# Cybersecurity Center of Excellence (CCOE) Recent Discovery

Uncompromised Defense using Machine learning

Only at ZolonTech

## Synopsis

Within just 5 years of introducing the internet to the world, the first cyber-attack took place in America called “The Morris Worm”, which spread like wildfire and slowed down many computers. Ever since then mankind has sought multiple ways of protecting the web and private networks, but with evolving security measures and firewalls, the cyber-attacks evolved with them getting more powerful and immune to anti-virus protocols and trespassing private networks to steal and misuse private information. Today, it has never been so important to protect your information as, cyber threats became an inevitable part of ever expanding modern digital environments, with targeted attacks and threats coming from both foreign and internal sources. But how do you protect against a threat that is continuously evolving and continuously fighting your networks? How do you implement a long-lasting system to protect your information? The obvious solution is to continuously update security measures and firewalls. But, to do so how much effort does one spend?

What if you don’t have to put in any effort? What if there is an intelligent automated system that updates on its own and fights back threats continuously and develops a robust system to keep your information safe at all times and with minimum human input? Enter, Zolon Tech Inc. (ZTI). Realizing cyber threat is an inevitable part of doing business, ZTI, has been exploring solutions on how it can provide a continuous approach to cyber security. ZTI’s Cybersecurity Center of Excellence (CCOE) is always evaluating new and emerging technologies to bring the best solutions to our government customers. In order to do this, we have developed an end-to-end cybersecurity solution using Darktrace, Splunk, and others to deliver an end-to-end cybersecurity technology solution that uses advanced machine learning and artificial intelligence algorithms to detect and respond to previously unknown cyber-threats as they emerge in real-time. Our solution of identifying threats early on and mitigating them before they become a full-blown crisis can be deployed across both IT and OT environments to provide full coverage of your organization. We will explore how ZTI can help your organization protect your information and continuously identify and mitigate cyber threats.

# Contents

# Modern Cyber Ecosystem

The importance of information protection and choosing the right security measure to defend your organization can never be overlooked. Defending against cyber-attacks has never been so critical with classified information being stolen such as the hack on Department of justice where information on 10,000 DHS and 20,000 FBI employees have been compromised on February of 2016. What could be more alarming then classified information being stolen? The Department of justice took one week to realize the hack and is still unaware of how it happened.

Access to data – and lots of it – has become an everyday norm. The ubiquitous nature of high–speed data connectivity, coupled with the ever–growing capacity of portable storage devices, means that an individual with intent can steal, corrupt and/or destroy vast amounts of data with relative impunity. Protecting private data from foreign and internal hackers has always been the primary objective of any basic cyber security. Yet, so many  have failed, one of the most notorious internal hacks was done by none other than Edward Snowden, a former CIA employee stealing thousands of classified documents from NSA's one of the most secure facilities in the world in 2013.

Cybersecurity is at a crisis point, with so many traditional security measures failing many organizations, and leading them to a disarray in choosing and implementing a robust defense against cyber-attacks. Attackers' are gaining the ability to iterate new and different versions of malware to evade detection has been potentiated over the last decade or so by the development of a market for exploit kits on the dark web, as well as the evolution of the cloud. Security research labs talk of half a million unique new pieces of malware appearing every day.  And to add on to this, organizations have to prepare for internal threats as if foreign threats weren't enough of a problem. With whistleblowers gaining momentum to expose organizations confidential data, today's organization are looking for an overall package that can provide security at multiple levels of the organization both from internal and external attacks effectively, efficiently and most importantly in real-time with rapid awareness and mitigation.

With so many backdoors, the defender is challenged with enhancing their visibility and insights into their own organizations' systems, in order to regain the advantage and inform critical, timely decision-making. And it's about high time that mankind sought a new type of defense to protect our valuable data from invaders. That has been the goal of ZTI's Cybersecurity Center of Excellence (CCOE) to find a solution that is capable of tackling a cyber-attack at scale. Through intensive research and testing we discovered that Darktrace's Enterprise Immune System was in a class of their own, Gartner named them "Cool Vender" in 2015. Darktrace's technology is founded in the fields of artificial intelligence and machine learning from the work of two renowned Mathematicians from the University of Cambridge remarkable; Professor Bill Fitzgerald was Professor of Applied Statistics and Signal Processing, and the Head of Research, in the Signal Processing Laboratory at the University of Cambridge. His ground-breaking work on Bayesian statistical methodology as applied to signal and data modelling had a profound impact on the study of signal processing, both within the University of Cambridge and internationally. Dr. Mike Lynch OBE is a renowned technologist, Fellow of the Royal Society, and an advisor to the UK government. His work and research in the area of Bayesian mathematics and machine learning built multi-billion dollar company Autonomy.

## Intelligent Cyber Defense

What could be more dangerous than your information being stolen, or your private systems and networks impaired? Small attacks which are quiet and almost unseen by many cyber defenses today that slowly cross the boundary defense of to your network unnoticed and remain dormant without sending any information back for many days waiting to be activated. Once activated these sophisticated attacks can change your systems at will, or install kill switches that could lead to fatal consequences. Attacks such as these require constant monitoring at each and every level of your organization to identify and mitigate them. Monitoring at this minute level with large networks requires a very sophisticated cyber defense system that could provide instant warnings and mitigation procedures to stop such attacks. Creating cyber intelligence using machine learning presents a significant opportunity to the cyber security industry to identify the most minuscule of threats.

ZTI – CCOE started testing Darktrace's technology, a machine learning company for cyber defense and we found a promising solution with results that started to make a difference in how we approach cybersecurity. ZTI quickly started experimenting with this technology at scale with a wide range of scenarios and various benefits we could create by adding value added services such as Splunk and Amazon Web Services. By creating an intelligent cyber defense solution, ZTI - CCOE was able to provide a sophisticated end to end cybersecurity solution to help organizations face many challenges that existing systems faced. With our innovative and an industry first cybersecurity suite we were able to provide total visibility and tailored, real-time insights into emerging anomalies. This intelligence-based approach is at the heart of the new generation of cyber defense, based on skilled people and cutting-edge 'immune system' technologies engaged in an ongoing process of learning, understanding and dealing with developing issues, before they turn into crises.

## Under the Hood

Using Darktrace, ZTI is able to provide an advanced Enterprise Immune System technology, powered by artificial intelligence capable of finding anomalies that bypass other security tools. With a proven track record ZTI's cyber defense suite is able to detect a wide range of cyber-threats, using a probabilistic approach that takes into account multiple weak indicators to form a compelling picture of overall threat. Here is underlying principle of our cybersecurity suite that is used by Machine learning to create next generation of cyber security solutions powered by Artificial intelligence:

- A system that can autonomously learn what is normal within a network – and doesn't depend upon knowledge of previous attacks.
- It thrives on the scale, complexity and diversity of modern businesses, where every device and person is slightly different.
- It turns the innovation of attackers against them – any unusual activity is visible.
- It constantly revisits assumptions about behavior, using probabilistic mathematics.
- It is always up to date and not reliant on human input.

Using a probabilistic approach to cyber security based on a Bayesian framework Darktrace integrates a huge number of weak indicators of potentially anomalous network behavior to produce a single clear measure of how likely a network device is to be compromised. This probabilistic mathematical approach is critical to our solution's unique ability to understand important information, amid the noise of the network – even when it does not know what it is looking for.

One could ask there could be so many anomalies happening in day to day operations of enterprise level organization, finding a critical threat is like finding a needle in a haystack. With the added challenge of haystack growing incrementally every day. And how do you define the needle? With millions of versions of sophisticated malware circulating, thousands of users accessing data, hundreds of supply chain companies and partners walking in and out of your digital premises every day.

The challenge of finding the needle is cumbersome and if neglected long enough we don't know how it is behaving or what its objective is, and by the time we find where it is, it could too late. Cyber-attacks are impossible to guess how and where will they start and finish. At ZTI we identified this problem early on and our team at CCOE experimented with countless technologies that was capable of a robust cyber security system that is one of discovery – of knowing, ahead of time, about the threats and can perform these activities with minimum human supervision. ZTI found an ingenious solution to identify and respond to in-progress cyber-threats by unsupervised machine learning. By implementing artificial intelligence with unsupervised machine learning we let the computer do all the hard work for us, it autonomously detects, prioritizes, alerts, mitigates by taking action against cyber-threats within all types of networks, including physical, cloud, virtual, IoT, and ICS environments and provide a very intuitive way of interaction with the system that is visually pleasing and easy to use; an industry first.

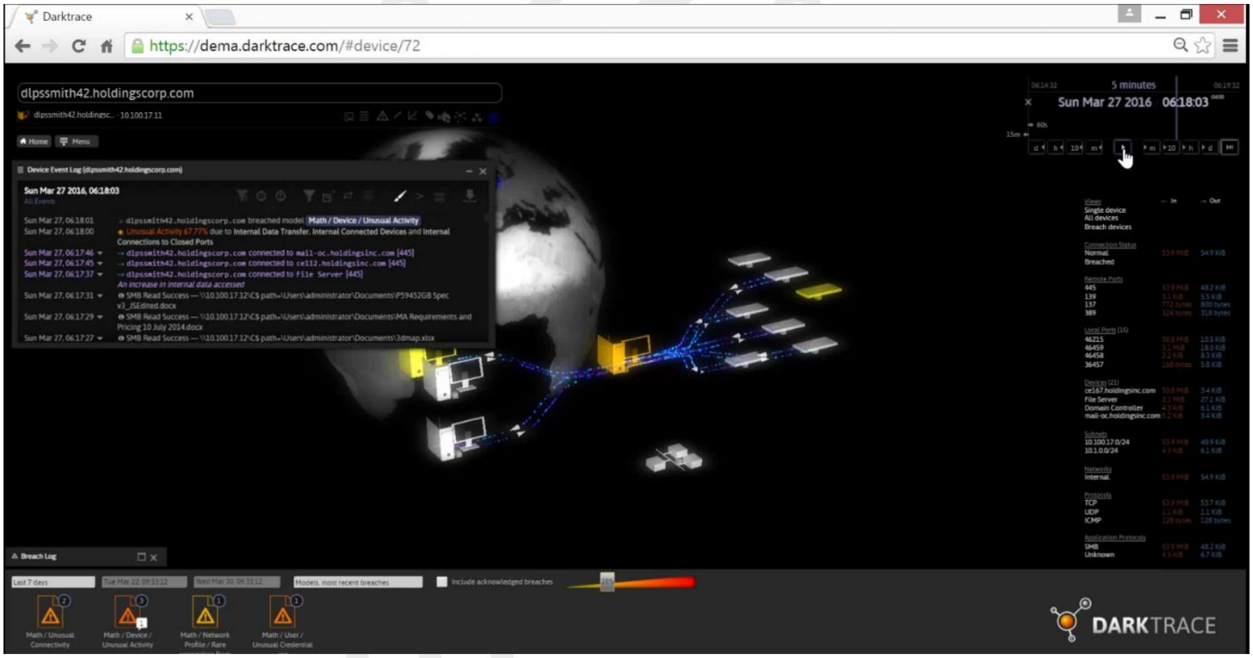
## Unsupervised Machine Learning

ZTI has mastered the means of delivering the next generation of machine learning cybersecurity solutions powered by artificial intelligence to any organization to continuously protect your data and fight against cyber attackers. With unsupervised machine learning methods we do not require training data with pre-defined labels. Instead the AI is able to identify key patterns and trends in the data, without the need for human input. The advantage of unsupervised learning is that it allows computers to go beyond what their programmers already know and discover previously unknown relationships. With unsupervised machine learning algorithms to analyze network data at scale, intelligently handle the unexpected, and embrace uncertainty. Instead of relying on knowledge of past threats to be able to know what to look for, it is able to independently classify data and detect compelling patterns that define what may be considered to be normal behavior. Any new behaviors that deviate from those, which constitute this notion of 'normality,' may indicate threat or compromise. The impact of unsupervised machine learning on cyber security is transformative:

- Threats from within, which would otherwise go undetected, can be spotted, highlighted, contextually prioritized and isolated using these algorithms.
- The application of machine learning has the potential to provide total network visibility and far greater detection levels, ensuring that networks have an internal defense mechanism.
- It has the capability to learn when to action automatic responses against the most serious cyber threats.

# Your New Dashboard

At ZTI we create solutions from the customer's perspective. We test our solutions as if we are the end user and test the system thoroughly to find flaws or other discomforts and work our way to provide a better service. We only want to provide what we would use, and at ZTI we do not compromise and seek only the best. Through this practice we are proud to say that our Cyber security solution has one of the most intuitive user interface than any other product in the world. Our dashboard is visually pleasing and easy to use by any member of your organization and does require a background in Cyber Security or as a matter of fact even in computer Science.


Darktrace
https://dema.darktrace.com/#device/72
dlpssmith42.holdingscorp.com
dlpssmith42.holdingsc... · 10.100.17.11
Home
Menu
Device Event Log (dlpssmith42.holdingscorp.com)
Sun Mar 27 2016, 06:18:03
All Events
06:14:32
5 minutes
06:19:32
Sun Mar 27 2016 06:18:03
60s
15m
d
h
10
m
m
10
h
d
Breach Log
Last 7 days
Tue Mar 22 09:33:12
Wed Mar 30 09:33:12
Models, most recent breaches
Include acknowledged breaches
Math / Unusual Connectivity
Math / Device / Unusual Activity
Math / Network Profile / Rare
Math / User / Unusual Credential
DARKTRACE

```
Sun Mar 27, 06:18:01      dlpssmith42.holdingscorp.com breached model Math / Device / Unusual Activity
Sun Mar 27, 06:18:00      Unusual Activity 67.77% due to Internal Data Transfer, Internal Connected Devices and Internal
                          Connections to Closed Ports
Sun Mar 27, 06:17:46 ▾    → dlpssmith42.holdingscorp.com connected to mail-oc.holdingsinc.com [445]
Sun Mar 27, 06:17:45 ▾    → dlpssmith42.holdingscorp.com connected to ce112.holdingsinc.com [445]
Sun Mar 27, 06:17:37 ▾    → dlpssmith42.holdingscorp.com connected to File Server [445]
                          An increase in internal data accessed
Sun Mar 27, 06:17:31 ▾    SMB Read Success — \\10.100.17.12\C$ path=\Users\administrator\Documents\P59452GB Spec
                          v3_JSEdited.docx
Sun Mar 27, 06:17:29 ▾    SMB Read Success — \\10.100.17.12\C$ path=\Users\administrator\Documents\MA Requirements and
                          Pricing 10 July 2014.docx
Sun Mar 27, 06:17:27 ▾    SMB Read Success — \\10.100.17.12\C$ path=\Users\administrator\Documents\3dmap.xlsx
```

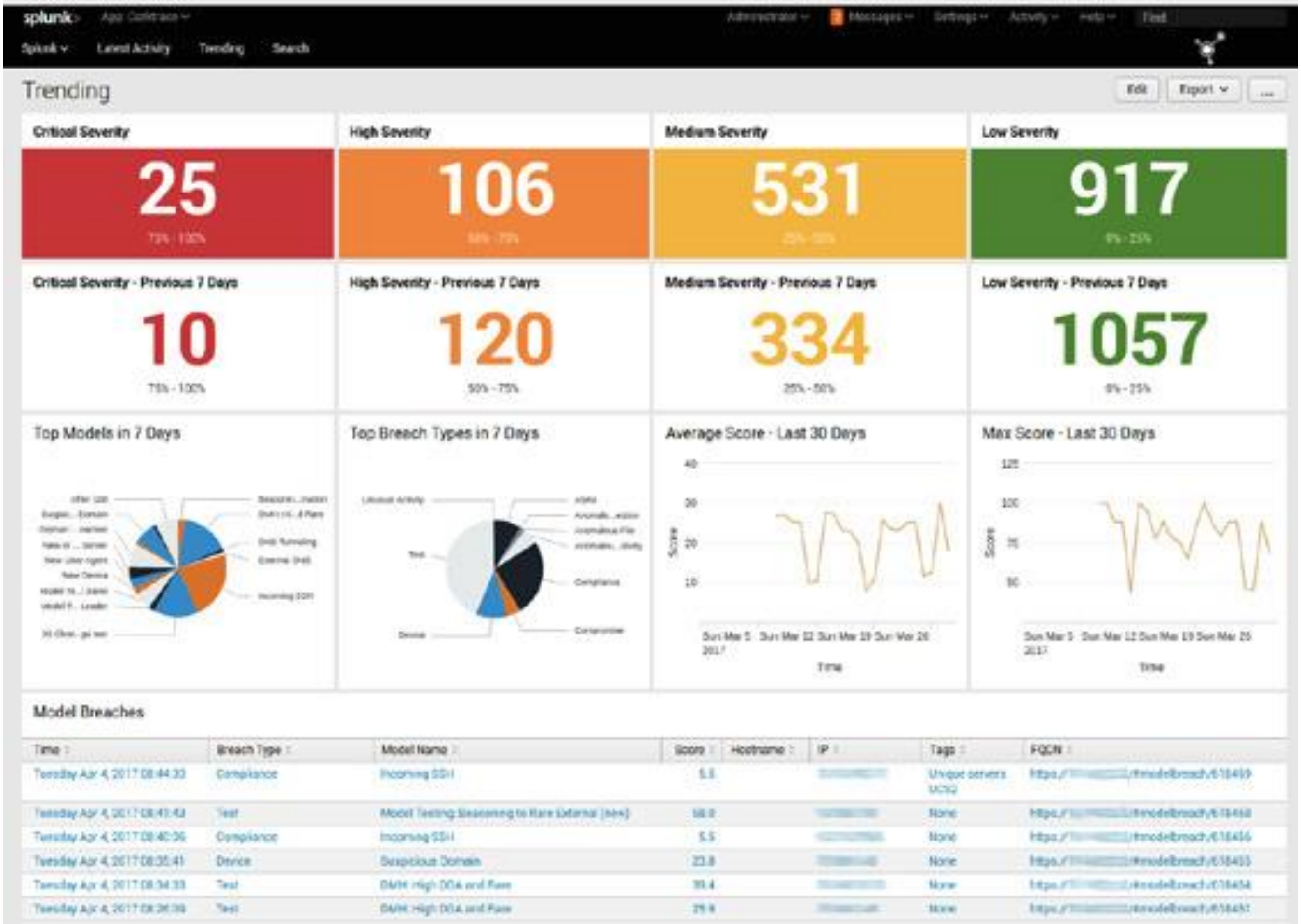
| Views | ← In | → Out |
|---|---|---|
| Single device | | |
| All devices | | |
| Breach devices | | |
| Connection Status | | |
| Normal | 53.9 MiB | 54.9 KiB |
| Breached | | |
| Remote Ports | | |
| 445 | 53.9 MiB | 48.2 KiB |
| 139 | 3.1 KiB | 5.5 KiB |
| 137 | 772 bytes | 800 bytes |
| 389 | 324 bytes | 318 bytes |
| Local Ports (15) | | |
| 46215 | 50.8 MiB | 10.5 KiB |
| 46459 | 3.1 MiB | 18.0 KiB |
| 46458 | 2.2 KiB | 8.3 KiB |
| 36457 | 168 bytes | 5.8 KiB |
| Devices (21) | | |
| ce167.holdingsinc.com | 50.8 MiB | 3.4 KiB |
| File Server | 3.2 MiB | 27.1 KiB |
| Domain Controller | 4.3 KiB | 6.1 KiB |
| mail-oc.holdingsinc.com | 5.2 KiB | 3.4 KiB |
| Subnets | | |
| 10.100.17.0/24 | 53.9 MiB | 40.9 KiB |
| 10.1.0.0/24 | 4.3 KiB | 6.1 KiB |
| Networks | | |
| Internal | 53.9 MiB | 54.9 KiB |
| Protocols | | |
| TCP | 53.9 MiB | 53.7 KiB |
| UDP | 1.1 KiB | 1.1 KiB |
| ICMP | 128 bytes | 128 bytes |
| Application Protocols | | |
| SMB | 53.9 MiB | 48.2 KiB |
| Unknown | 4.3 KiB | 6.7 KiB |

*Figure 1 Darktrace Dashboard*

The main interface shows a map with an overall view of your organization around the world. It is able to take in all raw network traffic and profile it even with multiple application protocols, with all your remote and local ports, which is displayed towards the right of the above figure. Once all the data is streamlined automatically by machine learning, it constructs a baseline of what normal activity looks like for individual users and devices and subnets as a whole. It automatically send you alerts when an anomaly occurs and the user is able to drill down to specific individual or device with their IP address, the time and the detailed information of the anomaly. The above figure shows a visual map of where an anomaly took place and shows the device in question in yellow color and the network it accessed in orange color and the unauthorized data it had accessed in yellow color towards the right. This is only one of many examples that our solution can provide.

## Real-Time Analysis

ZTI’s CCOE has developed a number of connectors that facilitate and integrate seamlessly with our end to end to cyber security suite with third-party platforms that enhance functionality. We have tested and evaluated many SIEM tools in the market today and integrated only the most versatile tool in our cyber security solution that can handle the most advanced of security cases. With the Darktrace Splunk Connector we have enhanced the Splunk user interface by populating it with real-time threat alerts from our Enterprise Immune System platform. The threat alerts link to detailed reports in the Darktrace Threat Visualizer, allowing for deep analysis of emerging vulnerabilities and early-stage threats. With straightforward installation and an intuitive dashboard, the connector is easily implemented within your existing Splunk interface.



Trending

| Critical Severity | High Severity | Medium Severity | Low Severity |
|---|---|---|---|
| 25<br>75% - 100% | 106<br>50% - 75% | 531<br>25% - 50% | 917<br>0% - 25% |

| Critical Severity - Previous 7 Days | High Severity - Previous 7 Days | Medium Severity - Previous 7 Days | Low Severity - Previous 7 Days |
|---|---|---|---|
| 10<br>75% - 100% | 120<br>50% - 75% | 334<br>25% - 50% | 1057<br>0% - 25% |

Model Breaches

| Time | Breach Type | Model Name | Score | Hostname | IP | Tags | FQDN |
|---|---|---|---|---|---|---|---|
| Tuesday Apr 4, 2017 08:44:33 | Compliance | Incoming SSH | 5.5 | | [redacted] | Unique servers UCSQ | https://[redacted]/#modelbreach/618459 |
| Tuesday Apr 4, 2017 08:41:43 | Test | Model Testing: Beaconing to Rare External (new) | 58.8 | | [redacted] | None | https://[redacted]/#modelbreach/618458 |
| Tuesday Apr 4, 2017 08:40:36 | Compliance | Incoming SSH | 5.5 | | [redacted] | None | https://[redacted]/#modelbreach/618456 |
| Tuesday Apr 4, 2017 08:35:41 | Device | Suspicious Domain | 23.8 | | [redacted] | None | https://[redacted]/#modelbreach/618455 |
| Tuesday Apr 4, 2017 08:34:33 | Test | DMM: High DGA and Rare | 39.4 | | [redacted] | None | https://[redacted]/#modelbreach/618454 |
| Tuesday Apr 4, 2017 08:28:39 | Test | DMM: High DGA and Rare | 29.8 | | [redacted] | None | https://[redacted]/#modelbreach/618451 |

*Figure 2 Splunk dashboard*

The connector allows for high-priority alerts generated by Darktrace to be displayed in the Splunk UI. Clicking on any of the panels will cause the table on the bottom of the screen to auto-generate with model breaches based on the input/filter pressed. For instance, clicking on the RED portions for 'High Impact' will filter the table to look for scores between 75% and 100%, the highest scoring models within Darktrace. While the connector can be customized depending on the needs of your organization, ZTI - CCOE recommends to aggregate the model breaches within Splunk and access them inside the Threat Visualizer for further investigation.

The model breaches in the dashboard link directly to the corresponding model breach, allowing for quick and easy investigation. The Latest Activity page highlights the alerts in the last 7 days, which can be easily filtered by timeframe, score, and model. Likewise, the Trending page highlights the performance of models and the system overall for the last 2 weeks, suggesting actionable changes to models or obvious devices that may need attention. ZTI’s solution for today’s cyber security environment allows for a simple, straightforward, automated, self-configuring cyber defense platform, generating real-time threat alerts that other security systems miss and provide an intuitive design of the suite that can easily be used and 100% reliable, consistently.

# Action Plan

A new era in computing power has begun from IBM’s Watson’s to Google’s deep mind, machines are getting more smarter and faster each day and what better system is there to tackle the most arduous task of fighting cyber-crime then a machine, powered by artificial intelligence. Threats that you do not know exist must nevertheless be found. This is only possible by moving on from rules, and embracing a continuous and more subtle approach that blends self-learning machine learning with skilled people and good process. Doing this, we give ourselves the best possible advantage in the perpetual battle against the sharp end of the cyber-threat spectrum.

Accessibility to this next generation of advanced cyber fighting machines powered by artificial intelligence is closer than you think. With one hour install time and a free trial with no obligations, use unsupervised machine learning to detect threats on your network in real-time with ZTI’s end-to-end cybersecurity solution using Darktrace and Splunk today to see the change yourself. With so many organizations moving to the cloud Darktrace Cloud Connectors allow ZTI to easily extend Darktrace’s visibility and detection capabilities to Cloud based offerings. This allows anomalous behaviors to be detected, extending Darktrace’s Enterprise Immune System defense beyond the physical enterprise network and into Cloud environments.

# Conclusion

‘Cyber’ is no longer simply an IT issue, but a consideration for all parts of the business that interact with the lifeblood of the organization – its data. With ever increasing scope and complexity of networks, the opportunities for attackers to exploit the gaps have increased. High-profile hacks against corporations have become a regular norm, many of which are household names, such as yahoo, where hackers stole millions of accounts data, twice! These attacks remind us that no one is invulnerable to cyber-attacks. Many organizations are still unable to determine the origin or sometimes even when their networks are being attacked. If these attacks were to teach us one thing; investment in traditional, security measures is not sufficient to protect and mitigate against cyber threats, due to the underlying flaw or a key concept that is often overlooked is, the failure to continuously adopt to ever-evolving cyber environment.

Machine learning is difficult to deliver, but ZTI’s machine learning cybersecurity solution based on Darktrace’s probabilistic approach to cyber security is proving that it works. The Enterprise Immune System approach to provide end to end cyber security from ZTI means that, detection no longer depends on an archive of previous attacks. Instead, attacks can be spotted against the background understanding of what represents normality within a network. No pre-definitions are needed, which allows for the best possible insight and defense against today’s threats.

With companies like Apple and Google already bringing AI to the consumer market through virtual assistants, it is in no doubt that Machine learning and Artificial Intelligence is going to change the entire world as we know it in the next coming decade. With so many advancements already in progress, and the computational power to deliver these methods are becoming widely accessible, Machine learning can progress exponentially. Ladies and Gentleman, the third great era of automation is here and this is your chance to make use of a unique opportunity from ZTI to avail this next generation defense system and start protecting your data today.

ZolonTech

**13921 Park Center Road, Suite 500**
**Herndon, VA 20171**
**www.zolontech.com**