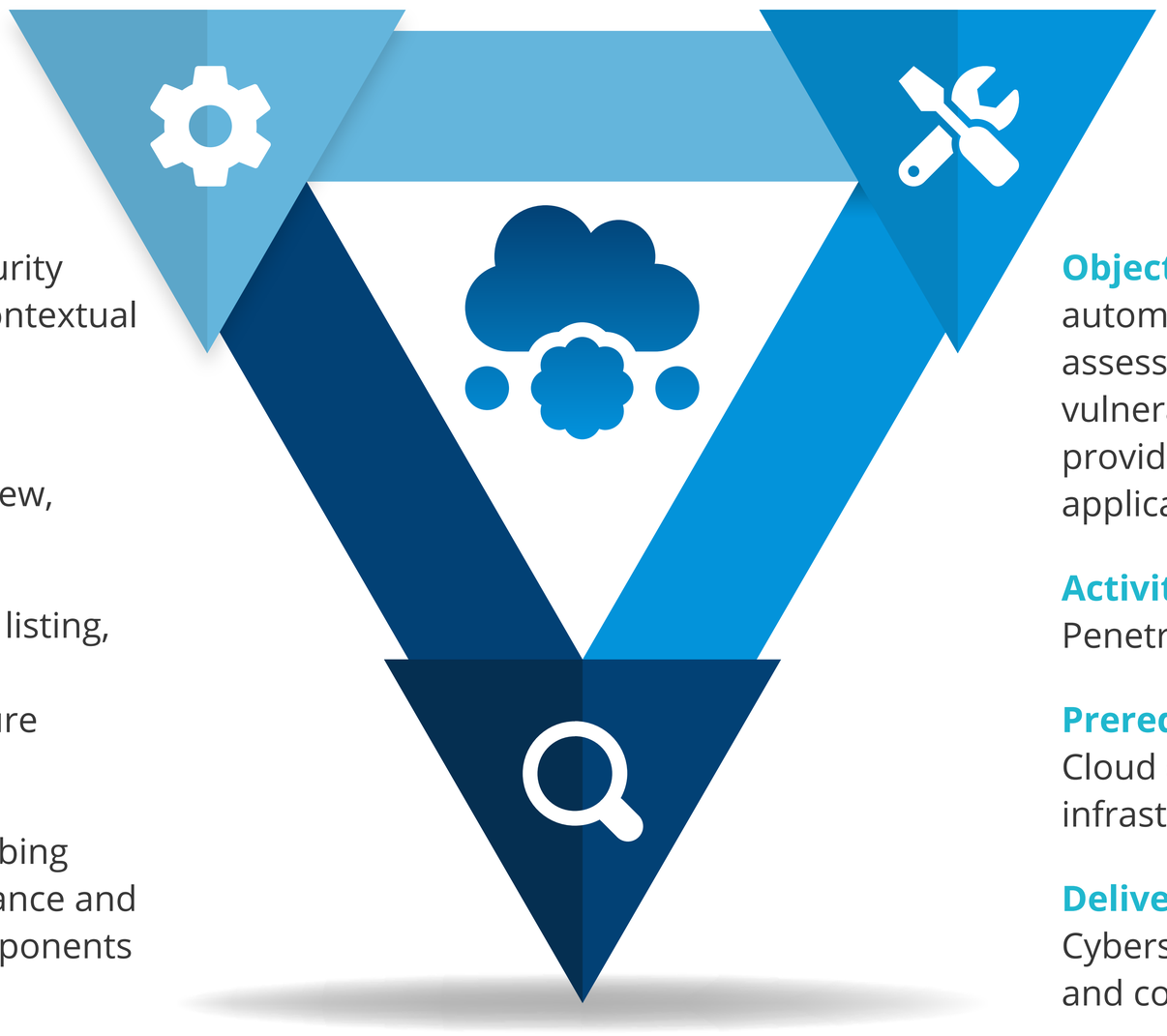
ENTERSOFT SECURITY

MANAGED CLOUD SECURITY

Comprehensive, Continuous and Transparent Cloud Security

Traditional on-demand security assessments, remediation implementation and risk management activities are slowing cloud application deployments and impeding companies achieve their full potential. Entersoft's Managed Cloud Security services enable your business transform your service offerings while we constantly manage application security controls and apply AI driven solutions to continuously monitor your Cloud applications.



Security Controls Engineering

Objective: Constantly identify security control deficiencies and provide contextual recommendations for the Cloud applications portfolio

Activities: Cloud Architecture Review, Configuration Review

Prerequisites: Cloud components listing, custom components integration architecture and cloud infrastructure architecture

Deliverables: Threat model describing controls recommendation, compliance and Cybersecurity risks and Cloud components configuration recommendations

Cybersecurity Assessments

Objective: Implement a combination of automated and manual Cybersecurity assessments to identify security vulnerabilities, assess cyber risk, and provide recommendations for Cloud applications portfolio.

Activities: Vulnerability assessments, Penetration testing

Prerequisites: Operational Application, Cloud components listing and Cloud infrastructure characteristics

Deliverables: Compliance and Cybersecurity risks, security vulnerabilities and contextual recommendations

Adaptive Security Monitoring

Objective: Continuous monitoring of security controls to identify, analyze, and report security events, their impact, and contextual recommendation for Cloud applications portfolio

Activities: Utilize AI-driven solution for continuous monitoring of cloud applications and user interactions

Prerequisites: Operational application, cloud components listing and cloud infrastructure characteristics

Deliverables: Immediate reporting of security incidents, events and risky activities. Provide critical insights on top security risks and most risky users

info@entersoftsecurity.com

www.entersoftsecurity.com

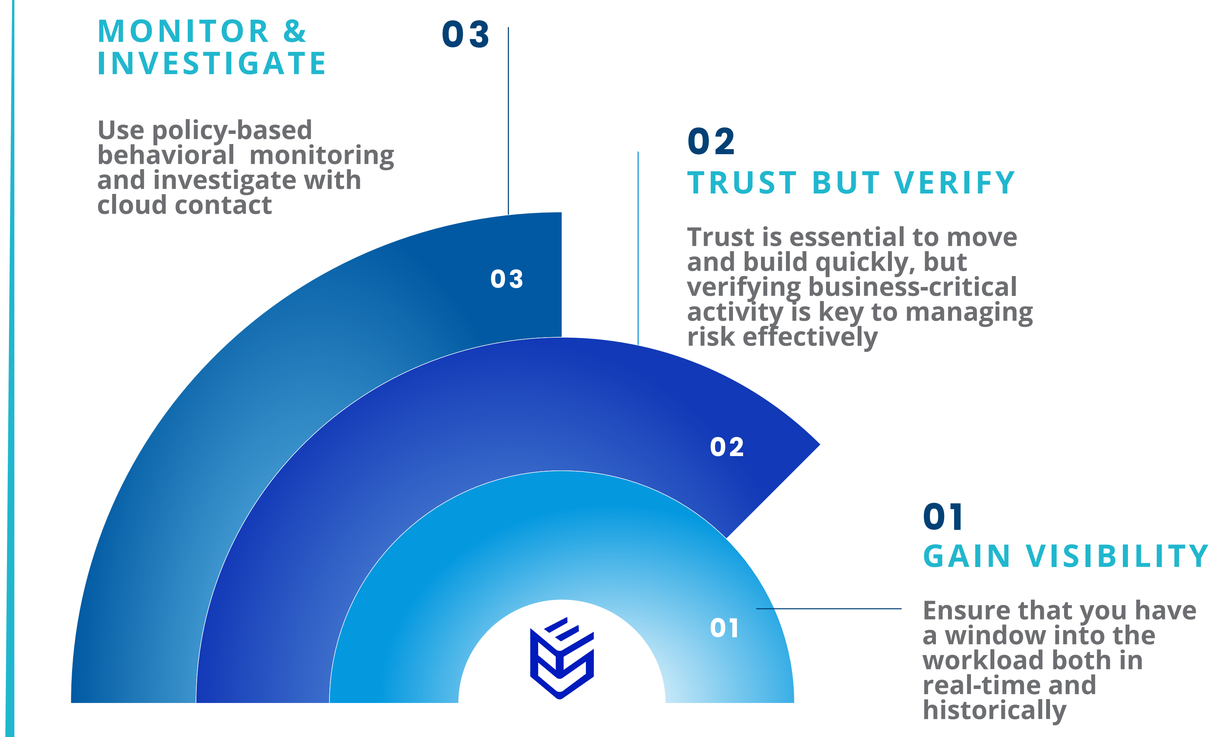
CLOUD ARCHITECTURE REVIEW

OVERVIEW

Cloud Architecture review constantly identifies security gaps within the cloud application environment and provides contextual recommendations to enable organizations prioritize and mitigate security risks.

THREAT MODELING

As part of architecture review, threat models are produced to provide the possible attacks scenarios that can adversely impact Cloud application security posture & provide contextual security controls guidance to respective technology & business stakeholders.



SUMMARY

As with all coherent security strategies, cloud security can seem dauntingly complex, involving many different aspects that touch all parts of an organization.

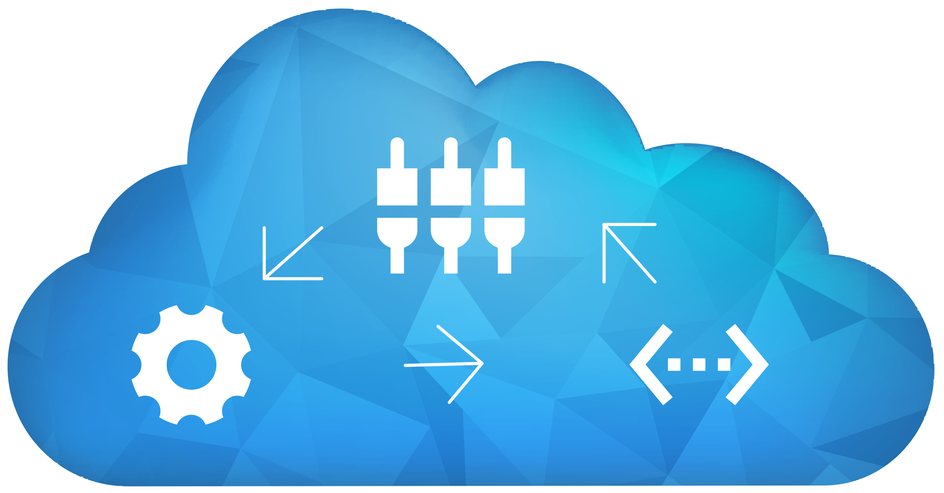
CIOs and their teams need to plot effective management strategies as well as understand the implications for operations and technology. In this section, we outline the key considerations.

SECURITY CONSIDERATIONS

01 Session Management
02 Access Controls
03 Input and Output Validations
04 Cryptography
05 Errors, Logging and Auditing
06 Data protection and Privacy
07 Communications
08 Malicious Software
09 Business Logic
10 Secure File Upload
11 API Architecture
12 Configuration

info@entersoftsecurity.com

CLOUD CONFIGURATION REVIEW



REVIEW INVOLVES

1. Authentication and Access Control Management

- Identity Access Management (IAM) Policy
- Users/User Groups evaluation based on Principle of Least Privilege
- Authentication best practices (MFA, Password Policy, Periodic Key)

2. Cloud Networking

- Isolation between multiple workloads
- Effective network security groups and ACLs
- Appropriate access controls of the users
- Secure communication within and outside the cloud

3. Cloud Compute

- Isolation between multiple workloads
- Effective network security groups and ACLs
- Appropriate access controls of the users
- Secure communication within and outside the cloud

4. Cloud Storage

- Data at rest protection
- Data in transit protection
- Unauthorized access to the files stored

5. Logging and Monitoring

- Review configurations of instances/virtual machines
- Appropriately restrict access to sensitive workloads

6. Additional Services

- Database Services
- Server-less functions
- Backup and Disaster Recovery

OVERVIEW

Configuration Review constantly monitors security controls configuration and identifies any misconfigurations that could allow attackers gain unauthorized access to the organization's cloud application environment or could use the cloud environment to perform malicious activity.

We typically require read only access to your cloud environment to enable our automation technology and security experts to constantly monitor and verify the cloud configurations against industry best practices and standards.

info@entersoftsecurity.com

PENETRATION TESTING

OVERVIEW

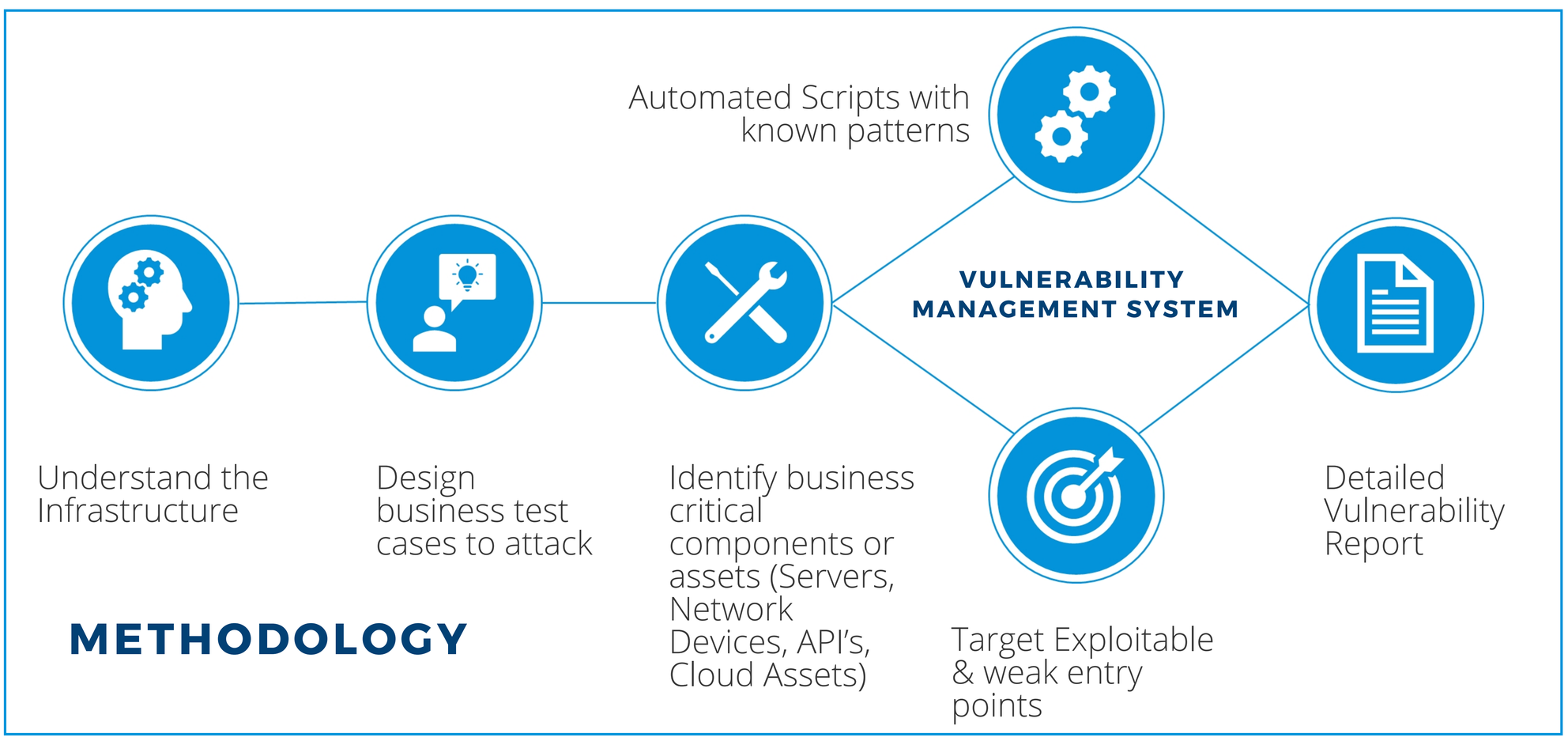
Application level vulnerabilities and misconfigurations are not the responsibility of your Cloud Service Providers (CSPs) as portfolios of cloud applications are developed, built and deployed by your development and operations teams. Applications hosted on your cloud environments such as Web, Mobile, APIs undergo the same level of scrutiny from hackers as would your on-premise applications. Remember, Security is a shared responsibility between your CSP and your organization.

We perform both **manual** and **automated** analysis on your applications to identify vulnerabilities and later demonstrate exploitation impact on your Cloud applications

OUR APPRAOCH

- Automated and Custom scripts combined with Open Source tools
- Multi-level information extraction regarding target application(s)
- Testing target applications for common vulnerabilities
- Dynamic screen capture of all checks performed
- Re-validation of results and further tool enhancement

METHODOLOGY

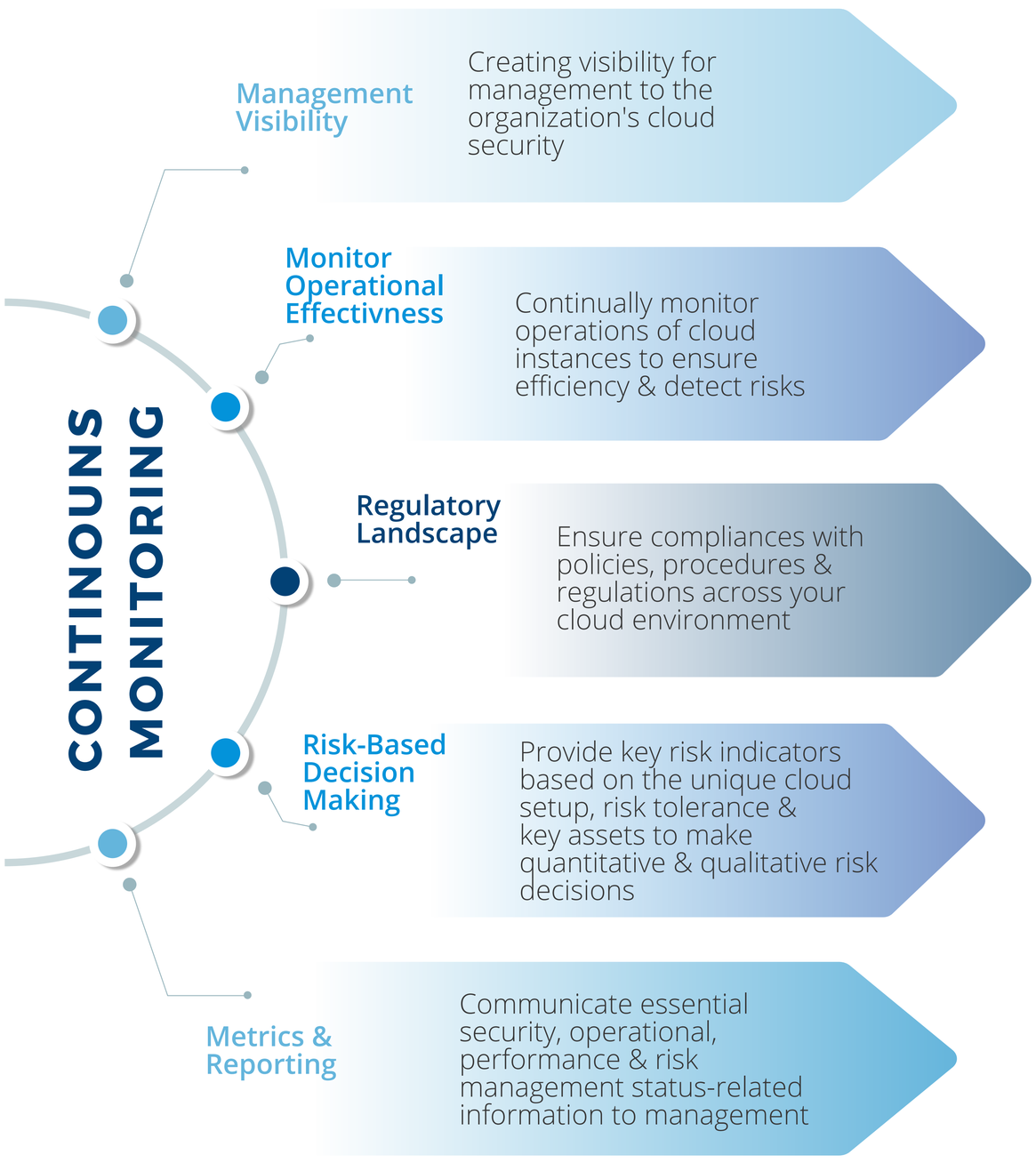


info@entersoftsecurity.com

ADAPTIVE SECURITY MONITORING

OVERVIEW

Our goal is 24/7/365 monitoring of the client's cloud application portfolio to provide real-time threat information about malicious actors from both external and internal to the network. Our real-time threat information includes immediate actions to be undertaken by the client and risk mitigation guidance after Security Operations Center's threat analysis.



OUR APPROACH

Cloud Component Discovery: Know who and what is connected to your cloud instances at all times

Vulnerability Assessment: Identify coding & configuration issues across your cloud models

Intrusion Detection: Continuously monitor your cloud workloads to detect anomalies and attacks like malware, ransomware, and brute force authentication.

Behavioral Monitoring: Our team with the help of correlation engine enables highly granular personal user behavior profiles to more accurately identify risky activity in cloud apps

Orchestrated Incident Response: Quickly contain and mitigate discovered threats across your on-premises and cloud environments, and your SaaS applications

SIEM Log Management & Reporting:

Aggregate, retain, and enable evaluation of security event data in your cloud ecosystem

Our reporting consists of

- Attack methods
- Related events source and
- Destination IP addresses

As well as incident response remediation recommendations

Integrated Threat Intelligence: Threat intelligence is gathered from our research team and multiple repositories which includes correlation directives, vulnerability signatures, indicators of compromise, guided threat responses, and more to provide a broad view of threat actors, attacker techniques and effective defenses.

info@entersoftsecurity.com

OUR MARK

FINTECH OF THE YEAR &
EXCELLENCE IN APP SECURITY

EXCELLENCE IN
CYBER SECURITY

BEST INNOVATION IN
CYBER-SECURITY &
ANTI-FRAUD

SUPERCHARGER
FINALIST 2017

ANZIA
FINALIST

OUR CERTIFICATIONS

KEY CLIENTELE

ENTERSOFT SECURITY

info@entersoftsecurity.com

AUSTRALIA | US | INDIA | HONG KONG | ISRAEL | MEXICO