Ensuring software integrity with comprehensive threat detection analysis

Overview

Vulnerabilities in the software supply chain have

uwr rqtvu" o qtg"vj cp"6 : 22"ˆ0ng"v{ rgu"kpcwfkp i "LCXC."
ˆ0PGV."R{vj qp." o ceQU."Nkpwz."CRM."cp f "Fqemgt"k o c i gu0

Threat Detection also generates comprehensive software bills of materials to comply with emerging regulatory requirements to provide transparency of software composition.

Mg{"Dgpg"0vu

- Reduce risk of compiled software containing malware, vulnerabilities or secrets
- Centralize control by making threat detection a part of your software supply chain practices
- Increase trust of your software by taking a policy driven 'go/no-go' approach to software release based on priority of risks discovered
- Meet emerging regulatory requirements for software bills of materials

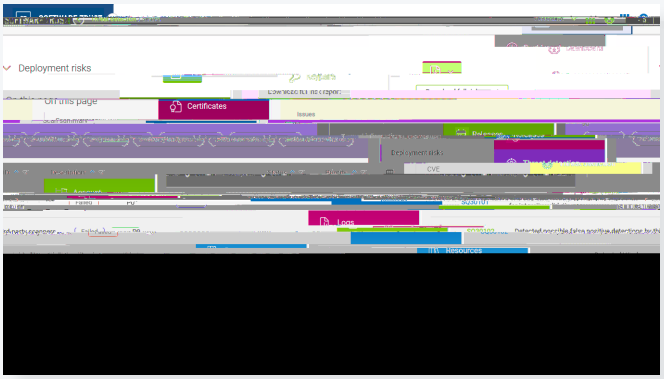
Mg{"Hgcvwtgu

Detect threats and vulnerabilities in software binaries
Malware, software tampering, CVE detection, secrets leakage, and other vulnerabilities can be detected even for binaries that contain third party open-source or commercial code.

Minimize possibility of tampering by using the same yqtm"0qy"cp f "rncvhqt o "vq"uecp"{qwt"uqhvy ctg"dghqtg"{qw" securely code sign it.

Fast and automated threat detection
Easily insert threat detection into CI/CD pipelines for any DevOps platform. Works for a variety of platforms and binary types.

Report on, and analyze, complex software composition
Uqhvy ctg"dkn"qh" o cvgtkcnu"*UDQO+"cp f "tkum"xwnpgtcdknkv{" reports are available to address emerging regulatory requirements such as those from the President's Executive Order 14028, M-22-18.



Threat Detection scans software binaries to ensure that malware and other vulnerabilities are not rtgugpv"cp f "i gpgtcvgu"UDQOu"cp f "tkum"cpcn{uku" reports.