ActiveEye Cloud℠

SECURITY AT THE SPEED OF BUSINESS

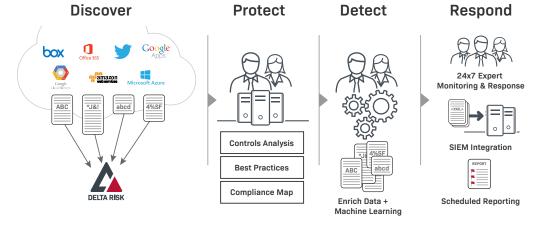**DELTA RISK**
A CHERTOFF GROUP COMPANY

Most organizations are rapidly adopting SaaS applications like Office365, Google Apps, Salesforce and more to run their business. Many are also leveraging AWS, Azure, or Google Cloud Platform to do research, develop new applications, or scale production workloads. Although businesses are benefiting from expanded IT capabilities, there's been an increase in data breaches due to mis-configuration of cloud services. Configuring these services often falls to developers and application owners who lack an understanding of best practices for cloud security.

To successfully adopt cloud and enable your teams to move at competitive speed, you need visibility into who is accessing your key enterprise cloud services, what activity is taking place, and how these services are being administered. You need a security partner with deep cloud security expertise. Delta Risk has you covered with ActiveEye Cloud, ActiveInsight cloud security assessments, and ActiveResponse services.

Visibility

Get full visibility into activity in all your cloud environments and accounts. Let your teams develop while having confidence there are no unknown risks.

Policy Monitoring

Apply best practice controls to your configuration and usage of cloud services. Arm your teams with best practices to quickly find misconfigurations.

Anomaly Detection

Detect malicious use from inside or outside your organization. Use advanced analytics to detect inappropriate use of resources from internal or external attacks.

Discover — **Protect** — **Detect** — **Respond**

Controls Analysis
Best Practices
Compliance Map

Enrich Data + Machine Learning

24x7 Expert Monitoring & Response
SIEM Integration
Scheduled Reporting

Get the people, process, and technology you need so you can focus on moving to the cloud instead of worrying about security.

Simple Deployment
10 minutes to full visibility, just a simple connection to cloud services via API

Integrate with Existing Security
Integrate simply with existing security SIEM for a complete view

24x7 Ops Support from an All-American Team
U.S.-based SOC monitors your activity around the clock

Analytic Examples

ACCESS

Suspicious Logon
Evaluation of device information, IP, location, and service accessed

Bruteforce Logon Attempt
Failed attempts over time, evaluation MFA failure vs PW

API Commands
API execution from known malicious IP

ADMINISTRATION

Unusual Administration
Unusual commands issued by administrators

Unusual Instance Start
Use of resources in a way not typical for a given admin

Disable Logging
Disabling of logging on compute or database instance

USER ACTIVITY

Attempted Privilege Escalation
Excessive attempts to access unapproved resources

Unusual Velocity of File Access
Access or downloads that violate user or peer norms

Communication with Known Malicious IP
File transfer or API access from known malicious IP

NETWORK

Command and Control
Communication outbound to known malicious IP

Use of Sensitive External Ports
Two-way connections over SSH, RDP, FTP

Unusual Traffic Pattern
Traffic flows that deviate from typical patters

Is ActiveEye Cloud Right for You?

▸ Do you need to know if stolen user credentials are used to access your Office365 applications?

▸ Should you identify when a user downloads an unusual number of files from Google Drive?

▸ Do you need to ensure security configurations in AWS accounts follow best practices?

▸ Should you be able to identify bitcoin mining servers started in an unused Azure region?

About Delta Risk LLC

Delta Risk LLC, a Chertoff Group company, provides customized and flexible cyber security and risk management services to government and private sector clients worldwide. Founded in 2007, we are a U.S.-based firm offering a wide range of advisory services as well as managed security services. Our roots are based in military expertise, and that background continues to drive our mission focus. We are passionate about keeping our clients safe and secure.

@deltarisk   /delta-risk-llc   /deltariskcyber