer.net/technologies/darktrace/faqs/
https://merlincyber.com/solarwinds-orion-breach-network-security-darktrace-cyberark-wickr/
https://www.darktrace.com/en/self-learning-ai/
https://www.darktrace.com/en/microsoft/
World–Leading AI for Cyber Security | Darktrace