

# CISO AS A SERVICE

Testing, Advisory, Detection, Monitoring & Response



## BENEFITS

- Access to security experts 24x7
- No capital investment
- Lower cost to delivery
- SLA based service delivery
- 24x7 incident detection & monitoring
- Technical guardianship support to deliver in-house services
- Monthly board-level reporting

## AT A GLANCE

Few enterprises can afford a dedicated security team headed by a CISO (Chief Information Security Officer). CISO as a Service enables your organisation to have all the benefits associated with a full security team, but without the capital outlay.

Our service provides a portfolio of security testing, 24x7 security monitoring, incident response and advisory services to not only defend against security breaches but to demonstrate compliance. We place our technology, skills and experience at our customers' disposal through a single technical advisory manager.

CISO as a service combines strategic support tasks with more routine or tactical services to deliver:



## WHAT IS INCLUDED

SECURITY TESTING	SECURITY ADVISORY	INCIDENT DETECTION & MONITORING	INCIDENT RESPONSE
Vulnerability Management	Compliance Audits (ISO27001, SANS20)	24x7 SIEM & SOC Monitoring	Security Incident Response
Penetration Testing	Security Road Mapping	Advanced Behavioral Analytics	Malware Remediation
Web Application Security Testing	Firewall Management	Active Honeypot Defense	Forensics

### SECURITY TESTING

The security testing programme includes monthly vulnerability scanning and 6-monthly penetration testing of your corporate network including public facing services, web applications, network, servers, databases and critical applications.

Security Testing enables us to identify potential vulnerabilities and risks from both internal & external attacks.

Service includes the following:

- Executive summaries (jargon-free, true executive-level summaries)
- Priority matrixes, indicating remediation priorities and risks
- Detailed impact analysis of the identified vulnerabilities
- Findings and recommendations to improve security posture
- Knowledge transfer to client's IT teams

### SECURITY ADVISORY

**Compliance Audit:** Including routine compliance audits against recognized Information Security Frameworks such as ISO27001 or best practice guidance such as SAN's 20 Critical Controls.

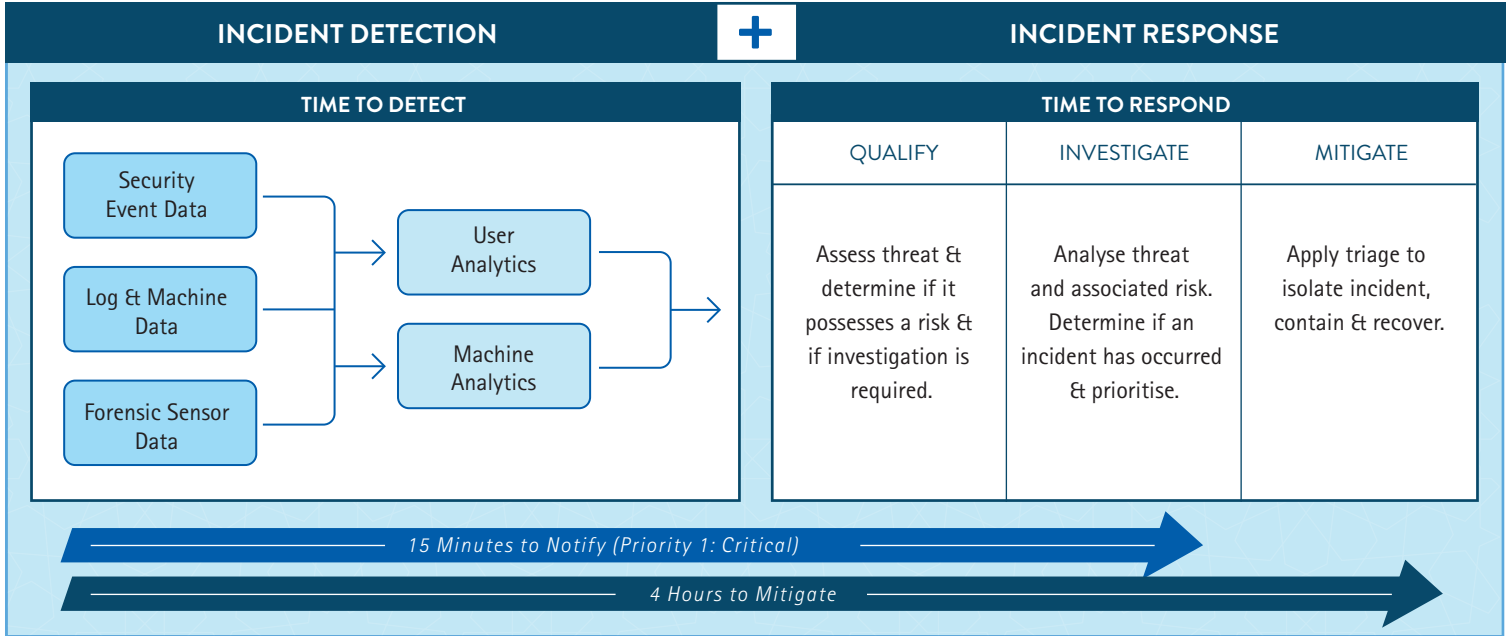
**Security Road Mapping:** Including the establishment of a maturity model for continual improvement of internal security services. This may include roadmaps for technology improvement, process optimization or investment in people or skill.

**Firewall Management:** Our certified engineers provide complete change, policy, fault and performance management on corporate firewalls, including:

- Firewall architecture planning
- Policy and rule-set management
- Performance / availability management
- Patch management, backup and recovery
- Compliance reporting

### INCIDENT DETECTION & RESOLUTION

Within Security Incident Monitoring & Management, success is measured in the speed to detect (MTTD), respond (MTTR) and the quality of the resolution. In simple terms a rapid MTTD + MTTR = Less Time = Less Damage



PACKAGE OFFERING				
	STANDARD	SILVER	GOLD	NOTES
<b>Security Testing</b>				
Vulnerability Management	✓	✓	✓	Monthly Vulnerability Scanning
Penetration Testing	✓	✓	✓	6 Monthly Testing
Web Application Testing	✓	✓	✓	6 Monthly Testing
<b>Security Advisory Services</b>				
Security Compliance Audit (ISO27001, SAN's 20)	✓	✓	✓	6 Monthly Audit
Security Advisory & Board Level Reporting	10 hrs / month	20 hrs / month	30 hrs / month	
Firewall Management	4	8	12+	Quantity inclusions
<b>Incident Detection &amp; Monitoring</b>				
24 x 7 Security Monitoring (SIEM)	200 EPS	400 EPS	600 EPS	SIEM based monitoring of Firewalls, Apps, Databases
Advanced Behavioral Analytics		✓	✓	
Active Honeypot Defense			✓	
<b>Incident Response</b>				
Incident Response & Digital Forensics	✓	✓	✓	On call basis

#### Technology Partners:

