May 2022

Tactical - Cybersecurity Services

Today’s Security Landscape and Need

- As the ransomware scourge keeps on spreading, ask yourself how helpless your business is to Cyber threats.
- The cyber security concern in global world is confronting a wide range of organizations. The costs incurred by a data breach can be destructive for any business, which makes it imperative to have cyber security conventions and standards. Despite the boundless actions to control cyber security risks and real advances in IT security innovation and practices, the quantity of cyber security issues debilitating organizations has really grown in the past few years.
- The vulnerabilities of today’s cyber security are not the vulnerabilities of yesterday. They will proceed to develop and change as time advances. That is the reason it's important that organizations remain avant-garde with regards to conceivable dangers to the security of their IT frameworks and data.
- The world is connected, information & integrations are what makes it go round. Information includes sensitive data, personally identifiable data (PII), protected health information (PHI), intellectual property, payment card information. It is important to protect information from theft and/or damage.
- Apart from risk, organizations need to also take a look at compliance requirements and regulations depending on their respective sectors (example PCIDSS, EAL/CC) and countries they operate in. (example – GDPR, HIPAA, SOX, etc.,)

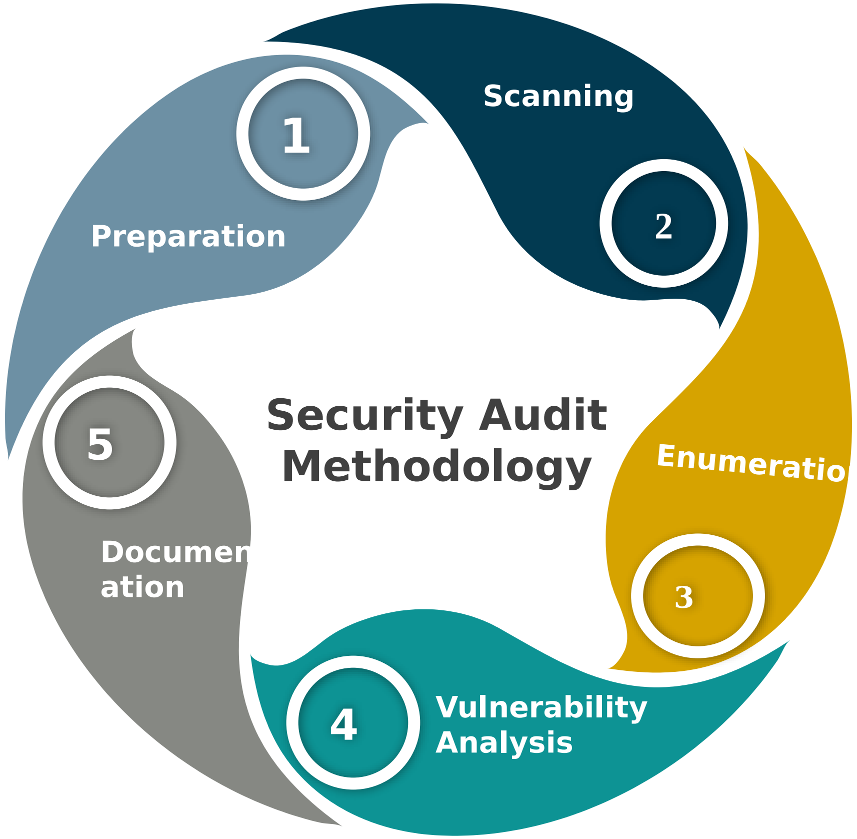
The rising danger of cyberattacks - Cyber threats are expanding in number and advancement, In the past 10 years the most reported cyber attacks were malicious code, Trojans and advanced worms, botnets, DNS attacks and spam sites. But today the cyber criminals are challenging the world with new malwares such as bitcoin wallet stealers, ransomware, PoS assaults, to give some examples.

Transformation in information security requirements - The Data security requirements are changing at a quickly quickening rate, as the Hackers are relentless and finding new techniques to penetrate a malware in the system. This makes the organizations to face complex challenges in the process of preparing for information security incidents

Traditional security solutions are ineffective for long-term - Security solutions such as (intrusion detection systems, antivirus, encryption, prevention systems, patching, etc.) are still a key control for combatting today’s known attacks. As Intruders find new ways of avoiding such controls, the effectiveness of such solutions diminishes over time

Gaps in finding the incidents - Organizations frequently do not have the capacity to identify data security occurrences because of essentially unavoidable gaps in detecting the incidents in their infrastructure.

Security Transformation services



- We provide a layered security approach that addresses the solution/infrastructure as a whole.
- Our security life cycle services comprises of people, processes and technologies that provide secure access to your business applications, from anywhere and from any device.
- We indeed integrate the best security testing practices of the industry (BSIMM, CREST, etc.,) conforming to Information Security compliance standards and our commitment to ensure the highest possible confidentiality. Every activity is performed only after identifying the complete architecture of the solution/network and its complexity.

Risk & Compliance Services

Cyber Security as a Service, predominantly Offensive Security, Attack Surface review, VAPT, Application Security, Hardening while a shift-left service viz., Secure Code Review is offered as best practice. affordable SOC & IR services (Basic to full feature) using managed XDR solution with a cloud native SIEM. Also offered are regional and industry/regulatory compliance services.

Risk focussed

-- Offensive security,

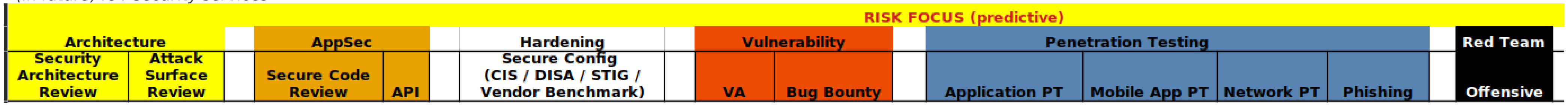
-- Vulnerability assessment and penetration testing,

-- Secure code reviews.

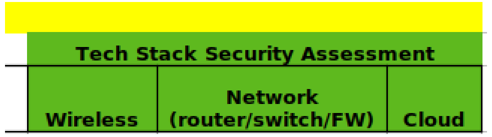
-- SOC & Incident Response.

-- Risk Data Analytics (using Splunk or ELK Stack)

** (in future) IOT security services*



RISK FOCUS (predictive)											
Architecture		AppSec		Hardening	Vulnerability		Penetration Testing				Red Team
Security Architecture Review	Attack Surface Review	Secure Code Review	API	Secure Config (CIS / DISA / STIG / Vendor Benchmark)	VA	Bug Bounty	Application PT	Mobile App PT	Network PT	Phishing	Offensive

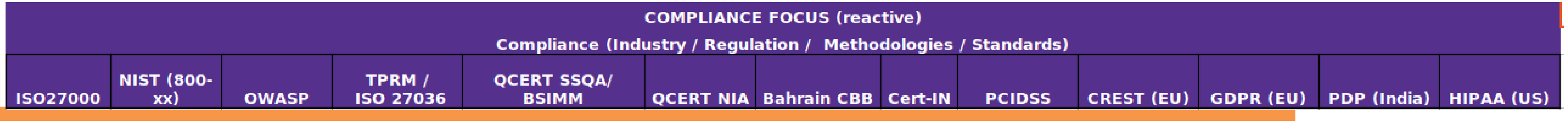


Tech Stack Security Assessment		
Wireless	Network (router/switch/FW)	Cloud

Compliance focussed

-- Standards/Regulations/Methodologies

(Qatar – qCERT NIA & SSQA;	Bahrain - CBB Compliance
Europe - GDPR/CREST;	US - NIST/HIPAA;
India – Cert-In & PDP;	Global – PCIDSS/ BSIMM / FIFA SCF;)



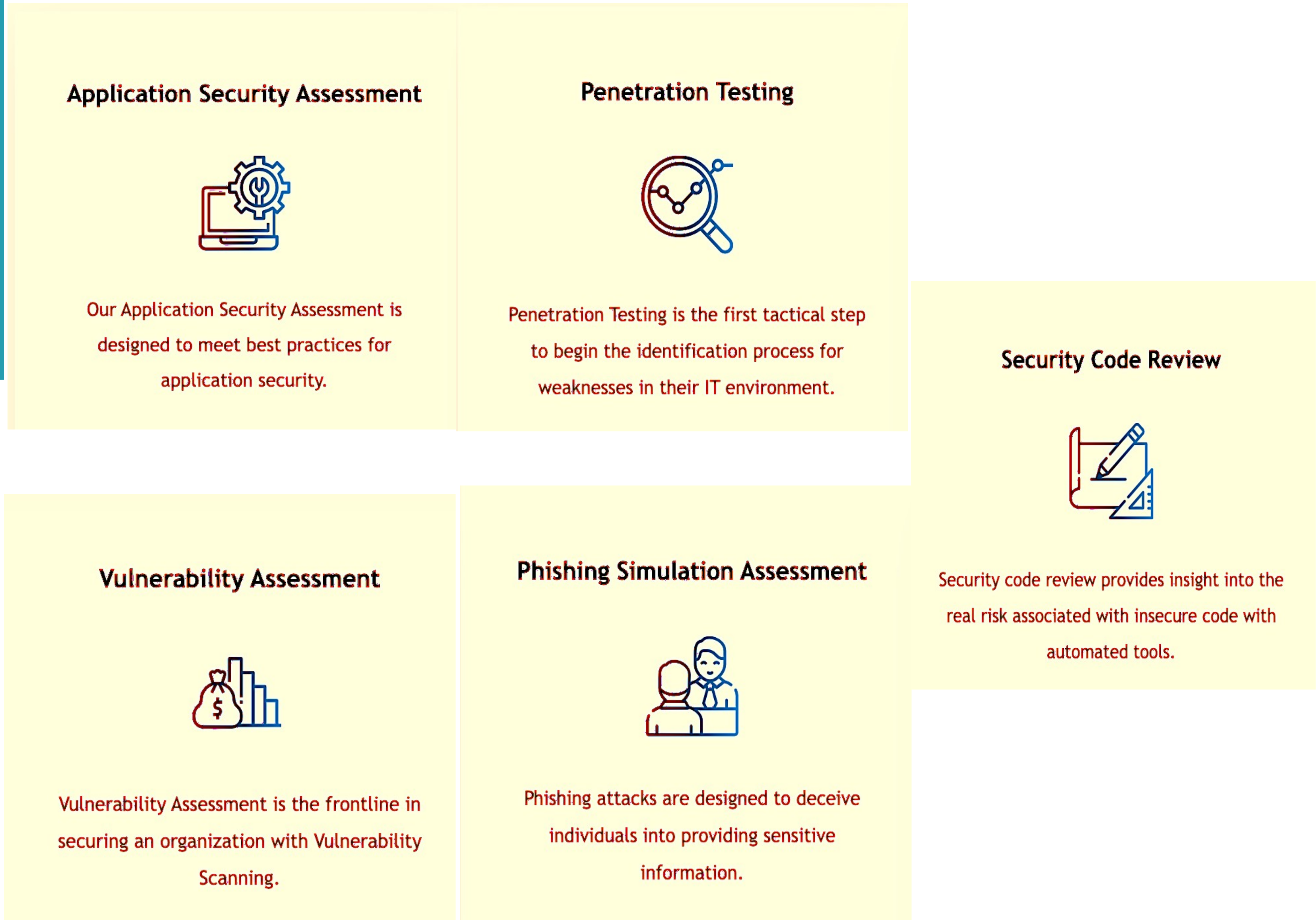
COMPLIANCE FOCUS (reactive)													
Compliance (Industry / Regulation / Methodologies / Standards)													
ISO27000	NIST (800-xx)	OWASP	TPRM / ISO 27036	QCERT SSQA/ BSIMM	QCERT NIA	Bahrain CBB	Cert-IN	PCIDSS	CREST (EU)	GDPR (EU)	PDP (India)	HIPAA (US)	

Team

Our premium global tactical service is delivered by international consultant team holding OSCP / CRTE / SANS certifications and relevant delivery expertise. Our consultants are working across Americas, Middle East and Asia.

Our team members have experience working for CERT, Big-4 accounting firms, ISPs, Infrastructure Companies and MNC Banks, Security Consulting companies.

Our services



Application Security Assessment

Our Application Security Assessment is designed to meet best practices for application security.

Penetration Testing

Penetration Testing is the first tactical step to begin the identification process for weaknesses in their IT environment.

Security Code Review

Security code review provides insight into the real risk associated with insecure code with automated tools.

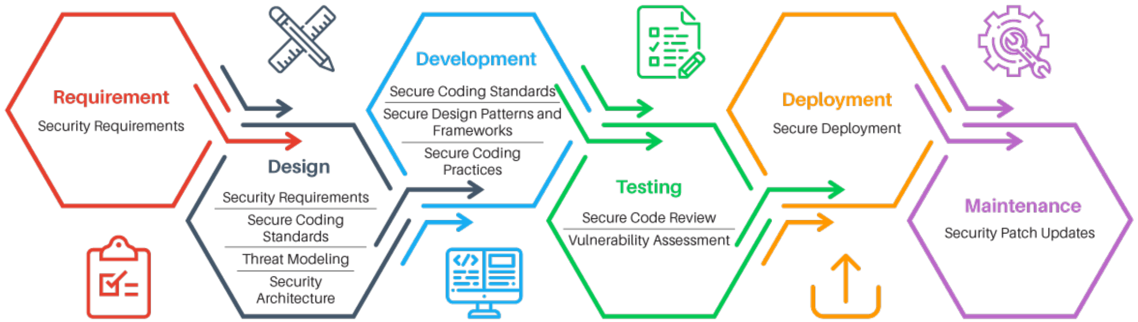
Vulnerability Assessment

Vulnerability Assessment is the frontline in securing an organization with Vulnerability Scanning.

Phishing Simulation Assessment

Phishing attacks are designed to deceive individuals into providing sensitive information.

Development Security (SecDLC) – Security by Design



Requirement

Security Requirements

Design

Security Requirements

Secure Coding Standards

Threat Modeling

Security Architecture

Development

Secure Coding Standards

Secure Design Patterns and Frameworks

Secure Coding Practices

Testing

Secure Code Review

Vulnerability Assessment

Deployment

Secure Deployment

Maintenance

Security Patch Updates

Software applications are integral components of an organization’s success. Unfortunately, while applications are built to support faster growth and enhanced user experience, these are also prone to security incidents in the absence of appropriate security mechanisms.

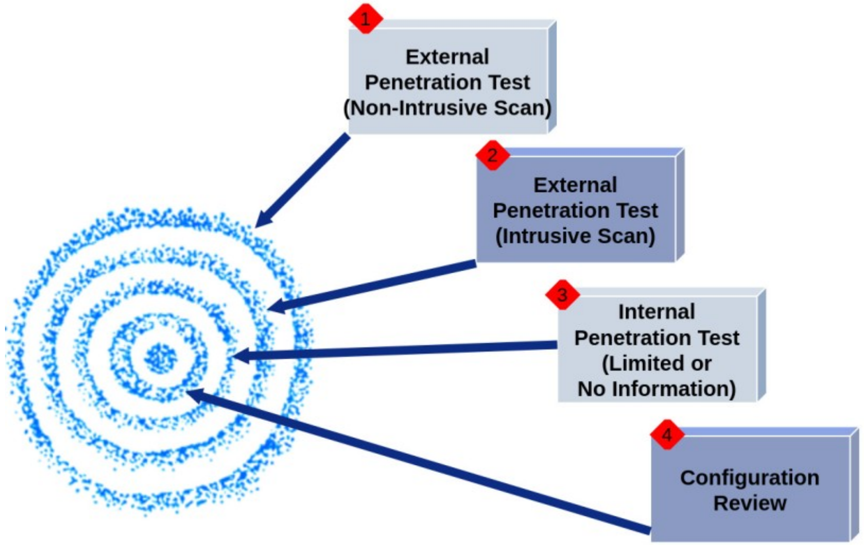
With the rising adoption of software applications in business, an increase in cybersecurity attacks shows an upward trend. Out of all such attacks, study reveals that most of cyber security attacks are carried out in the application layer.

To tackle such attacks, an efficient Application Security (AppSec) mechanism requires a combination of tools and practices for identifying, remediating, and preventing security vulnerabilities throughout the application development life cycle (using OWASP guidelines and BSIMM approach). By proactively fixing vulnerabilities, security teams improve the application’s security posture since threats are mitigated before being exploited in production.

As the cybersecurity landscape evolves, so do the tools and techniques used to secure applications. To mitigate cybersecurity threats, there are several commonly referred to as best practices and application security tools.

Onion Skin Approach for Security Assessment

“We provide a perspective of your organization’s digital infrastructure from the eye of a hacker”



Our approach is based on an ‘onion skin’ model. This gives a clear idea of the **extent of vulnerability** broken down by potential attack category. We follow CREST methodology.

While external hacking attacks attract greatest attention, **internal security weaknesses** account for the vast majority of security and services intrusions.

Vulnerability Assessment & Penetration Testing

- **Vulnerability Assessment** tools uncover all possible network weaknesses, leaving customers guessing as to which vulnerabilities pose real, imminent threats.
- **Penetration Testing** safely exploits vulnerabilities to eliminate "false positives" and reveal tangible threats. Penetration test results enable IT staff to delineate critical security issues that require immediate attention from those that pose lesser risks.

Vulnerability Assessment

Infrastructure Security:

- Vulnerability assessments on Internal/ External network
- Network architecture and firewall review
- Host and network device review

Application Security:

- Application vulnerability assessment is to maintain a resilient web presence, by detecting and remediating vulnerabilities. This process involves:
- Identify vulnerabilities visible from the Internet
- Security assessments over client-server application and Web .
- Mobile application assessments across most platforms.
- Software development lifecycle (SDLC) reviews
- Application architecture assessments
- Custom services as requested

Methodology

- **Preparation** In this phase, a formal contract is signed which also contains a Non-Disclosure Agreement. The contract also outlines infrastructure perimeter, evaluation activities, time schedules and resources available to a tester
- **Scanning** After gathering the preliminary information we will identify systems that are alive and reachable via the Network/Internet, and what services they offer. We define the Scan policy for each target. Scan policy to define the level of – Scan, Information gathering, policy checking, port scanning, Password analysis, attack stimulation etc. We perform followings activities based on the architecture and complexity of the network.
- **Enumeration** If acquisition and non-intrusive probing have not turned up any results, then a tester will next turn to identifying valid user accounts or poorly protected resource shares.
- **Vulnerability Analysis** Vulnerability Analysis is the act of determining which security holes and vulnerabilities may be applicable to the target network or host. The vulnerability analysis phase is started after some interesting hosts are identified via scanning tools and is preceded by the enumeration phase.
- **Documentation**
- **Submission of Reports**

Penetration Testing

External Penetration Testing

Audit of vulnerabilities that could be misused by external users without proper rights or credential to access a system

Internal Penetration Testing

Identifying and protecting internal threats and prevent internal users from misusing their privileges

Application Penetration Testing

Our application penetration testing services cover a wide scope, including web-based applications, mobile applications and complex reverse engineering of ‘thick-client’ applications. As part of our approach, we prefer to review source code, Where possible.
To identify vulnerabilities in the applications, Our grey box methodology combines white box testing with our black box testing techniques

Methodology

- **Exploitation** Our approach is to review the list of vulnerabilities collected in the VA stage and sort them by likelihood of success and potential harm to the target network to see which may be helpful in our exploitation efforts. We examine the list of known vulnerabilities and potential security holes on the various target hosts and determine which are most likely to be fruitful. Next we pursue exploiting those vulnerabilities to gain access on the target system. Primary targets are open ports and potentially vulnerable applications
- **Cleaning Up** Remove all testing traces of compromised systems based on the detailed and exact list of all actions performed during the penetration test; returning the system and any compromised systems to the exact configurations that they had prior to the penetration test.
- **Reporting**

Other Tactical Services

1. Web Application Security: Attempts to compromise data, elevate privileges, or gain unauthorized access to your application. Perform dynamic application security (DAST), a type of black box security testing in which tests are performed by attacking an application from outside/inside.

2. Mobile Application Security (iOS and Android): Assess the security perimeters within a mobile environment. Focus on static analysis, local file analysis, dynamic analysis, reverse engineering etc.,

3. API Security: APIs are used to connect various applications and services. As data flows through them, security is very important to prevent data leakage. It focuses on mitigating the authentication, authorization, resource level access control, input validation etc.,

4. Secure Source Code Review: Static Application Security Testing (SAST) can help analyze source code or compiled versions of code to find security flaws.

5. Secure Configuration Review of Network Devices: Discover vulnerabilities in firewalls, switches and routers, automatically prioritized to your organization.

6. Hardening Servers using Benchmarks: Review and implement the configuration best practices for securely configuring a system using CIS Benchmarks.

7. Third Party Reviews: Review the internal controls to ensure effective implemetation of control systems across organization/function or your supply chain or outsourced vendor services/development efforts.

SOC Technology & Service

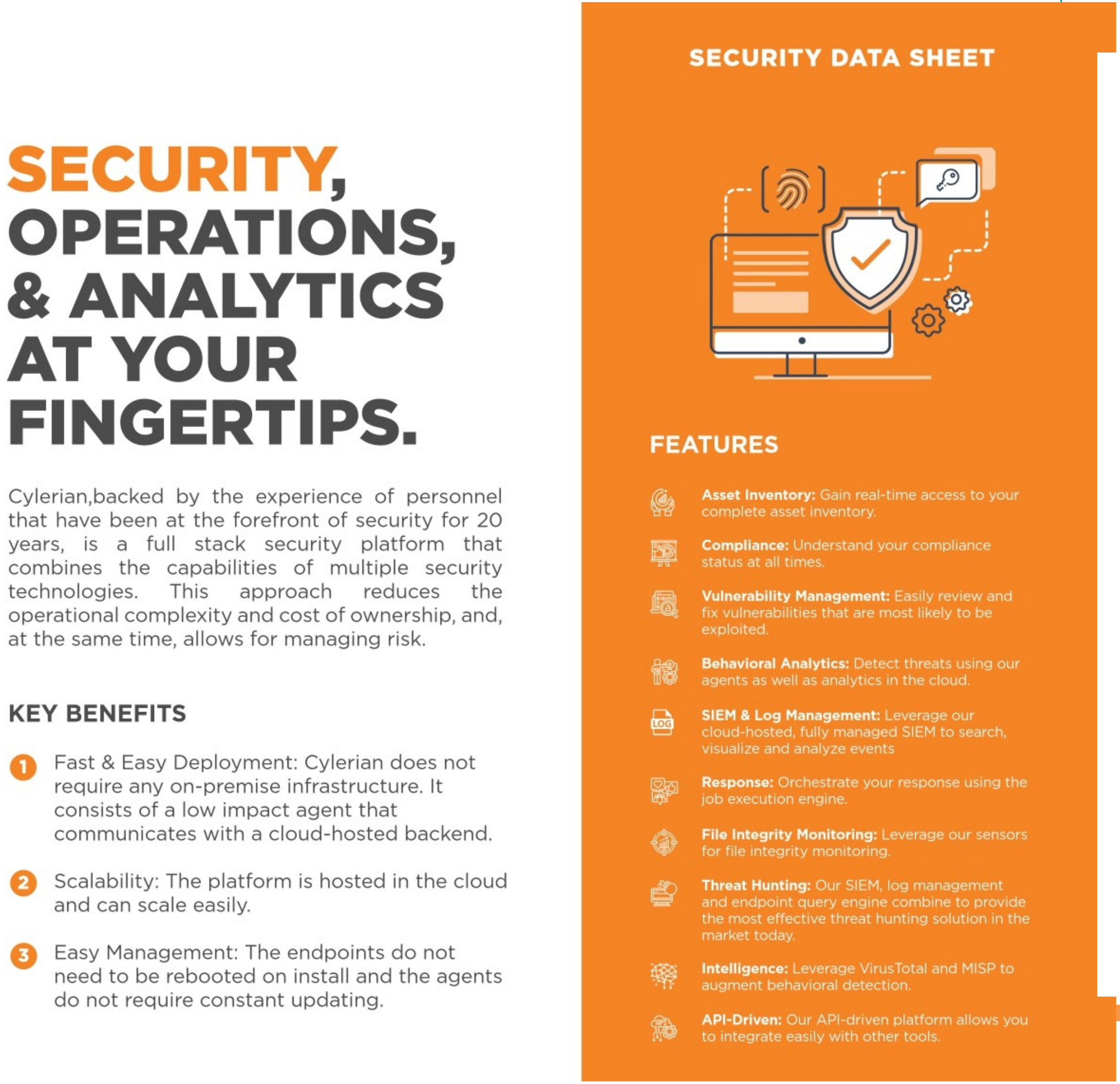
1. Tool: cloud hosted XDR w/SIEM:

Managed detection and response solution with cloud hosted SIEM solution, designed by exFireEye/Mandiant Team. This solution is customized to local tech stack, threat intel and regulatory needs.

2. Service: SOC MDR:

Basic to full service Security Managed Detection & Response service (IR) with SOC team operating between South America and India during (local timezone) day time to offer 24/7 support.

1. Tool: cloud hosted XDR w/SIEM



SECURITY, OPERATIONS, & ANALYTICS AT YOUR FINGERTIPS.

Cylerian,backed by the experience of personnel that have been at the forefront of security for 20 years, is a full stack security platform that combines the capabilities of multiple security technologies. This approach reduces the operational complexity and cost of ownership, and, at the same time, allows for managing risk.

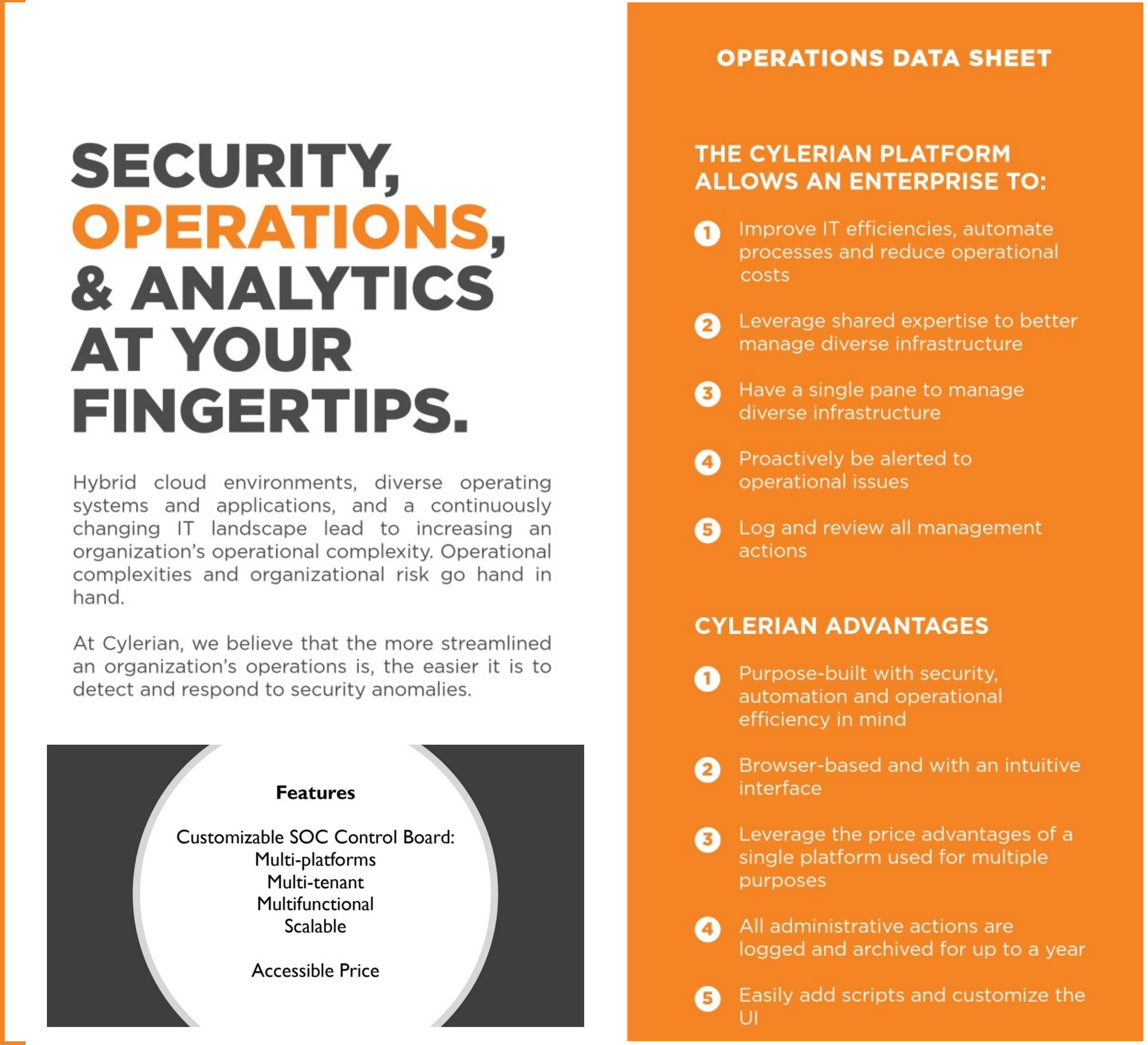
KEY BENEFITS

1. Fast & Easy Deployment: Cylerian does not require any on-premise infrastructure. It consists of a low impact agent that communicates with a cloud-hosted backend.
2. Scalability: The platform is hosted in the cloud and can scale easily.
3. Easy Management: The endpoints do not need to be rebooted on install and the agents do not require constant updating.

SECURITY DATA SHEET

FEATURES

- **Asset Inventory:** Gain real-time access to your complete asset inventory.
- **Compliance:** Understand your compliance status at all times.
- **Vulnerability Management:** Easily review and fix vulnerabilities that are most likely to be exploited.
- **Behavioral Analytics:** Detect threats using our agents as well as analytics in the cloud.
- **SIEM & Log Management:** Leverage our cloud-hosted, fully managed SIEM to search, visualize and analyze events
- **Response:** Orchestrate your response using the job execution engine.
- **File Integrity Monitoring:** Leverage our sensors for file integrity monitoring.
- **Threat Hunting:** Our SIEM, log management and endpoint query engine combine to provide the most effective threat hunting solution in the market today.
- **Intelligence:** Leverage VirusTotal and MISP to augment behavioral detection.
- **API-Driven:** Our API-driven platform allows you to integrate easily with other tools.



SECURITY, OPERATIONS, & ANALYTICS AT YOUR FINGERTIPS.

Hybrid cloud environments, diverse operating systems and applications, and a continuously changing IT landscape lead to increasing an organization's operational complexity. Operational complexities and organizational risk go hand in hand.

At Cylerian, we believe that the more streamlined an organization's operations is, the easier it is to detect and respond to security anomalies.

OPERATIONS DATA SHEET

THE CYLERIAN PLATFORM ALLOWS AN ENTERPRISE TO:

1. Improve IT efficiencies, automate processes and reduce operational costs
2. Leverage shared expertise to better manage diverse infrastructure
3. Have a single pane to manage diverse infrastructure
4. Proactively be alerted to operational issues
5. Log and review all management actions

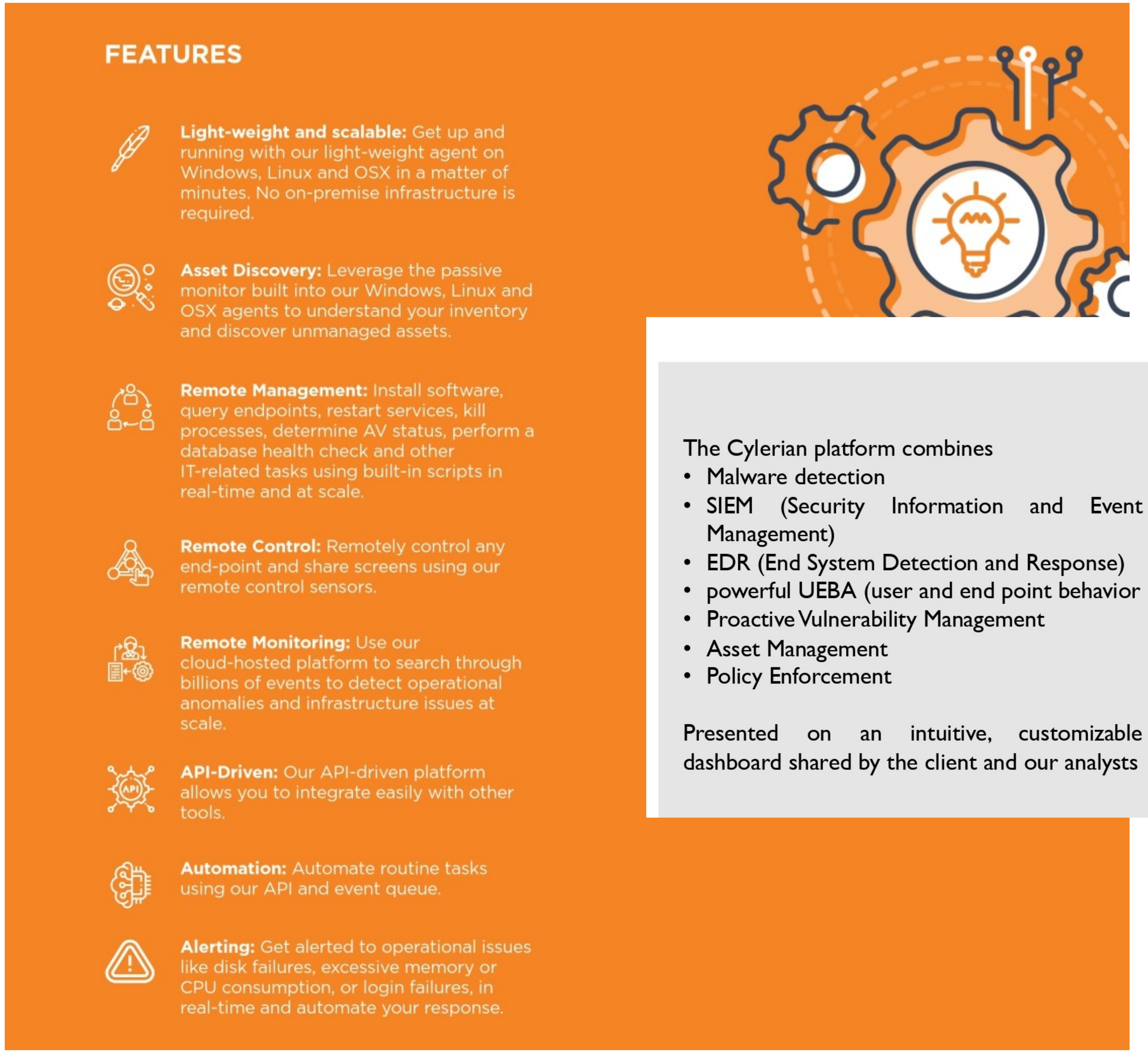
CYLERIAN ADVANTAGES

1. Purpose-built with security, automation and operational efficiency in mind
2. Browser-based and with an intuitive interface
3. Leverage the price advantages of a single platform used for multiple purposes
4. All administrative actions are logged and archived for up to a year
5. Easily add scripts and customize the UI

Features

Customizable SOC Control Board:
Multi-platforms
Multi-tenant
Multifunctional
Scalable

Accessible Price



FEATURES

Light-weight and scalable: Get up and running with our light-weight agent on Windows, Linux and OSX in a matter of minutes. No on-premise infrastructure is required.

Asset Discovery: Leverage the passive monitor built into our Windows, Linux and OSX agents to understand your inventory and discover unmanaged assets.

Remote Management: Install software, query endpoints, restart services, kill processes, determine AV status, perform a database health check and other IT-related tasks using built-in scripts in real-time and at scale.

Remote Control: Remotely control any end-point and share screens using our remote control sensors.

Remote Monitoring: Use our cloud-hosted platform to search through billions of events to detect operational anomalies and infrastructure issues at scale.

API-Driven: Our API-driven platform allows you to integrate easily with other tools.

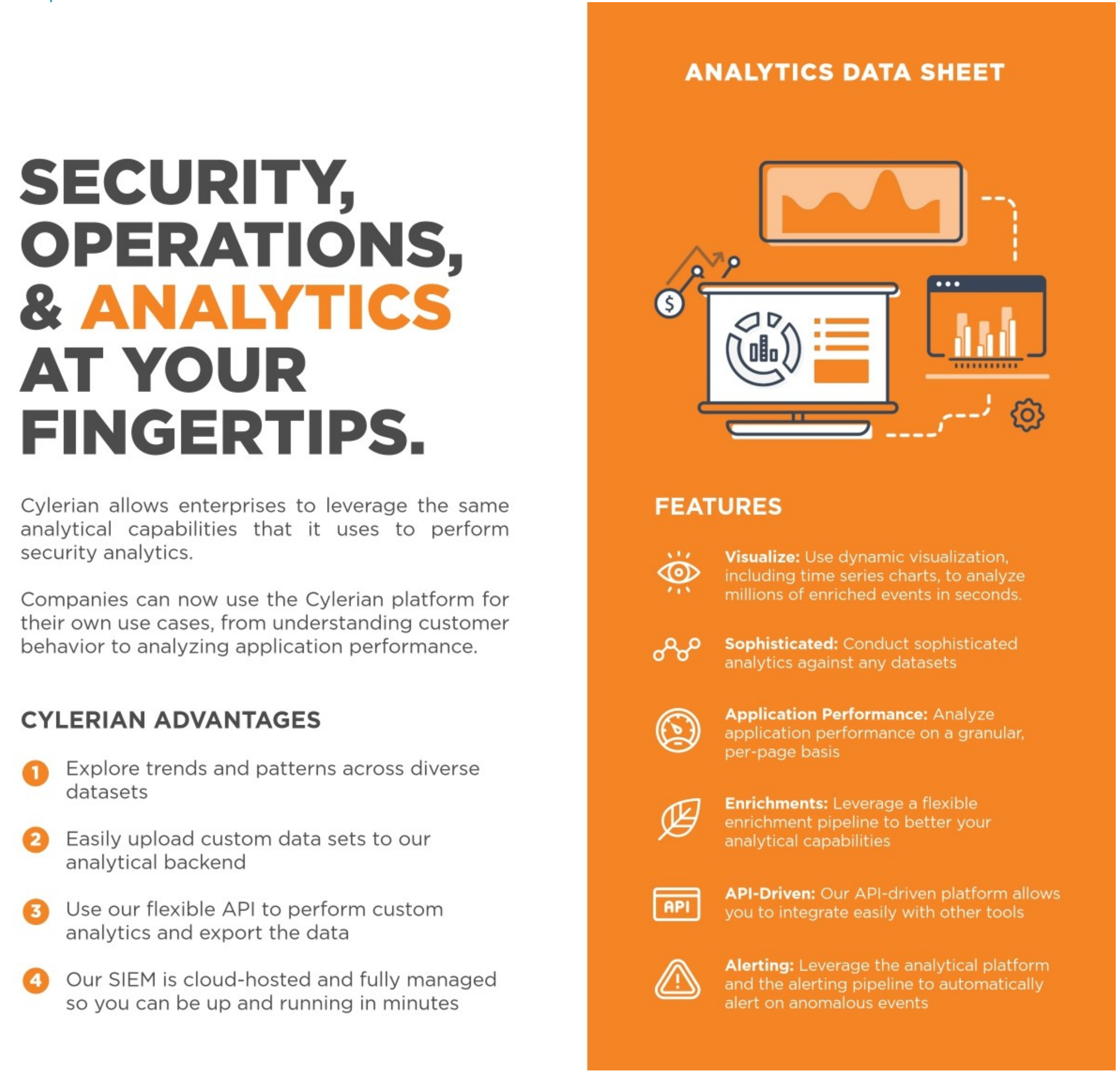
Automation: Automate routine tasks using our API and event queue.

Alerting: Get alerted to operational issues like disk failures, excessive memory or CPU consumption, or login failures, in real-time and automate your response.

The Cylerian platform combines

- Malware detection
- SIEM (Security Information and Event Management)
- EDR (End System Detection and Response)
- powerful UEBA (user and end point behavior
- Proactive Vulnerability Management
- Asset Management
- Policy Enforcement

Presented on an intuitive, customizable dashboard shared by the client and our analysts



SECURITY, OPERATIONS, & ANALYTICS AT YOUR FINGERTIPS.

Cylerian allows enterprises to leverage the same analytical capabilities that it uses to perform security analytics.

Companies can now use the Cylerian platform for their own use cases, from understanding customer behavior to analyzing application performance.

CYLERIAN ADVANTAGES

1. Explore trends and patterns across diverse datasets
2. Easily upload custom data sets to our analytical backend
3. Use our flexible API to perform custom analytics and export the data
4. Our SIEM is cloud-hosted and fully managed so you can be up and running in minutes

ANALYTICS DATA SHEET

FEATURES

Visualize: Use dynamic visualization, including time series charts, to analyze millions of enriched events in seconds.

Sophisticated: Conduct sophisticated analytics against any datasets

Application Performance: Analyze application performance on a granular, per-page basis

Enrichments: Leverage a flexible enrichment pipeline to better your analytical capabilities

API-Driven: Our API-driven platform allows you to integrate easily with other tools

Alerting: Leverage the analytical platform and the alerting pipeline to automatically alert on anomalous events

2. Service: SOC MDR

A team experienced in:

SIEM operations
Analytics
Incident Response
Vulnerability Analysis
Threat Hunting and Intelligence
Forensics
Orchestration and Automation
Security Management Systems
Customer Focus

A technology that integrates the key functionalities to simplify IT operations and security:

Malware Detection
Vulnerability management
SIEM
EDR
SOAR
UEBA
PEP
Asset Management

The dashboard is intuitive and customizable.

Several levels of service to fit your budget, then upgrade your service when time is right, without re-engineering your platform.

Service highlights

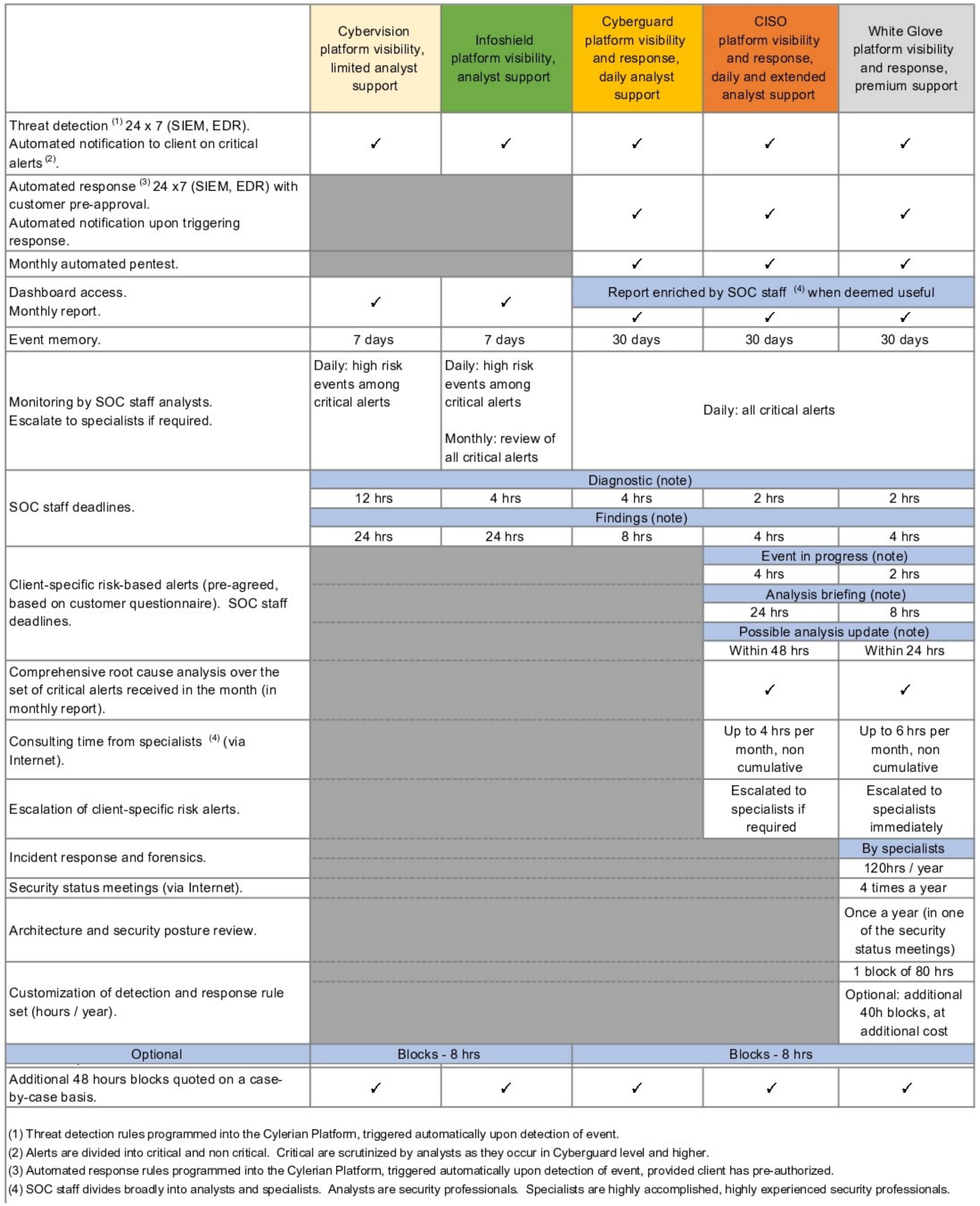
- 24x7x365 monitoring and alerts
- Automated authorized response
- Analysts monitoring daily
- Smart triage to prevent saturation
- Monthly status and incident reports
- Escalation to domain experts
- Access to Incident Response and Forensics
- Monthly standardized pentest
- Cost advantage

Choose the level that suits you

- Security alert and response
- Cyberguard
- CISO
- White Glove
- Options: 24x7 contact center, extended Incident Response, extended forensics, consulting

Our MSS solution:

- Agents on each node (real or virtual equipment) monitor all events.
- Network devices can be monitored via syslog and netflow.
- Logging and metadata collection capabilities for all users' activities, and security events configured.
- Captures all activity, even for applications that do not produce internal records.
- User and endpoint behavior analytics (ueba).



	Cybervision platform visibility, limited analyst support	Infoshield platform visibility, analyst support	Cyberguard platform visibility and response, daily analyst support	CISO platform visibility and response, daily and extended analyst support	White Glove platform visibility and response, premium support
Threat detection [1] 24 x 7 (SIEM, EDR). Automated notification to client on critical alerts [2].	✓	✓	✓	✓	✓
Automated response [3] 24 x7 (SIEM, EDR) with customer pre-approval. Automated notification upon triggering response.			✓	✓	✓
Monthly automated pentest.			✓	✓	✓
Dashboard access. Monthly report.	✓	✓	Report enriched by SOC staff [4] when deemed useful		
			✓	✓	✓
Event memory.	7 days	7 days	30 days	30 days	30 days
Monitoring by SOC staff analysts. Escalate to specialists if required.	Daily: high risk events among critical alerts	Daily: high risk events among critical alerts Monthly: review of all critical alerts	Daily: all critical alerts		
SOC staff deadlines.	Diagnostic (note)				
	12 hrs	4 hrs	4 hrs	2 hrs	2 hrs
	Findings (note)				
	24 hrs	24 hrs	8 hrs	4 hrs	4 hrs
Client-specific risk-based alerts (pre-agreed, based on customer questionnaire). SOC staff deadlines.				Event in progress (note)	
				4 hrs	2 hrs
				Analysis briefing (note)	
				24 hrs	8 hrs
				Possible analysis update (note)	
				Within 48 hrs	Within 24 hrs
Comprehensive root cause analysis over the set of critical alerts received in the month (in monthly report).				✓	✓
Consulting time from specialists [4] (via Internet).				Up to 4 hrs per month, non cumulative	Up to 6 hrs per month, non cumulative
Escalation of client-specific risk alerts.				Escalated to specialists if required	Escalated to specialists immediately
Incident response and forensics.					By specialists
					120hrs / year
Security status meetings (via Internet).					4 times a year
Architecture and security posture review.					Once a year (in one of the security status meetings)
Customization of detection and response rule set (hours / year).					1 block of 80 hrs
					Optional: additional 40h blocks, at additional cost
Optional	Blocks - 8 hrs		Blocks - 8 hrs		
Additional 48 hours blocks quoted on a case-by-case basis.	✓	✓	✓	✓	✓

[1] Threat detection rules programmed into the Cylerian Platform, triggered automatically upon detection of event.

[2] Alerts are divided into critical and non critical. Critical are scrutinized by analysts as they occur in Cyberguard level and higher.

[3] Automated response rules programmed into the Cylerian Platform, triggered automatically upon detection of event, provided client has pre-authorized.

[4] SOC staff divides broadly into analysts and specialists. Analysts are security professionals. Specialists are highly accomplished, highly experienced security professionals.