



 **Threat Doctor**
Discover. Analyze. Protect

Quadrasystems.net India
Private Limited

Traditional security solutions lack completeness of vision and collective intelligence.



Data is inherently dumb. It doesn't do anything unless you know how to use it, how to act on it.

- Gartner



Too many security solutions to evaluate, buy and integrate!

The image displays a comprehensive grid of security solutions, categorized into various domains. The categories and their associated companies are as follows:

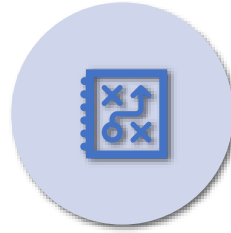
- Network & Infrastructure Security:** Advanced Threat Protection (SentinelOne, Palo Alto Networks, Fortinet, etc.), NAC (Cisco Duo, Duo Security), SDN (Cisco ACI, VMware NSX), DDoS Protection (Akamai, Cloudflare), DNS Security (Cisco Umbrella, Fortinet), Network Firewall (Cisco Firepower, Palo Alto Networks), Deception (Cisco Stealthwatch, Palo Alto Networks).
- Web Security:** Akamai, Cloudflare, Imperva, etc.
- Endpoint Security:** Avira, Avast, Avast Secure, etc.
- Application Security:** WAF & Application Security (Akamai, Cloudflare, Imperva), Application Security Testing (Veracode, Checkmarx).
- MSSP:** Traditional MSSP (Verizon, AT&T), Advanced MSSP & MDR (Arctic Wolf, SecureWorks).
- Data Security:** DLP (Symantec, McAfee), Data Privacy (OneTrust), Data Centric Security (Druva, Rubrik).
- Mobile Security:** Mobile Device Management (VMware Workspace ONE, Microsoft Intune), Mobile Security (Avast, McAfee).
- Risk & Compliance:** Risk Assessment & Visibility (PwC, Deloitte), Risk Quantification (RiskLens, FICO), Pen Testing & Breach Simulation (Cobalt, Rapid7), CRC (Checkmarx), Security Awareness & Training (KnowBe4, SANS).
- Security Operations & Incident Response:** SIEM (Splunk, IBM QRadar), SOAR (Palo Alto Networks, ServiceNow), Incident Response (CyberArk, Palo Alto Networks).
- Threat Intelligence:** Anomali, Blueliv, etc.
- IoT:** IoT Devices (Cisco Duo, Palo Alto Networks), Automotive (Ford, GM), Connected Home (Cisco Duo, Palo Alto Networks).
- Messaging Security:** AGARI, AREA 1, etc.
- Identity & Access Management:** Authentication (Okta, OneLogin), Privileged Management (CyberArk, BeyondTrust), Identity Governance (SailPoint, ADAMICS), Consumer Identity (Okta, OneLogin).
- Security Analytics:** Awake, Broadcom, etc.
- Threat Intelligence:** Anomali, Blueliv, etc.
- IoT:** IoT Devices (Cisco Duo, Palo Alto Networks), Automotive (Ford, GM), Connected Home (Cisco Duo, Palo Alto Networks).
- Messaging Security:** AGARI, AREA 1, etc.
- Digital Risk Management:** Digital Shadows, etc.
- Security Consulting & Services:** Deloitte, EY, etc.
- Blockchain:** Blockchain (Blockchain.com, etc.).
- Fraud & Transaction Security:** Fraud (FICO, etc.), Transaction Security (FICO, etc.).
- Cloud Security:** Container (Aqua Security, etc.), Infrastructure (Palo Alto Networks, etc.), CASB (Cloud Access Security Broker) (Symantec, etc.).

Our approach to security

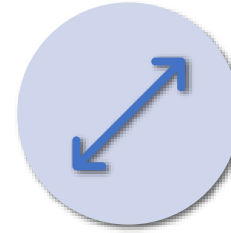
- A holistic approach to security across people, processes and infrastructure
- Connect security to business outcomes
- Make security simple with managed services and insightful analytics



Seek order from chaos with Quadra's AI infused threat intelligence service



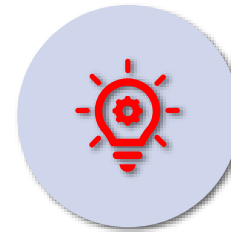
The threat landscape
is evolving at pace
faster than most
businesses can
manage



The massive shift to
the cloud provides the
best opportunity to
manage this
avalanche of attacks



Microsoft's global
cloud infrastructure
monitors 6.5 trillion
signals



How can we turn
this to your
advantage?

Threat Doctor: **how does it help?**

01

Get the power of AI and ML behind your security strategy - use Azure Cognitive services to detect latent threats that can affect your business

02

Enable a proactive approach to security


03



Correlate what's happening in your enterprise with global security signals

Comprehensive insights with MISP

- MISP is a threat intelligence platform for gathering, sharing, storing and correlating indicators of compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information
- Threat Doctor integrates Security Graph API signals and indicators from MISP to provide customers a truly holistic view of their security landscape

OSINT - CVE-2015-2545: overview of current threats

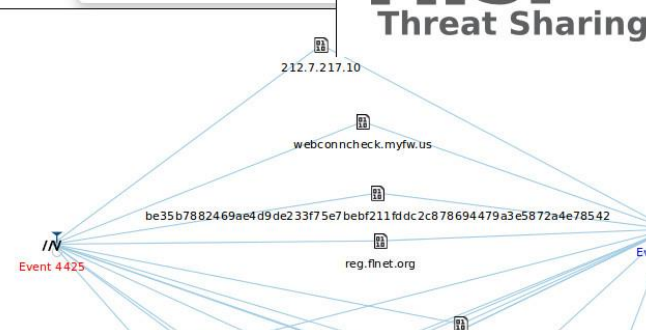
Event ID	3865
Uuid	57460863-76dc-4272-8116-4ea302de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	tjp:white x circl:osint-feed x Type:OSINT x estimative-language:likelihood-probability="very-unlikely" x +
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability="almost-no-chance"	
Likelihood or probability: Very unlikely - highly improbable - 05-20%	0	estimative-language:likelihood-probability="very-unlikely"	

Related Events

- [2016-05-27 \(3883\)](#)
- [2016-05-23 \(3844\)](#)
- [2016-05-06 \(3828\)](#)

Org: CIRCL
Date: 2016-05-23
Info: OSINT - Operation Ke3chang Resurfaces With New TidePool Malware



Get started right away!



Activate trial

Analysis of existing environment

Enabling trial EM+S E5 and O365 ATP P2 trial

Identify PoC users

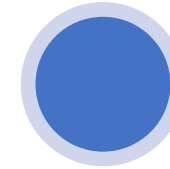
Configuring required policies in Admin centre to capture the Security logs



Consolidate logs

Intelligent Automation tool downloads logs at 15-day and 30-day intervals

Multiple logs are consolidated and prepared for analysis

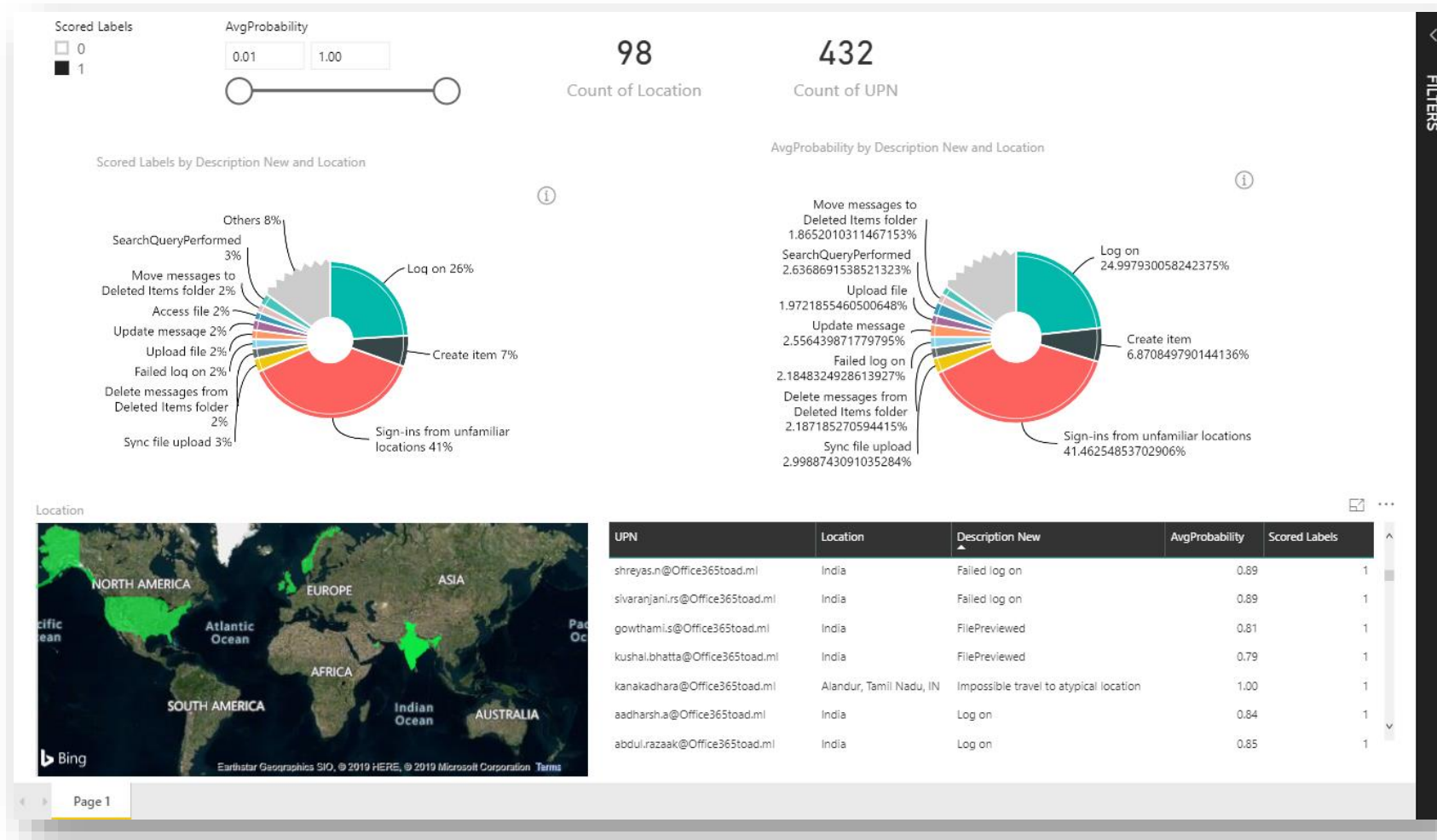


Intelligent analysis

Threat Doctor's Anomaly detection ML Engine will intelligently analyse and interpret the collected logs; correlated with threat indicators from MISP

Deliver predictive analysis of threat landscape through PowerBI report

Your security posture, simplified.



Get secure, stay secure

Quadra Security Center | Threat Doctor Managed Services

24x7 Security with Managed Services

Quadra Security Center

Quadra's Threat Doctor doesn't just give you security insights. It keeps your business secure. Managed Services complete the security lifecycle, from technology acquisition to management. Across five distinct stages of cyber security management, rely on our managed services to:



Establish high level of security preparedness



Ensure always-up-date security posture



Reduce complexity and cost

Threat Doctor Managed Services

5 reasons why your business is in safe hands



Built on the **Microsoft Zero Trust Assessment Model**



No logs – only **curated actionable insights** driven by AI and ML



360° protection across security lifecycle– Identify, Protect, Detect, Respond and Recover



Monitor **both cloud and on-premises** environments with Azure Sentinel integration



Remote monitoring and onsite remediation options give you maximum flexibility

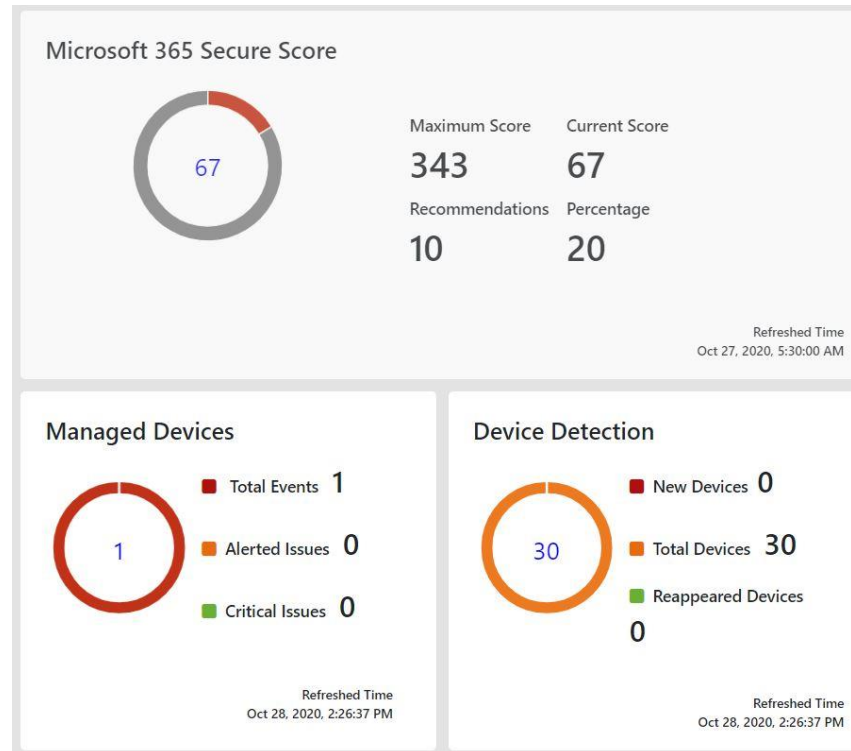
IDENTIFY



Right from the trial stage, Threat Doctor helps you to understand and document cybersecurity risk to your systems, people, assets, data, and capabilities, including:

- Identifying physical and software assets to establish an Asset Management program
- Identifying cybersecurity policies to define a Governance program
- Identifying a Risk Management Strategy for your business





IDENTIFY



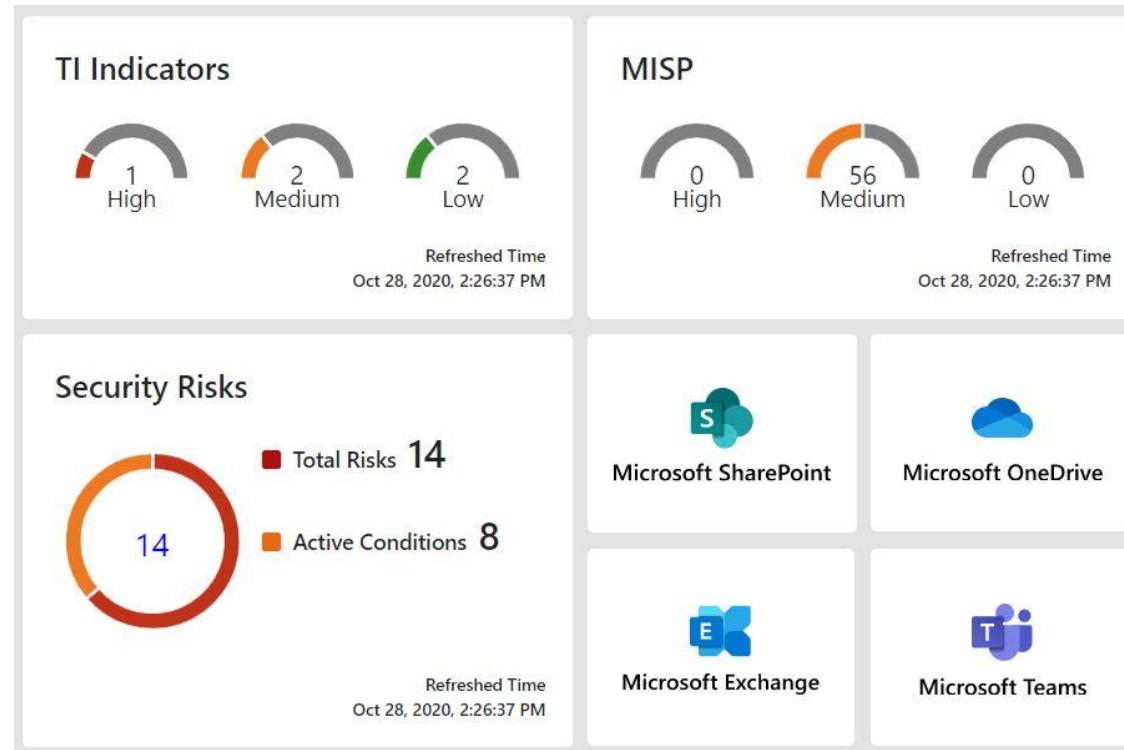
PROTECT



Threat Doctor enables you to limit or contain the impact of potential cybersecurity events and outlines safeguards for delivery of business-critical services, by:

- Protecting the confidentiality, integrity, and availability of your data
- Ensuring the security and resilience of systems
- Empowering your IT and cyber security team with awareness and training

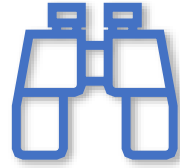




PROTECT

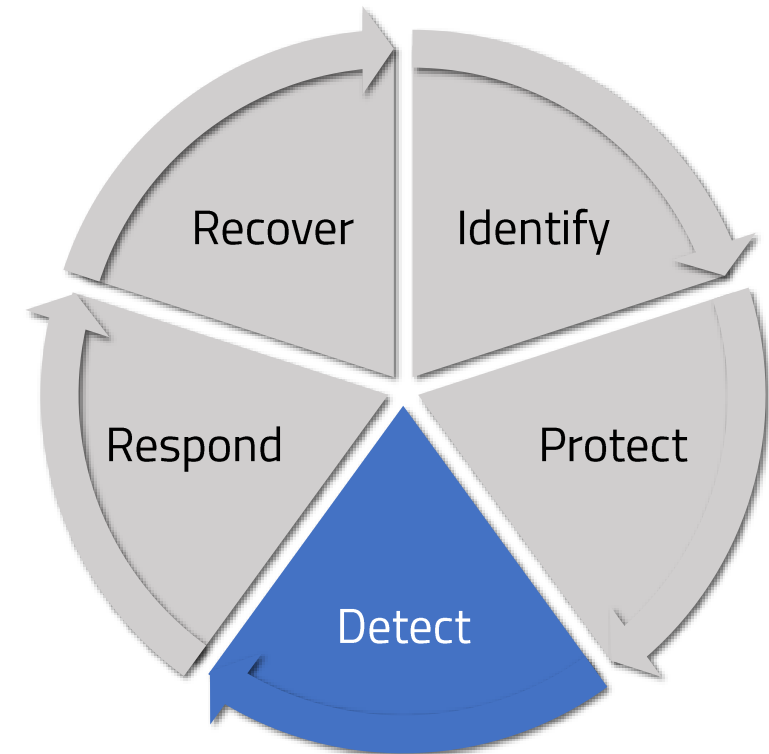


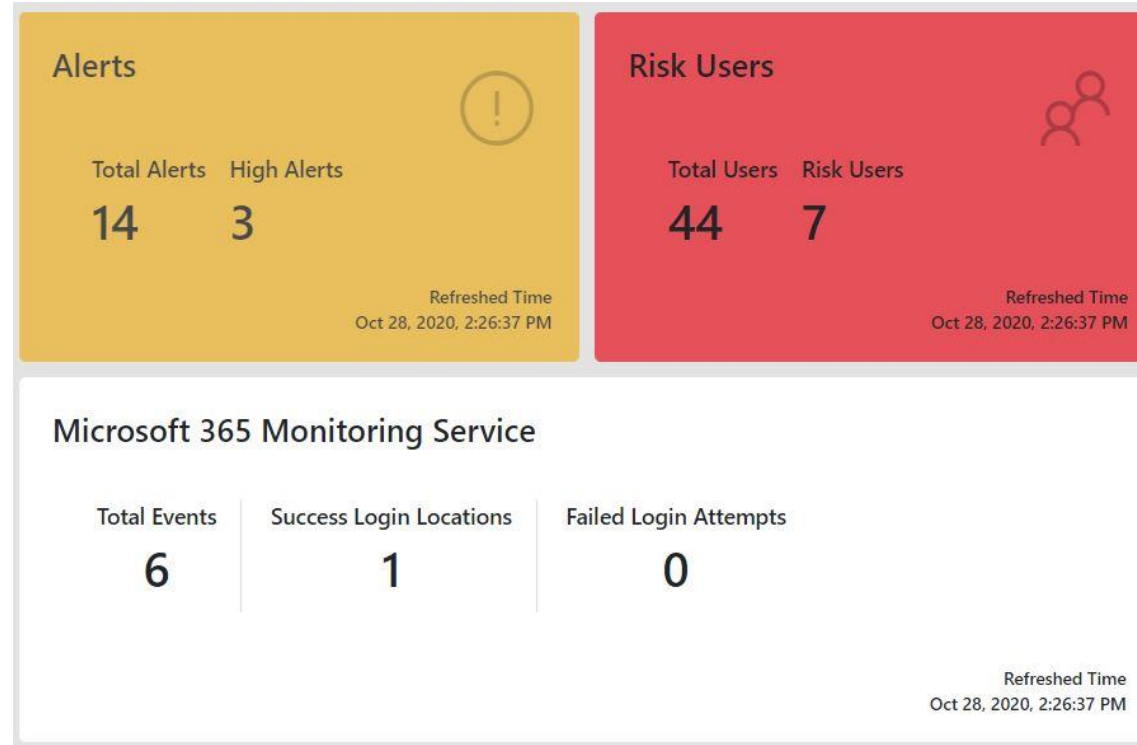
DETECT



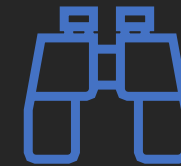
Threat Doctor helps you to define the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner, including:

- Implementing Security Continuous Monitoring capabilities to monitor cybersecurity events
- Ensuring anomalies and events are detected, and their potential impact is understood
- Verifying the effectiveness of protective measures





DETECT

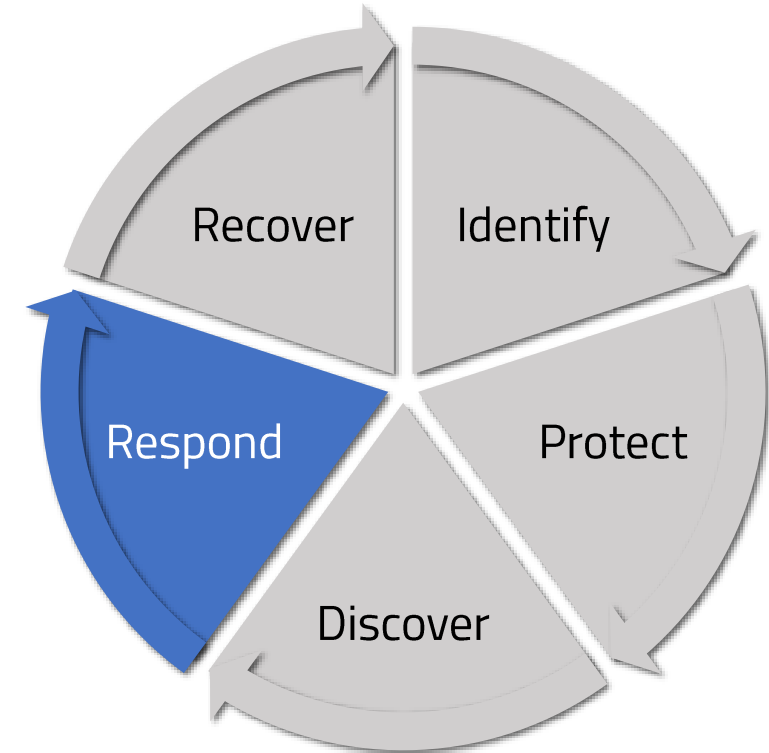


RESPOND



Threat Doctor empowers you to take action regarding a detected cybersecurity incident to minimize impact to your business, by:

- Ensuring Response Planning processes are executed during and after an incident
- Managing communications during and after an event
- Analyzing effectiveness of response activities

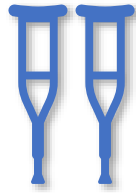


Total Alerts		High Alerts				
14		3				
<input type="text" value="Search Alerts"/>						
Title	Severity	Status	Category	Created Date Time	Provider	View
Unfamiliar Sign-in Properties	Medium	Newalert	UnfamiliarLocation	10/27/20, 1:18 PM	IPC	View
Unfamiliar Sign-in Properties	Low	Newalert	UnfamiliarLocation	10/23/20, 9:49 AM	IPC	View
Activity From Infrequent Country	Medium	Newalert	MCAS_ALERT_ANUBIK	10/21/20, 6:19 PM	MCAS	View
Activity From Infrequent Country	Medium	Newalert	MCAS_ALERT_ANUBIK	10/20/20, 2:04 PM	MCAS	View

RESPOND



RECOVER



Threat Doctor helps you to plan for resilience and the ability to restore services impaired during cybersecurity incidents, by:

- Ensuring your business implements Recovery Planning processes and procedures
- Implementing improvements based on lessons learned
- Coordinating communications during recovery activities



High 15		Medium 10			Low 15	
<input type="text" value="Search"/>						
Title	Severity	Status	Category	Created Date Time	Provider	View
An Analysis Of Godlua Backdoor	Low	Allow	WatchList	10/7/19, 5:12 PM	Azure Sentinel	View
An Analysis Of Godlua Backdoor	Medium	Allow	WatchList	10/7/19, 5:12 PM	Microsoft Defender ATP	View
An Analysis Of Godlua Backdoor	Low	Allow	WatchList	10/7/19, 5:12 PM	Azure Sentinel	View
An Analysis Of Godlua Backdoor	High	Allow	WatchList	10/7/19, 5:12 PM	Microsoft Defender ATP	View
An Analysis Of Godlua Backdoor	Medium	Allow	WatchList	10/7/19, 5:12 PM	Azure Sentinel	View

RECOVER



Threat Doctor: **securing your business**

Updated
threat
landscape

Real time security
threats over the last
30 days

Weakest
links

Identify the most
vulnerable users and
data

Outcome
focussed

Recommended
actions to be taken to
stay safe

Let's get started!