



Measuring Risk at Cloud Speed With AI



Nayeem Islam
VP Product Management – Cloud Security
October 2023



Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.



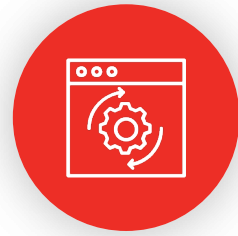
**...You Can't Effectively Detect Threats
In the Cloud Without AI**

The background features a deep blue underwater scene with sunlight filtering through the water's surface, creating a shimmering effect. In the lower right corner, there is a network diagram consisting of several thin white lines connecting various nodes. Some nodes are represented by small white dots, while others are red dots, suggesting a complex data or threat network.

Measuring Risk the Wrong Way, Can lead to breaches



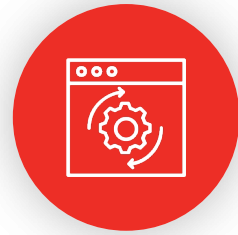
Vulnerability
High Risk



Vulnerability
High Risk



Vulnerability
High Risk



Vulnerability
High Risk



DETECTION BARRIER

Beacon activity

Unauthorized activities

Malware...

Crypto Mining

Suspicion
Communication

Threats Are Hard to Detect



Million new malware samples created everyday
Automated techniques are getting more common



Sandboxes being evaded
And take time to produce results



Signature based detection
too late

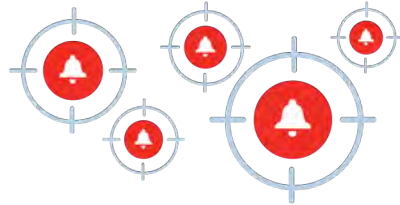


Threat Intelligence needs to be constantly updated for real-time detection

Traditional Signature-Based Techniques Cannot Detect at Cloud Speed



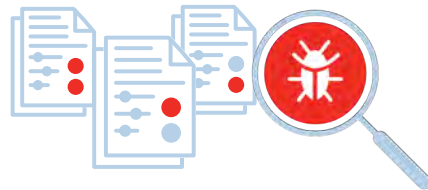
Malware Detection



Known Threat Signatures



Malware sandbox



Execute unknown files in isolated environment

Dynamic Analysis

Classify

Human threat researcher analysis

Create signature

Test signature

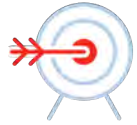
Signature added for next "update"

Almost **12-24 hours** (best case, sometimes days, weeks) before the results of a sandbox analysis are transformed into a signature and downloaded onto a security device

The background of the slide is an underwater scene with sunlight filtering through the water, creating a shimmering effect. In the bottom right corner, there is a network diagram overlay consisting of several thin white lines connecting various points. One point is a white dot, and four others are red dots, arranged in a roughly diagonal line from the bottom left towards the top right.

**...You Can't Effectively Detect Threats
In the Cloud Without AI**

Qualys TotalCloud: Applying Deep Learning AI to Cloud Security



Detects known and unknown threats with **99%+ accuracy**



Detects threats in milliseconds



Self learned, less manual interventions



No signatures, reduced operational overhead



Centrica

Measuring Risk at Cloud Speed with AI

Company

- Founded: 1997
- HQ: London, UK
- Employees: 25,000+
- Industry: Energy and services company

Challenges

- Lack of comprehensive security posture against advanced threats in a multi-cloud environment.
- Accurately identifying threats
- No real-time visibility
- Complex infrastructure with multiple point products

RESULTS



Protected entire multi-cloud infrastructure with a **single unified cloud hardening and real-time security**

>99%

Detected **known** and **unknown** threats with the **highest accuracy**

1 sec

Real-time detection of threats at **sub-second** speed



Seamless integration with existing tools enhanced productivity and provided higher ROI



We selected Qualys TotalCloud because of its forward-looking approach to securing multi-cloud environments with unparalleled threat detection capabilities based on advanced deep-learning AI technology.



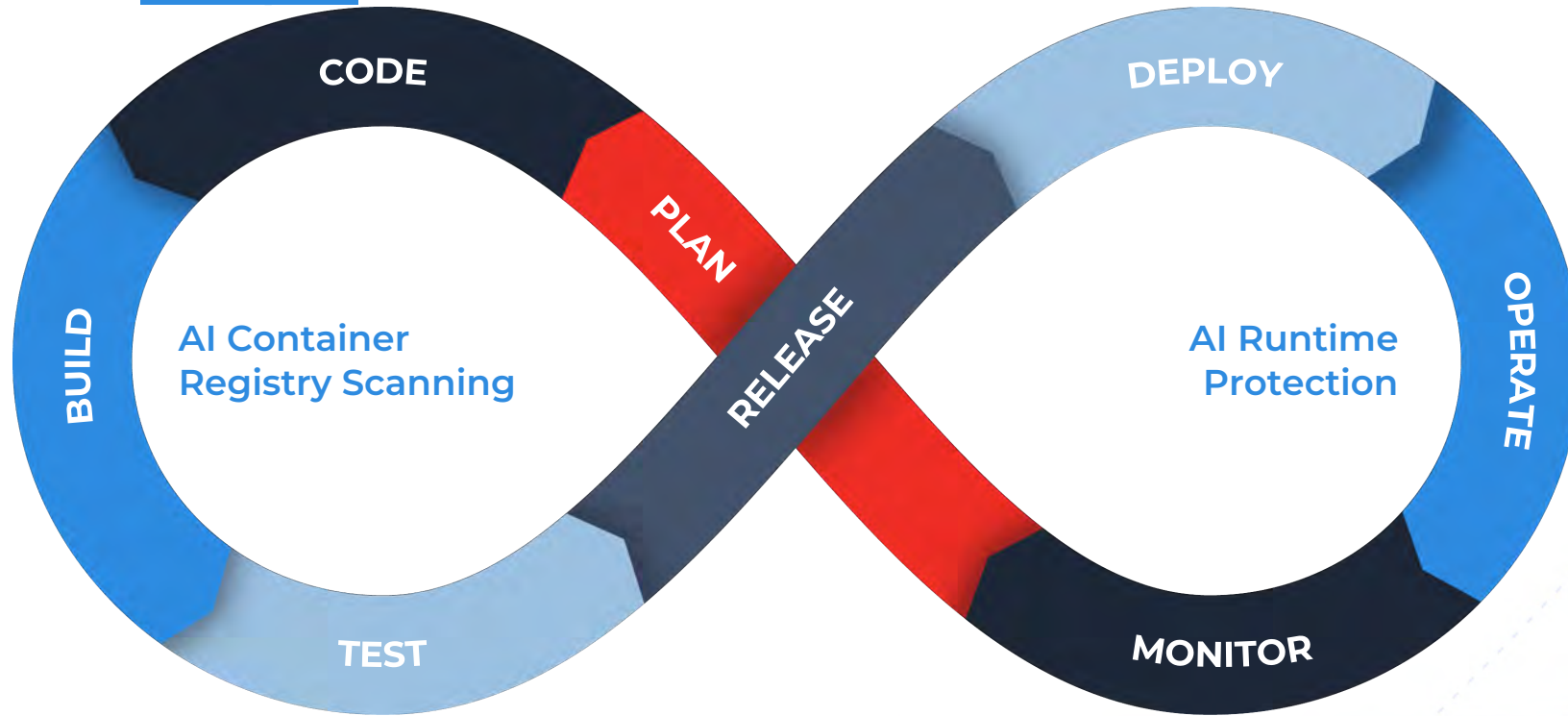
Mark Wootton

Head of Threat and Vulnerability Management

centrica

Qualys TotalCloud Secures Workload from Build to Runtime

Unique End-to-end AI-based Threat Detection



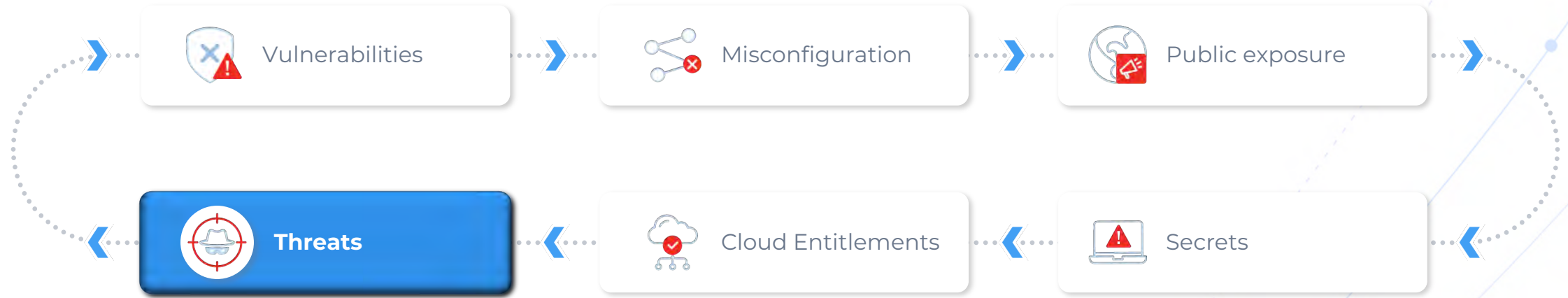
AI Container Registry Scanning

- Malware

AI Runtime Protection

- Malware
- Unauthorized communications
- Suspicious communications
- Cryptomining
- C2C (Beaconing)

TruRisk Insights: Detecting Threats is Critical



Critical vulnerability with a known exploit found on Publicly Exposed VM with **unauthorized communications**

Publicly exposed asset, Vulnerability and **C2 beaconing to malicious IP**

Malware and vulnerabilities detected on containers

Container with **Malware** and secrets exposed

Qualys TotalCloud Container Security Detects **Malware Variants**

Qualys Express | Qualys Cloud Platform

Inventory Details: i-0ed9a98cfd94ed38 | More Details

Security Threats

MALWARE (5) | Command & Control (6) | CRYPTOJACKING (4) | UNAUTHORIZED ACTIVITY (31) | SU...

TROJAN (1) | RANSOMWARE (3) | UNKNOWN (1)

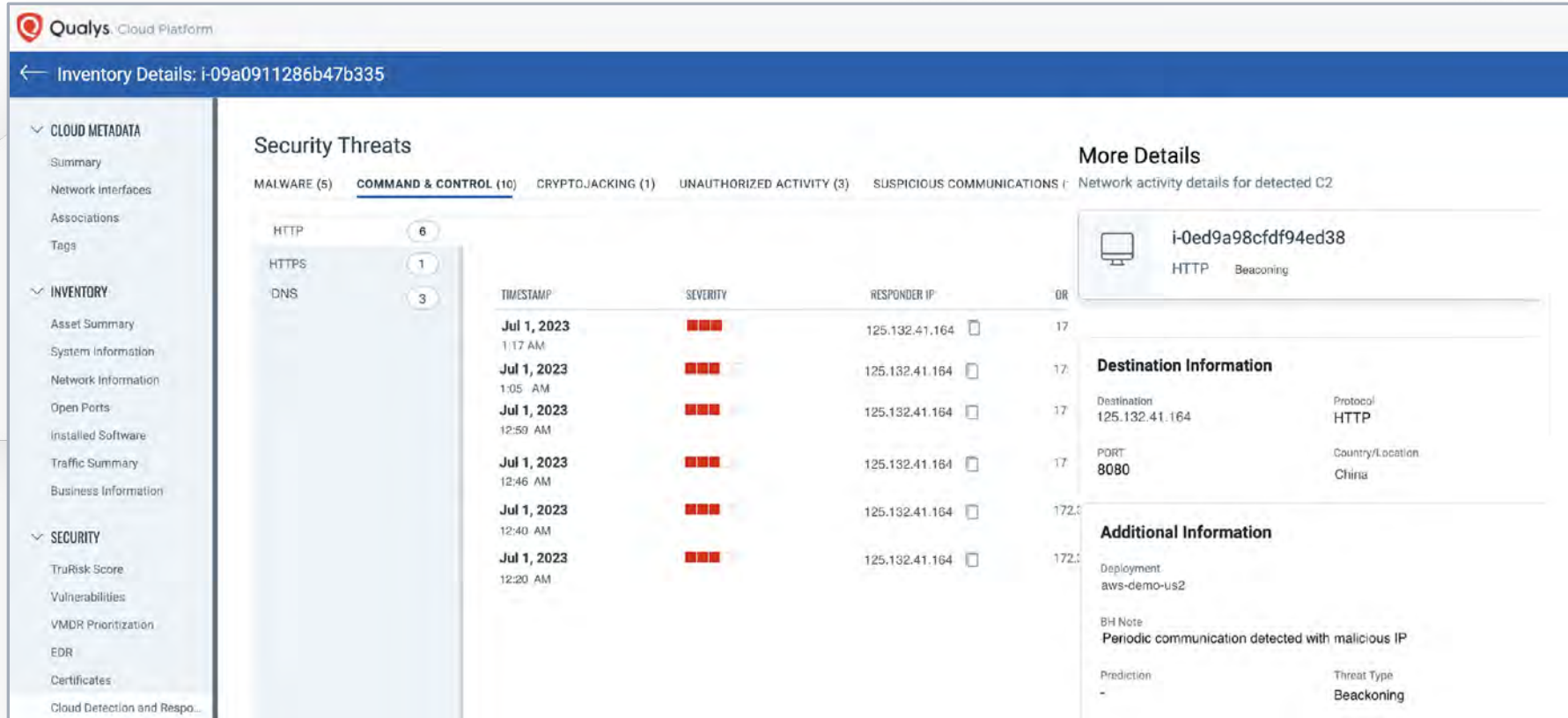
ILY	THREAT CATEGORY	SOURCE IP
	ransomware	175.6.176.117
	ransomware	125.132.41.164
	ransomware	175.6.176.117

Different Hash, Similar behavior

- Hash 1:** 44c0774f53ab5071ee2969c5e44df56b13f5047e3fca6108375e6055998b86f2
- Hash 2:** cd8ad31e1d760b4f79eb1c3d5ff15770eb88fa1c576c02775ec659ff872c1bf7
- Hash 3:** ad8d1b28405d9aebae6f42db1a09daec471bf342e9e0a10ab4e0a258a7fa8713

Indicator	Description	Severity
System Information Discovery		
UpdateProcessPersistenceonlogon	Update Service information to persist the process across logon	Informative
UpdateProcessPersistenceonboot	Update Service information to persist the process across boot	informative
Virtualization / Sandbox Evasion		
ProcessDisableVMEEnv	Detect VME to disable core function	informative

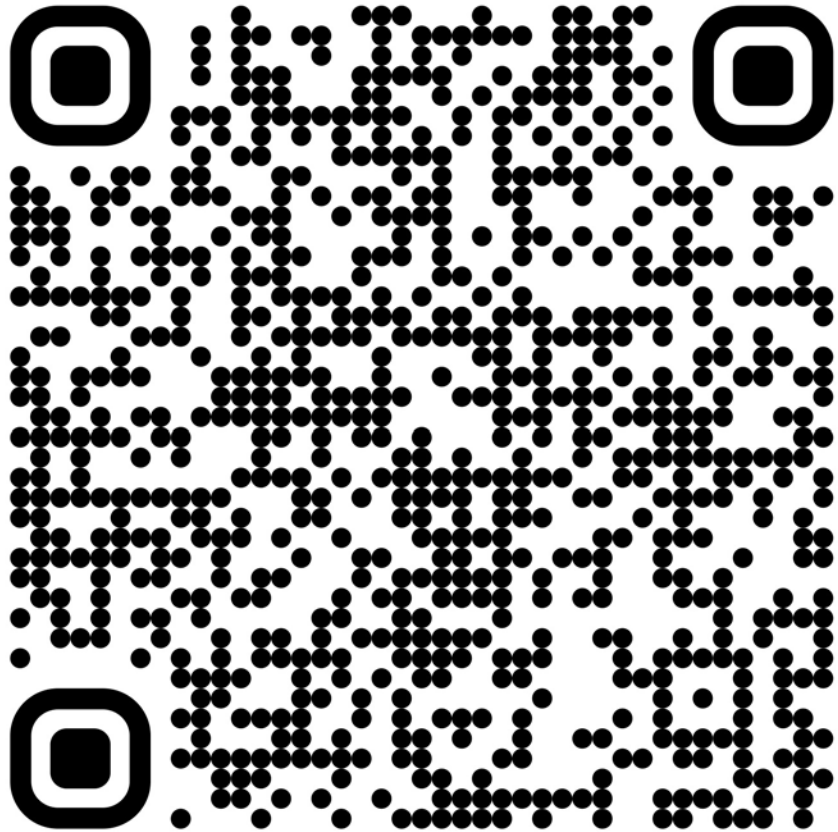
Qualys TotalCloud detects Stealthy Beaconing Attacks



The screenshot displays the Qualys Cloud Platform interface for an inventory item with ID i-09a0911286b47b335. The main section is titled "Security Threats" and shows a list of detected threats. The "COMMAND & CONTROL" category is selected, showing 10 threats. The table below lists several threats, all of which are categorized as "Beaconing" and have a severity of "High".

Protocol	Count	Timestamp	Severity	Responder IP	Port
HTTP	6	Jul 1, 2023 1:17 AM	High	125.132.41.164	172.17.0.1
HTTPS	1	Jul 1, 2023 1:05 AM	High	125.132.41.164	172.17.0.1
DNS	3	Jul 1, 2023 12:59 AM	High	125.132.41.164	172.17.0.1
		Jul 1, 2023 12:46 AM	High	125.132.41.164	172.17.0.1
		Jul 1, 2023 12:40 AM	High	125.132.41.164	172.17.0.1
		Jul 1, 2023 12:20 AM	High	125.132.41.164	172.17.0.1

The "More Details" section provides information for a specific threat (ID: i-0ed9a98cfd94ed38). It identifies the threat as "Beaconing" over "HTTP". The destination information shows the destination IP as 125.132.41.164, protocol as HTTP, and port as 8080. The country/location is listed as China. The additional information section notes the deployment as "aws-demo-us2" and includes a "BH Note" stating "Periodic communication detected with malicious IP". The prediction is listed as "-" and the threat type is "Beackoning".



Book a Meeting with me and my team

- Get free health check for your cloud environment
- Get tailored recommendations to de-risk your cloud environment

Thank You

