CSA | AI Summit at RSAC 2024

Harnessing AI for End-to-End Cloud Security: From Development to Runtime

PRESENTED BY

Qualys

Nayeem Islam

VP Product Management – Cloud Security

… As cloud adoption accelerates…

Leading causes cloud breaches

Vulnerabilities, Misconfigurations, and Malware

Most Misconfigured Controls Across Major CSP

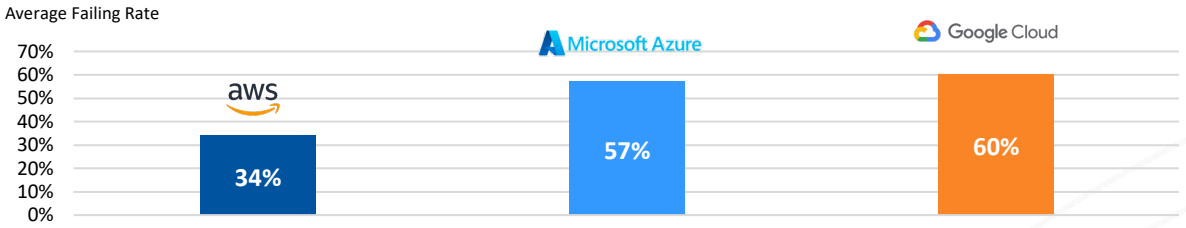
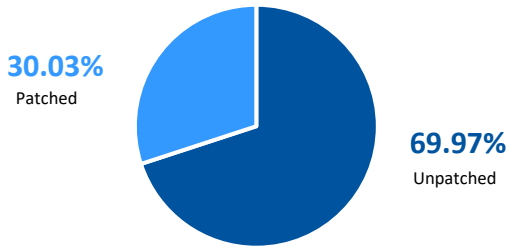


Figure 1: Average Failure Rates for AWS, Azure, and GCP for CIS Benchmarks

High Unpatched Rate



136 Days

Average Remediation Time of Log4Shell

CIS benchmarks controls across major CSP's are not meet 50% of the time on average

70% of Log4Shell vulnerabilities have still not been fixed, since last 2 years

Crypto mining malware is a growing threat

CIS = Center for Internet Security; CSP = Cloud Service Provider; AWS = Amazon Web Services; GCP = Google Cloud Platform

Source: Qualys TruRisk 2023 Cloud Insights Report

Misconfigurations And Vulnerabilities Are Important

Check for misconfigurations, like assets exposed to the internet and secrets that should be protected

Get an understanding of the extent of vulnerabilities and their criticality

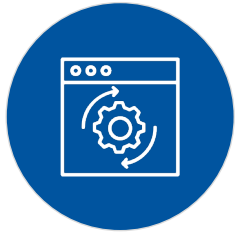
Make sure best practices are followed

Remediate based on priorities

…You can't effectively measure risk
in the cloud without detecting threats

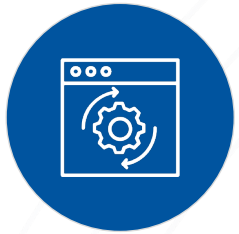
Measuring risk the wrong way, can lead to breaches

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

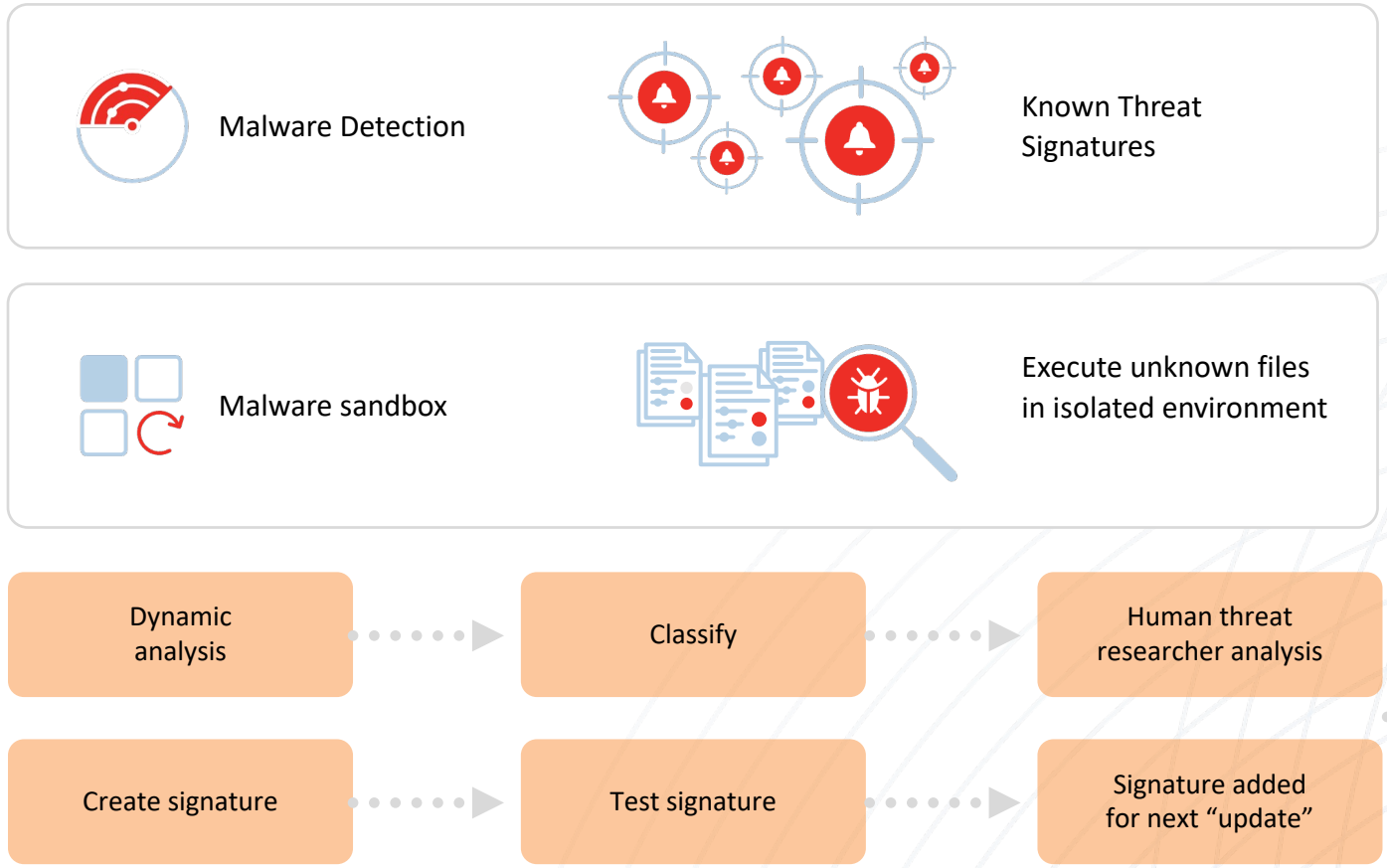
Million new malware samples created everyday. Automated techniques becoming more common

Sandboxes being evaded and take time to produce results

Signature-based detection is too late

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

Traditional signature-based techniques cannot detect at cloud speed



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

…Generative AI will accelerate number and sophistication of attacks

Automated attacks accelerate

Phishing Attacks

LLMs generate convincing emails mimicking trusted sources to trick users into divulging sensitive information.

Social Engineering

LLMs assist attackers in crafting persuasive messages, social media posts, or chat interactions to manipulate targets.

Malware Creation

LLMs aid in generating code snippets, camouflage techniques, or obfuscation methods to create sophisticated malware.

Automated Vulnerability Exploitation

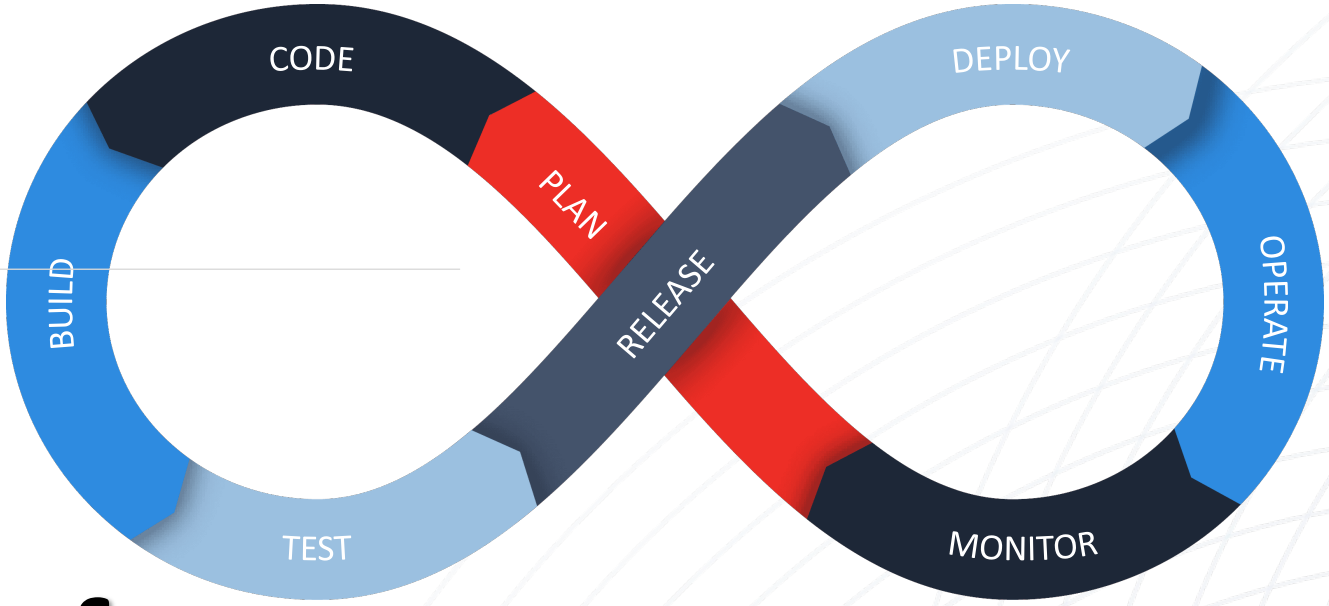
LLMs automate the process of identifying and exploiting vulnerabilities in software or networks.

…You can’t effectively detect threats in the cloud without AI

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

Cloud Environments are Difficult to Protect



Shift Left

Shift Right

…AI will be used extensively for defense

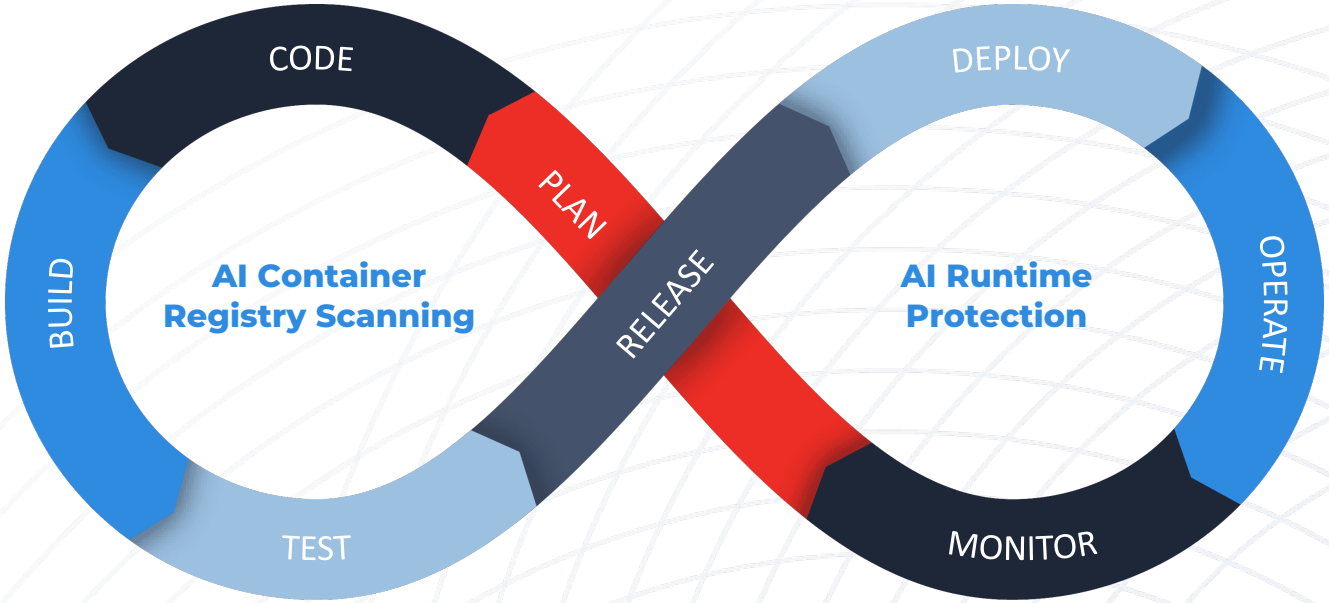
AI Detection must be end to end -- from build to runtime

AI Container Registry Scanning

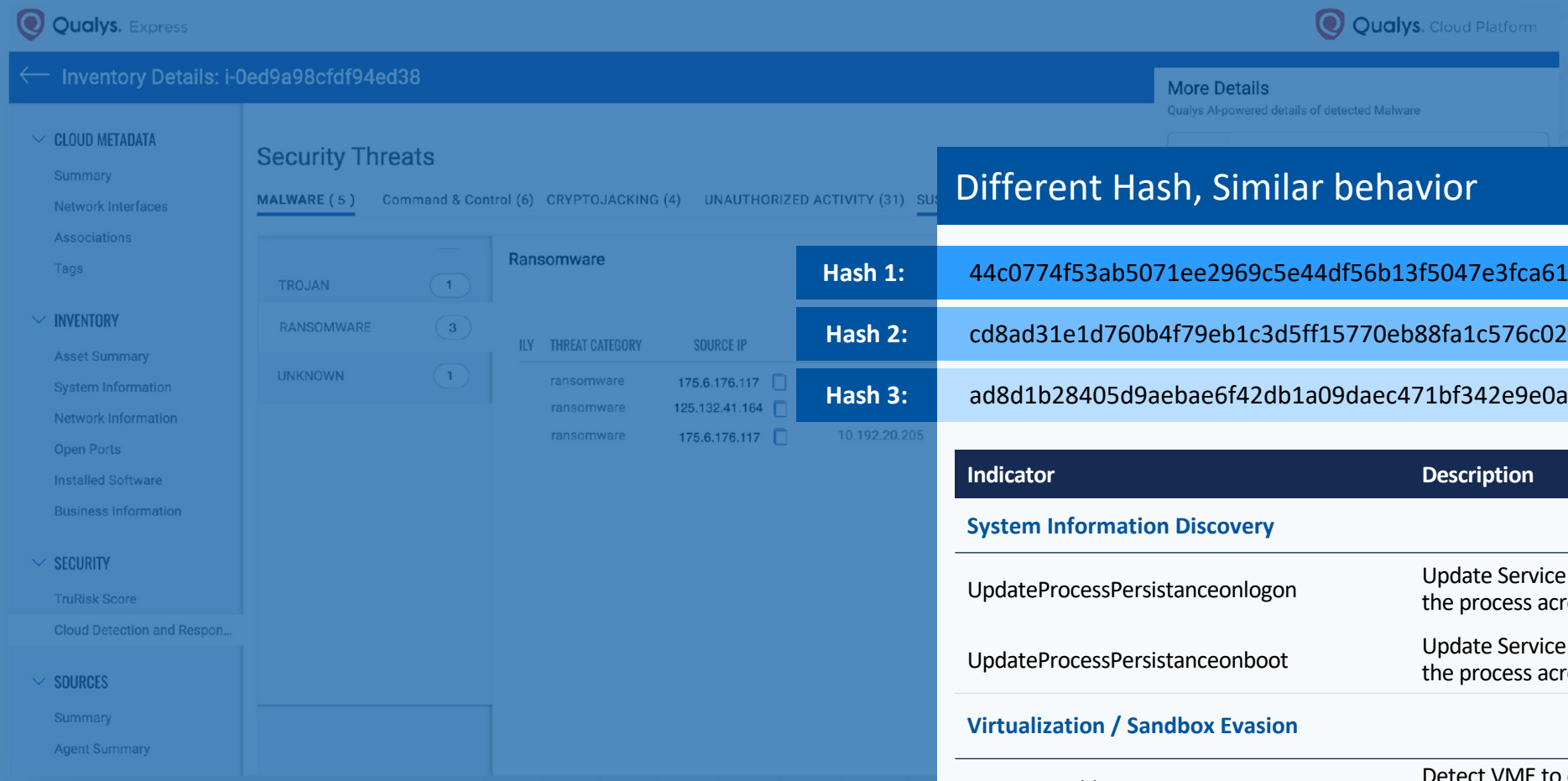
- Malware

AI Runtime Protection

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



Container Security Detects Malware Variants

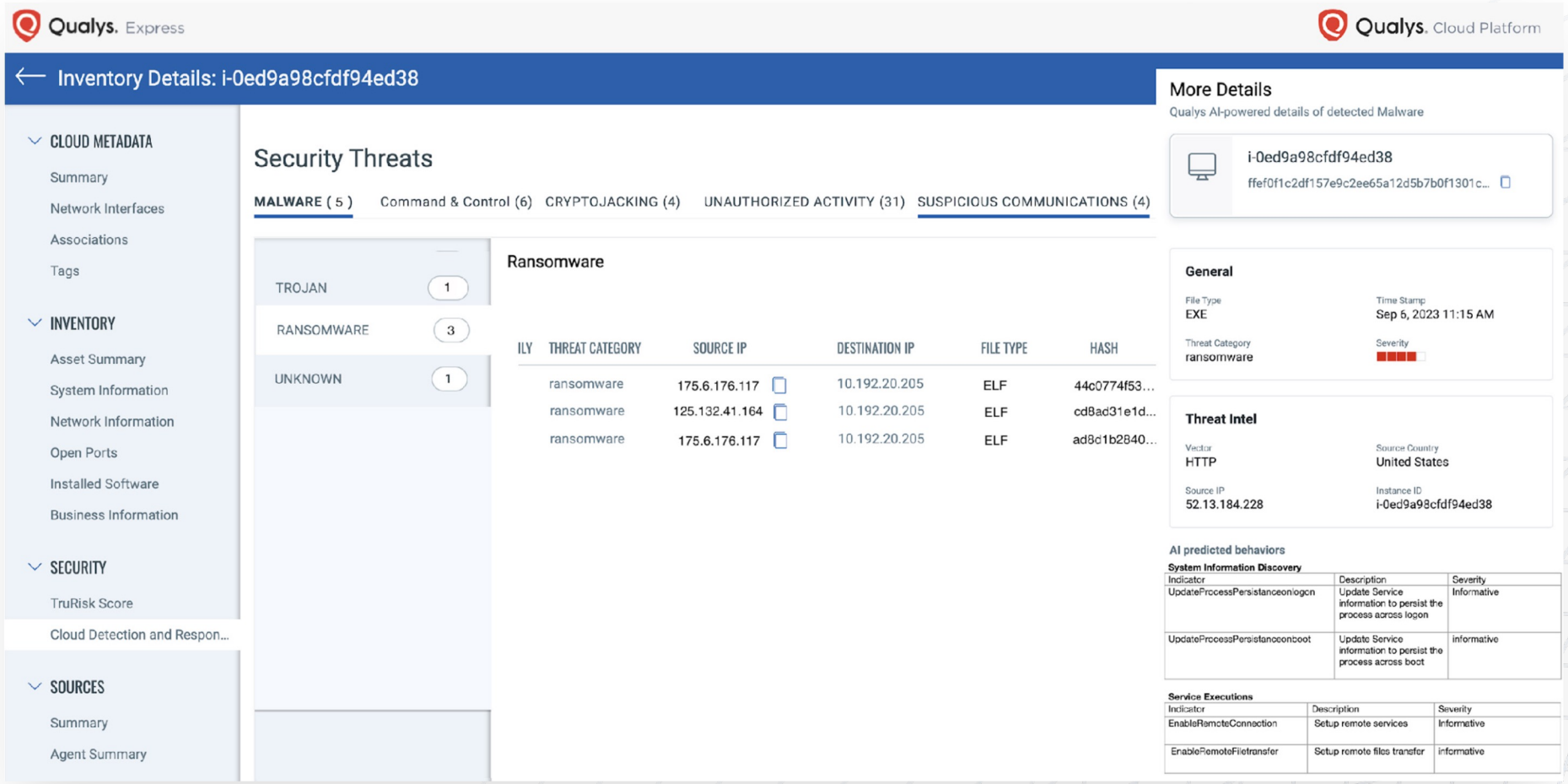


Different Hash, Similar behavior

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

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

Detect Stealthy Beaconing Attacks



What the future holds

More and more automation in attacks

Generative AI will change the game

However the good news is that

Generative AI will be used extensively in defense

Threat Detection, SOAR, Remediation and more

Many areas will be automated and improved

Qualys®

Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.

To learn more about how AI can help you protect your Cloud

Book a meeting with my team

Thank You