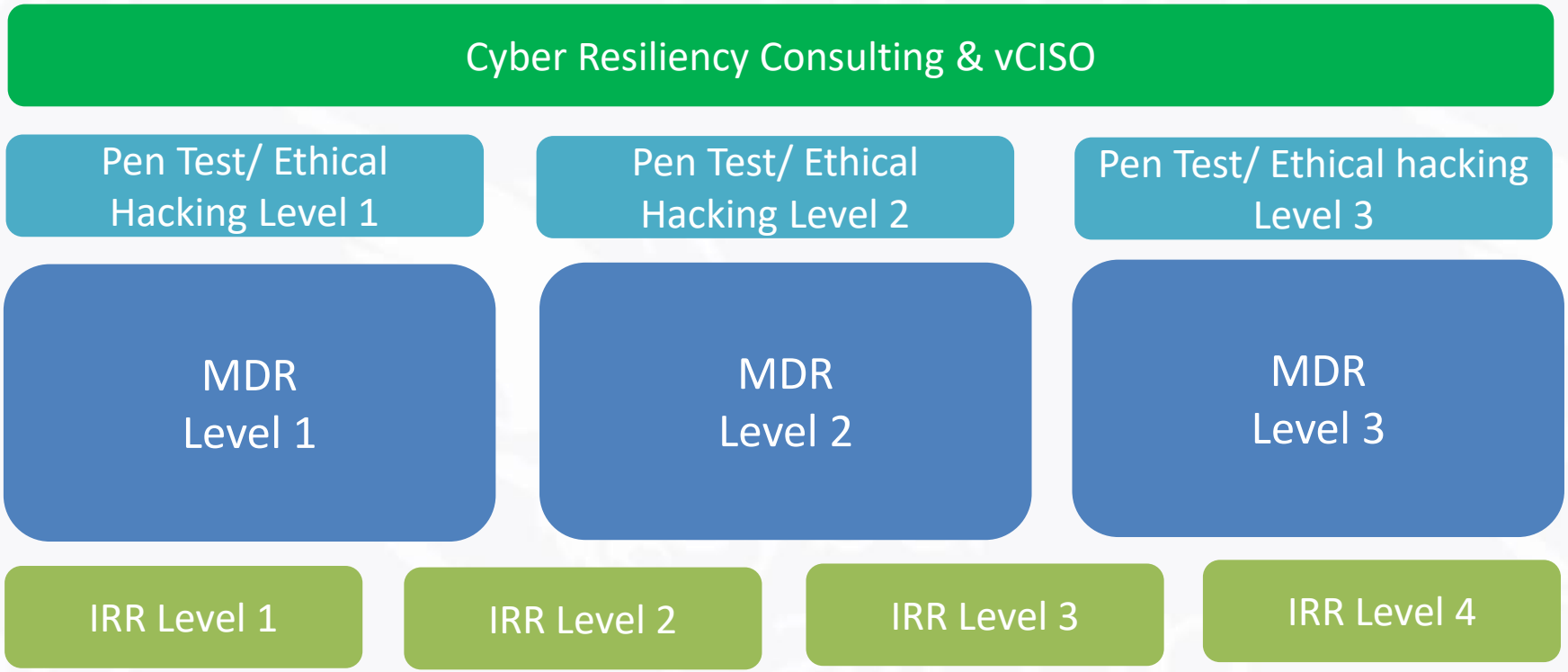
ENTERPRISE CYBER RESILIENCY SERVICES

ENTERPRISE CYBER RESILIENCY SERVICES



Cyber Resiliency Hardening of a business involves far more than throwing tools at a SOC, responding to alerts, and buying cyber insurance. CYBERFALCON's Enterprise Cyber Resiliency addresses every thread in the tapestry of an organization – This is a must, because a cyber attacker only needs to find one loose thread to unravel Business Continuity

MOHAMMAD HASAN SAJJAD – CTO – Transborder Ventures, LLC

AWARDS AND RECOGNITIONS

Clutch top Cyber Security Company in 2020

UnderDefense awarded as Top Cyber Security Consultants company in 2020 Worldwide

Ranked in best 1% of companies in CyberSecurity at the Manifest

Proud to state that we are ranked #5 among more than 300 CyberSecurity Companies at The Manifest

Gartner Top 10 Security Consulting Vendor

Ranked among top 10 Security Consultants worldwide by Gartner Peer Insights

Boss of the SOC at Splunk .conf2019

At the Splunk.conf event in Las Vegas, we participated in an amazing challenge Boss of the SOC and got 9th place among 1357 participating teams

#3 at SecOps in EU

Won a bronze medal in the International Exercise and Conference on Security Operations challenge in Budapest

#2 in Clutch Leaders Matrix

A key player in Clutch leaders matrix in Cyber Security solutions ranked as #2 among 3,674 Firms

comparitech EDITOR'S CHOICE

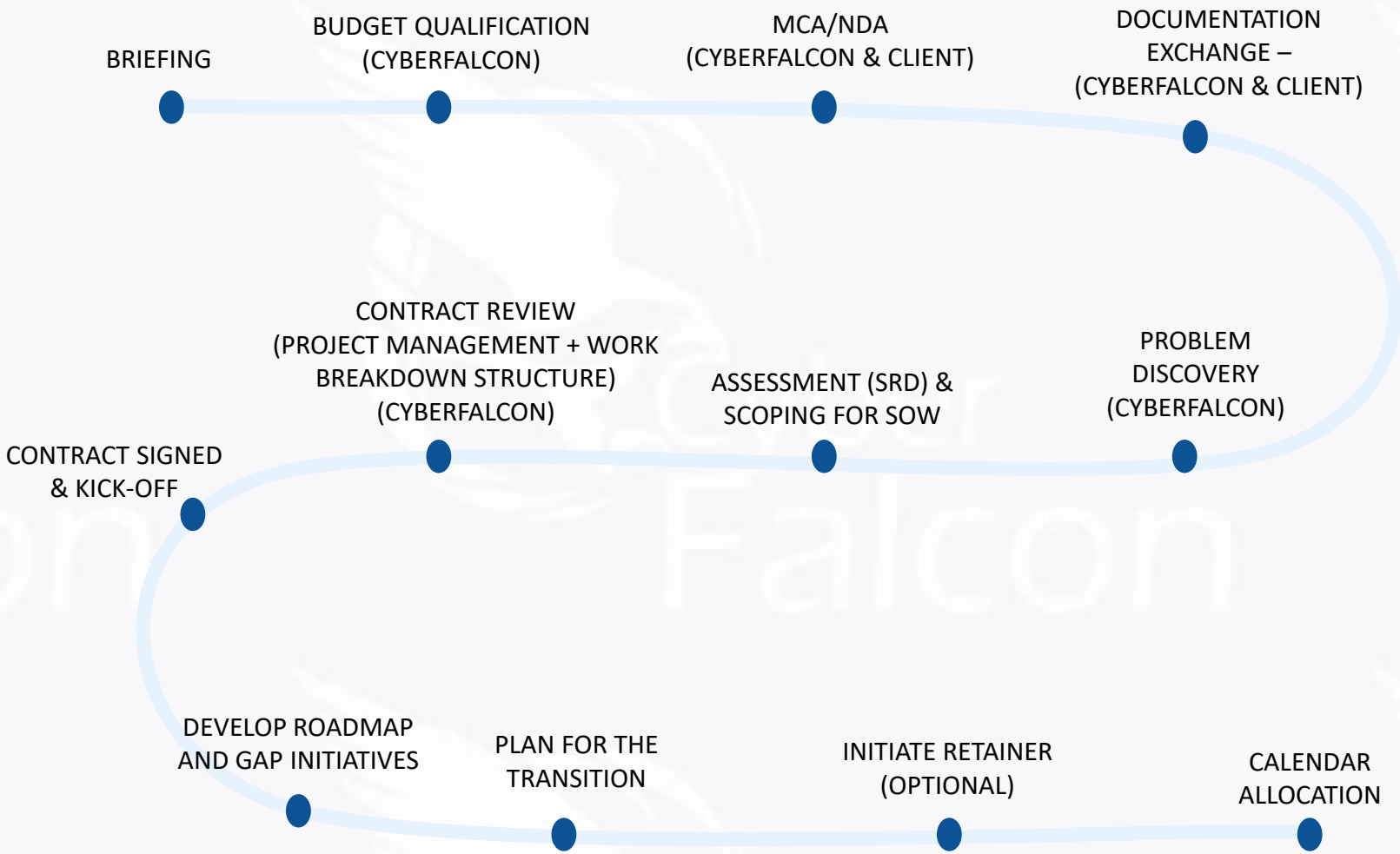
A SIEM service provided by an expert Security Operations Center and cybersecurity consultancy; choice of managed SIEM, on-premises software, or co-managed SIEM.

RECOGNITIONS, AWARDS & PARTNERSHIPS

CERTIFICATIONS

Ph.D.'s in IT Security

CUSTOMER ENGAGEMENT PROCESS

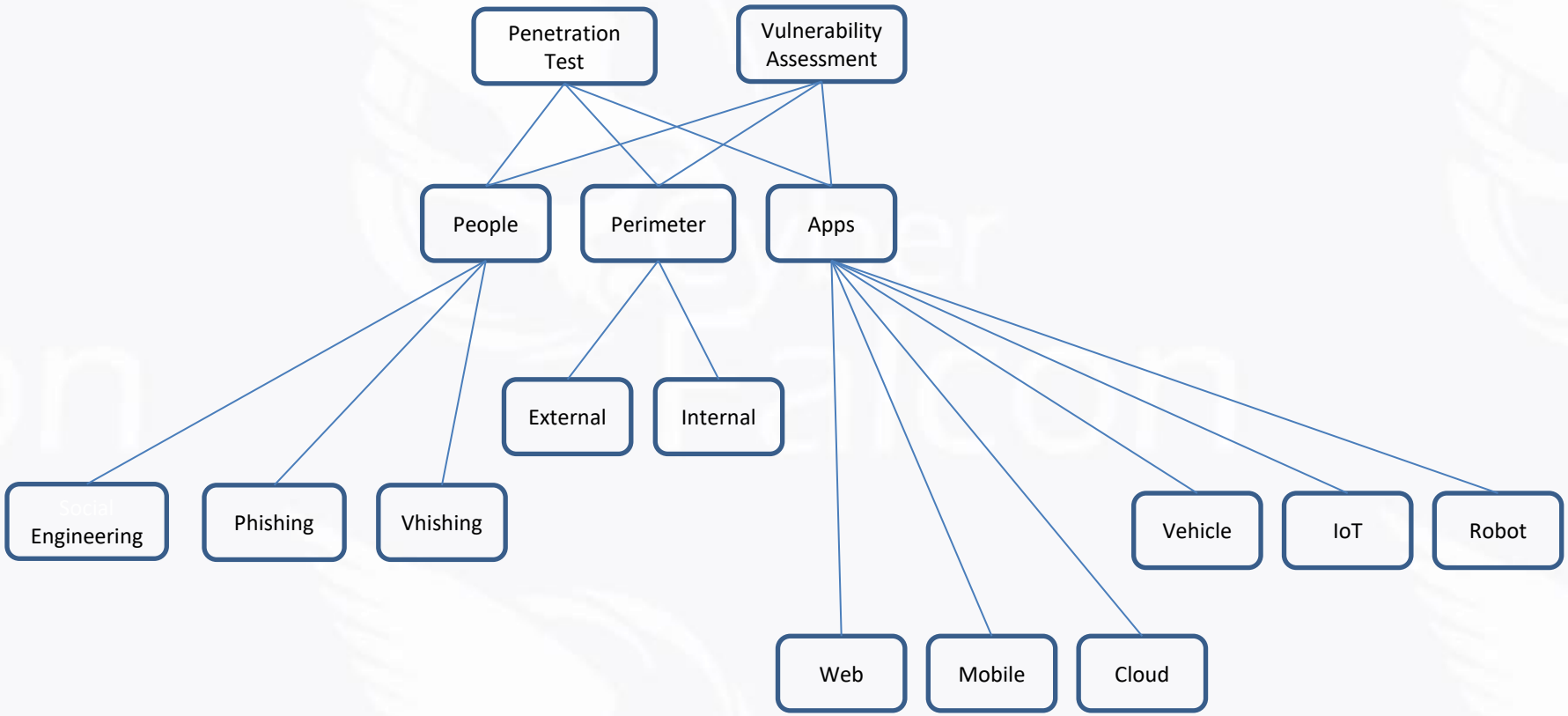


Cyber Falcon

PENETRATION TESTING | ETHICAL HACKING & VULNERABILITY ASSESSMENTS

PENETRATION TESTING | ETHICAL HACKING & VULNERABILITY ASSESSMENTS

- Application Penetration Test
- External/ Internal Vulnerability Assessment & Penetration Tests
- Organization Penetration Test/ Ethical Hacking Options & Bundles



VULNERABILITY ASSESSMENT VS. PENTEST

	Vulnerability Scan	Penetration Test
Purpose	Identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system.	Identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components.
When	At least quarterly and after significant changes[1].	At least annually and upon significant changes[2].
How	Typically a variety of automated tools combined with manual verification of identified issues.	A manual process that may include the use of vulnerability scanning or other automated tools, resulting in a comprehensive report.
Reports	Potential risks posed by known vulnerabilities, ranked in accordance with NVD/CVSS base scores associated with each vulnerability. For PCI DSS, external vulnerability scans must be performed by an ASV and the risks ranked in accordance with the CVSS. Internal vulnerability scans may be performed by qualified personnel (does not require an ASV) and risks ranked in accordance with the organization's risk-ranking process as defined in PCI DSS Requirement 6.1. An external vulnerability scan is conducted from outside the target organization. An internal vulnerability scan is conducted from inside the target organization.	Description of each vulnerability verified and/or potential issue discovered. More specific risks that vulnerability may pose, including specific methods how and to what extent it may be exploited. Examples of vulnerabilities include but are not limited to SQL injection, privilege escalation, cross-site scripting, or deprecated protocols.
Duration	Relatively short amount of time, typically several seconds to several minutes per scanned host.	Engagements may last days or weeks depending on the scope of the test and size of the environment to be tested. Tests may grow in time and complexity if efforts uncover additional scope.

PEN TESTING VS. ETHICAL HACKING

PEN TEST	ETHICAL HACKING
Focuses on identifying risks	Goes beyond identifying risk but to show and demonstrate the exploitation
Seeks to find security vulnerabilities and weaknesses in a targeted IT system at a point in time often because of budget constraints	Seeks to find as many vulnerabilities and security flaws as possible in the IT environment
Is usually not conducted on the entire application or IT infrastructure	Uses wide-ranging techniques and attack vectors
Seeks to tell the business how their security systems respond to real-time attacks	Seeks to provide a holistic evaluation of cybersecurity and has a broader scope and assesses the IT environment holistically over longer periods of time
Suggest measures to strengthen their systems	Offers more remediation and risk mitigation recommendation and assistance is provided by ethical hackers in comparison to pen-testers
Web application pen-testing and other types of pen-testing are targeted, the testers require access and permissions only for those targeted systems/ areas they are testing	Tester needs access and permissions to a whole range of systems and areas, based on the defined scope
Can be conducted by someone with knowledge and expertise in the specific area of testing	Ethical hackers must have comprehensive knowledge of software, programming techniques, hardware, and the IT environment to be effective
Knowledge of hacking and attack methodologies in the targeted areas is adequate for pen-testers	Ethical hackers must have a broader knowledge of attack methodologies and attack vectors
Detailed reporting is necessary for pen-testing	Ethical hackers must be experts in report writing and be capable of producing in-depth reports with recommended solutions
Certification may be recommended but not required	Ethical hackers must be certified
Pen testing is good when you don’t have an environment where you can carry out the exploit	
The goal for the ethical hacker is to see exactly how far they can get into your environment, identify high-value targets, and avoid any detection	

Cyber Falcon

24X7 MANAGED DETECTION & RESPONSE | MANAGED SIEM | MANAGED ENDPOINT PROTECTION | MANAGED SOAR

EDR AND MDR SERVICES

Detection	SMB Level 1	Mid-Enterprise Level 2	Enterprise Level 3
Co-Managing your EDR/NGAV	X	X	X
24x7 monitoring and notifications	X	X	X
Alert triage	X	X	X
Direct Chat with our analysts in 24x7 mode	X	X	X
Remediation guidance	X	X	X
Co-Managing your SIEM, WAF, NGFW (Splunk, Elastic, Logrythm. IBM Qradar, Archsight, RSA etc)		X	X
Proactive threat hunting		X	X
Advanced Metrics, reporting and summaries for Compliance		X	X
UnderDefense Library with 1500+ detection rules		X	X
Reporting Weekly		X	X
Several best of breed Threat Intel Feeds			X
Tuning your security tools			**X**
Malware analysts			**X**
Response			
Incident validation and notification	X	X	X
Manual Remote response with customer IT (40 hours/y)		X	X
Containment and remediation			X
Resilience recommendations			X
Automated Response Integration with customer Tools			X
Advanced service details			X
24x7 Alert triage performed by UD analysts	X	X	X
Scheduled Automated Reports	X	X	X
Office 365 / Google Apps & Cloud API Integration AWS Cloud Trail API Integration	X	X	X
Alerting via Slack or Email enabled	X	X	X
Nessus Vulnerability Scan Log Integration		X	X
Free Knowledge Transfer		X	X
Vulnerability Management		X	X
Web-based portal login		X	X
Handle multi-step investigations: trace activities associated with compromised systems and apply the kill-chain methodology to see the attack lifecycle		X	X
Compliance Management		X	X
Dedicated Customer engagement manager		X	X
8x5 Technical Support		X	
Continuously monitor: clearly visualize security posture with dashboards, key security indicators, static & dynamic thresholds, and trending		X	X
PCI, HIPAA and CIS Top 20 Pre-Defined Reports		X	X
24x7 Technical Support			X
Prioritize and act: optimize, centralize, and automate incident detection workflows with alerts, centralized logs, and pre-defined reports and correlations			X
Custom Reporting Enabled			X

MDR SLA EXCEPTIONS

The SLA will be null and void under the following circumstances:

- Client makes changes which generate more than 35 alerts per hour inundating the SOC.
- Client enables changes to send alerts the SOC, but alert does not follow the alert onboarding procedures.
- Mutually agreed non standard requests.
- Requests for features that fall outside of the ability to deliver with the standard SOC technology
- Changes made by the client or client's representatives which cause the loss of connectivity or security.
- Planned outages or maintenance windows.
- Outages caused by a Force Majeure event.

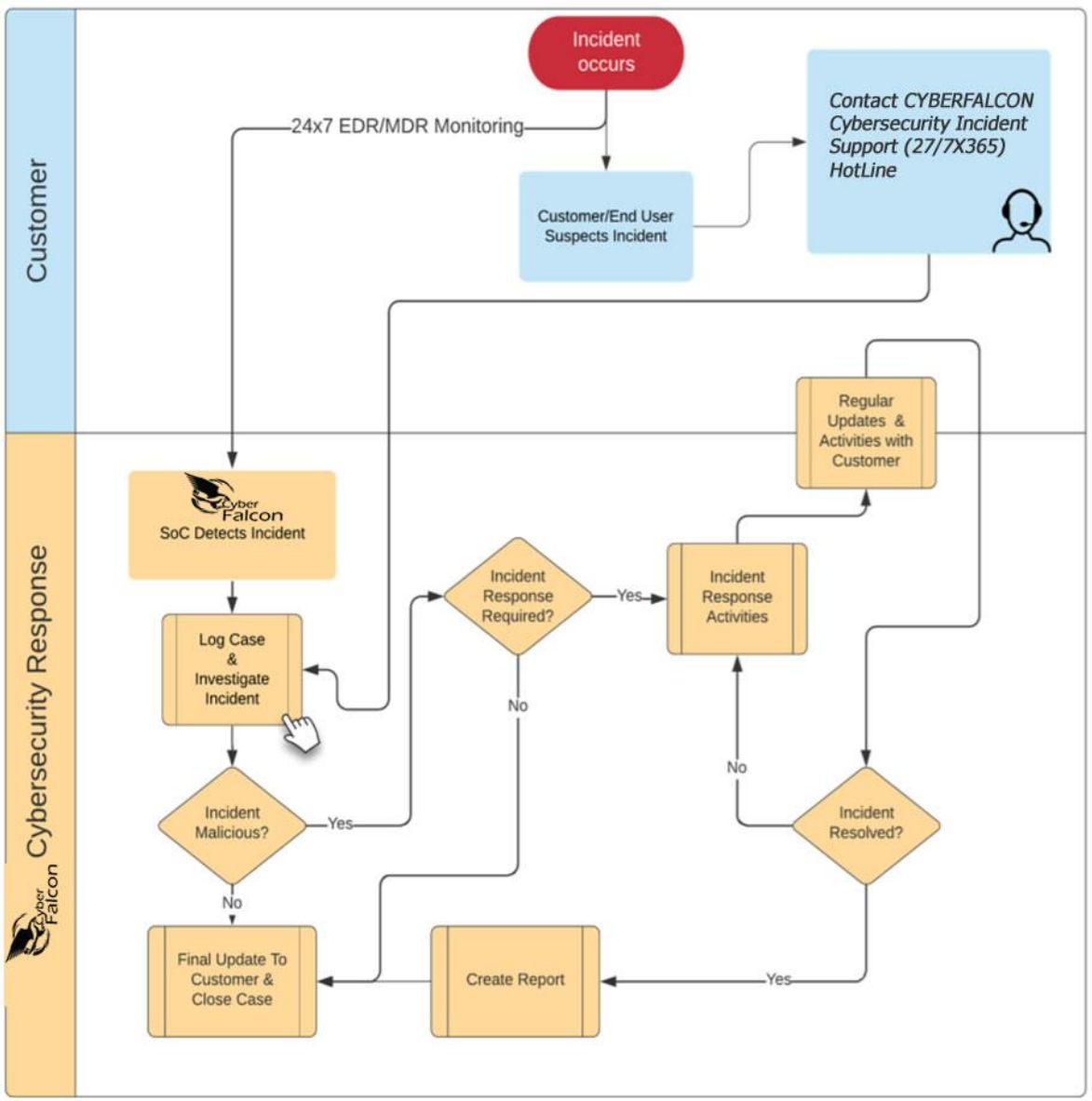
The SLA will be paused under the following circumstances:

- Client fails to respond to notifications or escalation attempts from the SOC and has attempted to contact all client resources on the client escalation list
- Cases, incidents, service disruptions or outages requiring escalation to the product vendor or 3PP (PaaS, IaaS, SaaS, etc.)
- Cases awaiting response from client
- Outages, loss or degradation of performance due to the client choosing to run the other software

Cyber Falcon

INCIDENT RESPONSE

OPERATING ENGAGEMENT MODEL



Cyber Falcon

ENTERPRISE CYBER RESILIENCE CONSULTING

CONSULTING SERVICES

Customer Engagement Process

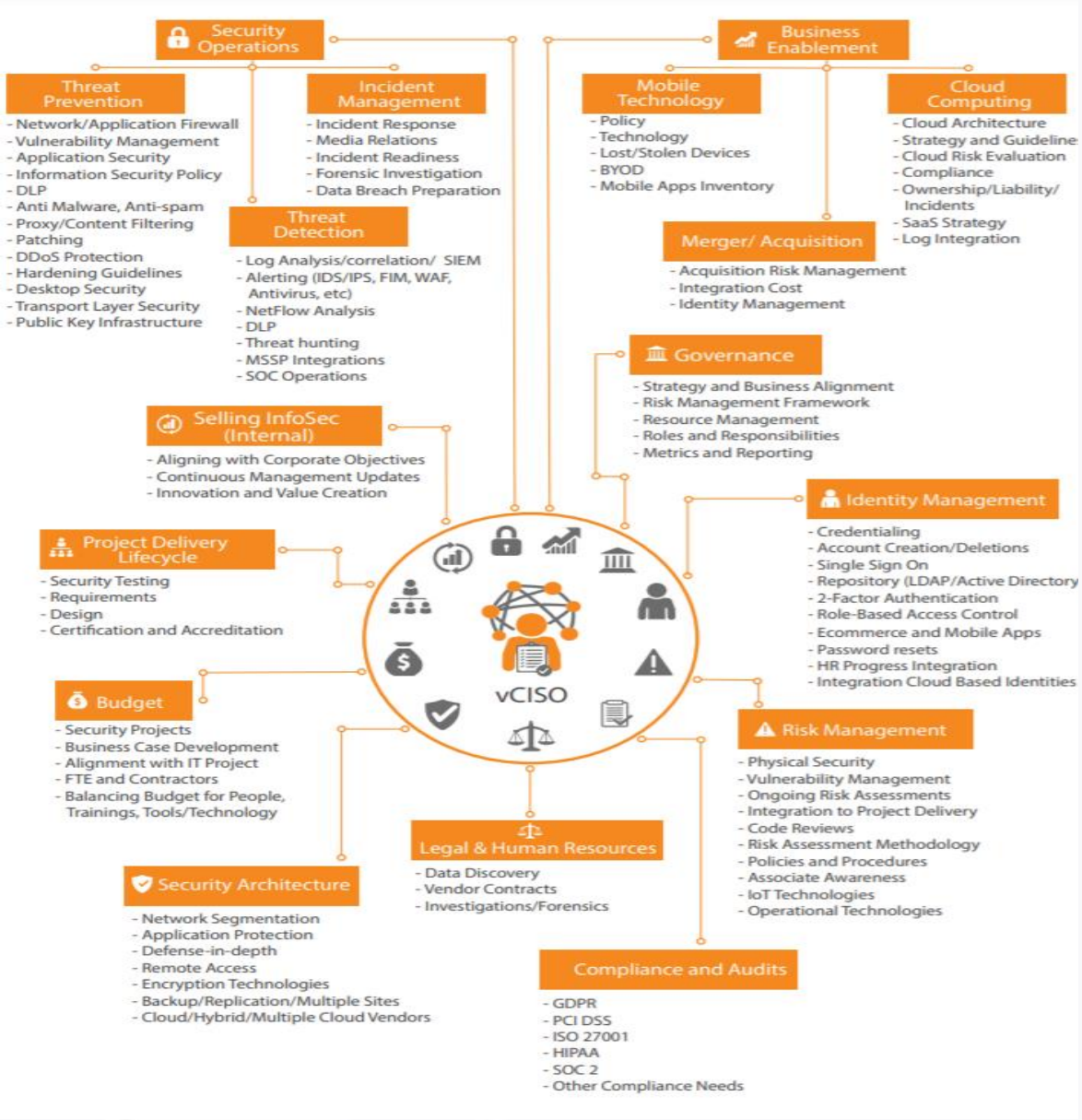
- ❑ Problem Discovery
- ❑ Contract Signed & Kick-off

General Consulting T&M, based on Scope

400/h (min $4K)

- ❑ Digital Transformation Cyber Resiliency For Boards & C-Suites
- ❑ Cyber Resiliency and Business Continuity
- ❑ Security Program Strategy
- ❑ Risk optimization
- ❑ Building Coordinated Protection
- ❑ Enterprise Incident Management
- ❑ Hybrid Cloud Security
- ❑ Secure and Compliant Cloud adoption
- ❑ Secure Cloud Migration
- ❑ Industrial and IoT security

CONSULTING SERVICES



Cyber Falcon

APPENDIX A: PENETRATION TEST

APPENDIX A: PENETRATION TEST

Full-scale Organization Penetration Testing components/tests provided

- **External and internal vulnerability scanning** to detect all the outdated and unpatched informational systems visible inside and outside the customer network perimeter and exploitable by malicious actors.
- **Network traffic sniffing** to uncover possible ways of sensitive data interception through unencrypted traffic.
- **Remote administration tools security assessment** to check security misconfigurations during work-from-home period caused by COVID-19.
- **Check access to sensitive data inside the customer network** to find overlooked gaps in data access security.
- **VPN security testing** to check security misconfigurations during work-from-home period caused by COVID-19.
- **DNS security assessment** to uncover misconfiguration and exposure to DNS-targeted attacks.
- **Email security assessment and alignment with best practices** to decrease probability of phishing attacks.
- **Accounts takeover attack** to expose domain controller misconfiguration
- **Cloud Security Audit for 3 platforms (Google Cloud Platform, Microsoft Azure, Amazon AWS)** to check if core business services hosted in these environments are vulnerable to internal and external threats or misconfigurations.
- **Social engineering with data exfiltration and lateral movement** to measure customer employees readiness to withstand deceiving human interaction.
- **Open source Intelligence (OSINT) on key employees** to uncover possible exploitation vectors by malicious actors and SaaS based products.

APPENDIX A: PENETRATION TEST

CYBERFALCON will assess the overall network security including the network perimeter devices residing on network segments and the Internet for potential vulnerabilities that could expose critical organizational systems and applications; customer information; organization information, and financial assets.

This assessment will be conducted combining the tools and techniques used by malicious "hackers" with disciplined scientific procedures to provide unique insight into the state of security in the customer Information Systems environment. During the Penetration testing CYBERFALCON will use our own software licenses (shown below in applicable sections).

The CYBERFALCON Penetration Testing will provide customer with a diagnosis of network vulnerabilities from an external hacker perspective (from the Internet into customer internal network) and from the internal provided connection. Network devices including firewalls, routers, switches, servers, printers, remote-access devices, mainframes, middleware, and backend services connected to the Internet (DMZ and LAN in case of internal penetration test) will all be assessed. During this project CYBERFALCON experts will be driven by following official standards and best practices:

The engagement will provide customer with an overall security assessment of the organization that addresses risk exposures noted during the evaluation. The results of this review will help strengthen the established security controls, standards, and procedures to prevent unauthorized access to the organizational systems, applications, and critical resources. As a result of our tests, the CYBERFALCON will prepare detailed work papers documenting the tests performed, a report of findings including recommendations for additional security controls as required.

#	Standard/Methodology	Link
1.	Penetration Testing Execution Standard	http://www.pentest-standard.org/index.php/Main_Page
2.	OWASP Application Security Verification Standard	https://www.owasp.org/index.php/Projects/OWASP_Application_Security_Verification_Standard_Project
3.	Information Systems Security Assessment Framework (ISSAF)	http://www.oissg.org/issaf
4.	SANS: Network Penetration Testing and Ethical Hacking	http://www.sans.org/security-training/network-penetration-testing-ethical-hacking-937-mid

APPENDIX A: PENETRATION TEST

Phases of Execution

Phase 1: *Footprinting* – The purpose of this phase is to gather relevant information about customer available on public resources. During this phase, we will create a complete profile of the customer security environment. Information related to customer Internet, intranet, remote access, and extranet will be identified. CYBERFALCON will identify all relevant network targets, domain names, network blocks, and customer Systems individual IP addresses that will be provided within the white-box conditions. Every new finding in this phase will be used to identify more opportunities to exploit.

Phase 2: *Enumeration and Network Reconnaissance* – During this phase of the assessment, CYBERFALCON will gather more specific information about customer network topology, active hosts, potential access paths into the networks, and the type of traffic that moves through customer networks. The main objective in this phase is to gather as much information as possible about the target networks and interconnected systems to start exploiting potential vulnerabilities. Specifically, during this phase, CYBERFALCON will perform DNS interrogation, NIC querying, and ICMP ping-swiping. This phase will be conducted in addition to possible extensions provided by customer scope of IP's.

Phase 3: *Network Scanning* – Once CYBERFALCON completes gathering information about the customer networks and related systems, CYBERFALCON will focus their attempts on specific servers at known IP addresses and specific openings on those servers such as unprotected shares and ports. During this phase, CYBERFALCON will identify the specific operating systems and applications used by various hosts as well as services that can be exploited. To accomplish this task, CYBERFALCON will use a variety of methods and tools to scan the networks and related hosts.

Phase 4: *Risk and Vulnerability Assessment* – During this phase, CYBERFALCON will consolidate, document, and analyze all the information gathered to develop an approach for focused attacks. At this stage, CYBERFALCON will also embark on the process of eliminating false positives by analyzing platform discrepancies, hacker return on investment and feasibility, potential vulnerabilities that have most likely been addressed in the latest patches, manual vulnerability identification and confirmation, etc. Specifically, once CYBERFALCON finishes analyzing all the information gathered during prior phases and potential vulnerabilities have been identified, CYBERFALCON will determine the level of risks related to all the found vulnerabilities. CYBERFALCON will meet with customer Management at this time to discuss and refine the scope of the subsequent phases of the project. CYBERFALCON and customer will agree on targets, scanning windows, obtain agreement on CYBERFALCON exploitation approaches and tools, and agree on a definition of success for the various attack vectors.

Phase 5: *Exploitation* – During this phase, CYBERFALCON will examine the documented vulnerabilities and potential security deficiencies on the various target hosts and determine which are more likely to be successful. At this point, we will notify customer about discovered vulnerabilities and ask for the right to develop this attack and exploit a selected number of the found vulnerabilities starting with the one with the highest level of risk to the one with the lowest level of risk.

Phase 6: *Documentation of Findings, Presentation to Management and Final Report* – CYBERFALCON will document the work using a detailed documentation methodology followed by standard industry practitioners. We will provide the detailed vulnerabilities prioritized by risk exposure. Additionally, we will prepare a formal report summarizing our findings and recommendations to enhance the security of customer external and internal networks. Furthermore, the results of our findings will be summarized for customer management with a formal presentation.

APPENDIX A: PENETRATION TEST

Social Engineering Attacks with Lateral Movement and Sensitive data hunting

CYBERFALCON will perform online and verbal phishing attacks using such methodology:

Phase 1: *Threat modeling* – The initial stage of any social engineering assessment is to assess the likely threats to a business. These threats may be theft from a warehouse, dumpster or attack on network resources from internal employees. In our case only online and phone attacks will be performed.

Phase 2: *Reconnaissance* – This phase of the assessment is concerned with collecting as much information about the business as possible. This information is primarily collected from public resources such as DNS records, search engines, forums and new groups.

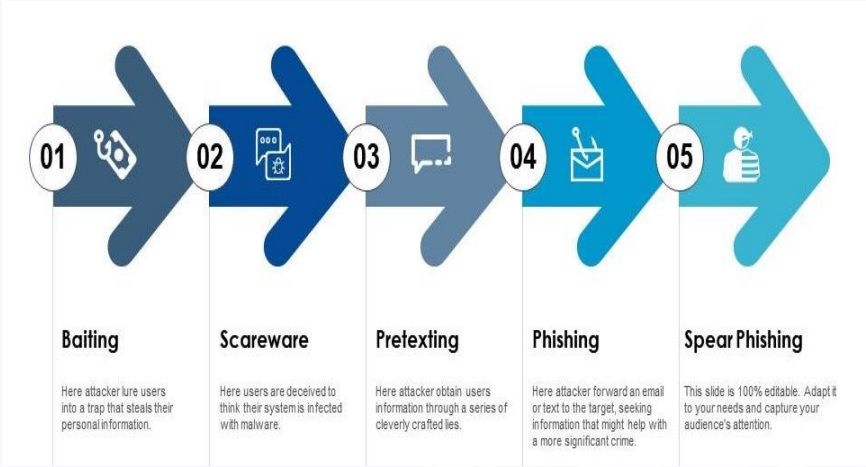
Phase 3: *Scenario creation* – The social engineers will use the gathered information and likely threats to the business and create possible scenarios to play out. These scenarios will be constructed to address a specific threat of the company to assess whether or not procedures are in place to protect against them.

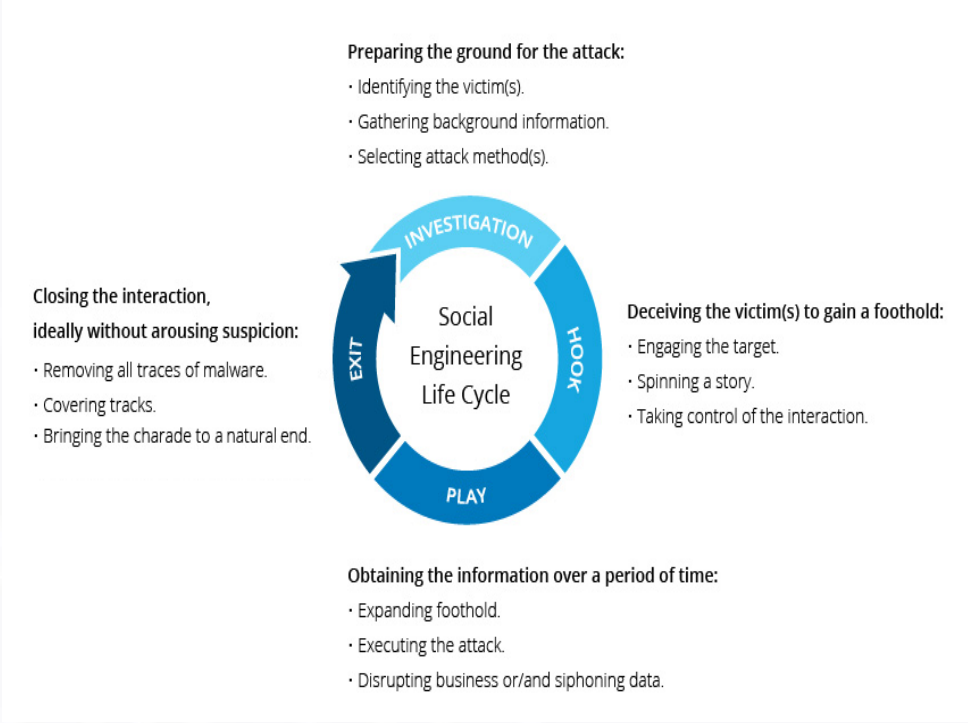
Phase 4: *Scenario execution* – Once the scenario has been constructed, the social engineers will play them out using a variety of techniques. The social engineering techniques used could include deception, pretexting, distraction and impersonation.

Phase 5: *Reporting* – After fully completing all scenarios the gathered information is used to construct a report detailing the results of the assessment. This report will show the scenario timeline, complete with vulnerability, exposure and remediation advice.
In scope targets will include web servers, database servers, network services, and Active Directory.

APPENDIX A: PENETRATION TEST

SOCIAL ENGINEERING ATTACKS WITH LATERAL MOVEMENT AND SENSITIVE DATA HUNTING





For **Social Engineering Testing,** the following Open Source software and frameworks will be used:

- Maltego – open source intelligence and forensics application.
- Kali Linux - Security Testing Distro with best open source tools
- SET – Social Engineering Toolkit
- The harvester - search engine information collecting tool
- Nmap dns-brute module
- Dnsmap - DNS reconnaissance tool

APPENDIX A: PENETRATION TEST

DELIVERABLES AND CLOSE-OUT PLAN

CYBERFALCON will provide reports with detailed information on identified gaps, their criticality, likelihood, and recommendation for improvement and review key findings and results during a facilitated discussion.

As an outcome of this project, we expect to deliver an aligned with client, clearly defined and approved remediation strategy that will help the organization to achieve its business goals and meet security compliance and best practices.

Key deliverables:

- Presentation and demo that represent key findings
- Screenshots and Video Proof of Vulnerability (PoV) and detailed description of how to reproduce security defect
- Vulnerabilities ranked by Risk level, CVSS v.3 rank
- Remediation recommendations, guidance and Technical references

Cyber Falcon

APPENDIX B: ARCTIC WOLF COMPARISON

	CYBERFALCON	Arctic Wolf
Technology	**Industry Leading SIEM, MDR, EDR, SOARs**	**Own, proprietary, not enterprise scalable**
24x7 availability	X	X
Concierge service (SOC analysts directly available)	X	X
Customized IR plan and playbook build with customer IT	X	X
Threat hunting	X	X
Dedicated account managers	X	X
Data enrichment	X	X
Threat intel	X	X
Triaging	X	X
Remediation guidance	X	X
Cloud security monitoring	X	X
All data can be hosted in customer facility (DC, Cloud)	X	
Cloud hosted option available	X	X
Customer portal		X
Tuning your security tools	X	
Response on incidents, contain and mitigate threat on your behalf	X	
SOAR of your choice (Phantom, Siemplify, Demisto)	X	
Offensive security capabilities (Ethical Hacking, Penetration Testing)	X	
Security hardening and implementation	X	
Compliance visibility and implementation capabilities (SOC2, ISO, HIPAA)	X	
Can support your existing security investment	X	
Vulnerability scanning	X	
Executive and board level cyber resiliency consulting	X	
Cloud security setup and hardening	X	
Self provisioning portal with all agents		
Cyber Resiliency training and program guidance	**X**	
Malware analysts	X	
Office 365 / Google apps & cloud API integration AWS cloud trail API integration	X	
Alerting via Slack or email enabled	X	
Deep Dark Web monitoring / leaked accounts monitoring	X	

Cyber Falcon

SERVICE DESCRIPTIONS

ENTERPRISE CYBER RESILIENCY SERVICES

Managed Detection & Response (MDR)

MDR is a 24x7 Security Monitoring Service as a subscription that delivers the proper people, process, and top SIEM technology for an effective security program. Security Analysts will continuously monitor and make customers aware of potential security incidents. The service will help customers implement best practices for the maintenance, monitoring, and analysis of audit logs as recommended by SANS and the Center for Internet Security (Critical Security Control #6). Additionally, the on-premises deployment includes a security controls dashboard that provides additional insight into seven of the CIS Critical Security Controls.

Key Benefits of 24x7 Security Monitoring Service are:

- Avoid the hassle
- Integrated workflow to analyze and respond to threats
- Saves Money
- Reduces capital investment in costly hardware and or dedicated security technology
- Affordable subscription-based service delivers exceptional return on investment (ROI)
- Get value on day one
- Access top security pros
- Continuous monitoring of log and event data to detect potential security incidents
- Daily and monthly reporting on security events and alerts
- Assistance with compliance needs regarding PCI DSS, HIPAA, and other industry regulations
- Ongoing monitoring of the security monitoring application
- Monthly review with Security Analysts covering the customer's overall security posture and overall system health
- Auditing IT infrastructure against Critical Security Controls for Effective Cyber Defense as recommended by SANS and the Center for Internet Security (Currently available for on-premises deployments only)

Our security monitoring team will realize the following elements of SOC mission:

- Continuously monitor: clearly visualize security posture with dashboards, key security indicators, static & dynamic thresholds, and trending
- Prioritize and act: optimize, centralize, and automate incident detection workflows with alerts, centralized logs, and pre-defined reports and correlations
- Conduct rapid investigations: use ad-hoc search and correlations to detect malicious activities
- Handle multi-step investigations: trace activities associated with compromised systems and apply the kill-chain methodology to see the attack lifecycle
- Manage Enterprise SIEM deployment
- View and manage alerts and incidents
- Initiate and manage tickets
- Response and react on incidents, isolate and block threats
- Track remediation outcomes

ENTERPRISE CYBER RESILIENCY SERVICES

Cyber Resiliency Consulting & vCISO

The objective of this service is to help the customer to harden the security posture and setup policy documents with a vCISO Service.

A Security Consultant works as an advisor and supervisor for all identified security measures necessary to effectively protect a company or client's assets. Security Consultants use their knowledge and expertise to assess possible security threats and breaches in order to prevent them and create contingency protocols and plans for when violations occur. Examples of supported areas are:

- Digital Transformation Cyber Resiliency For Boards & C-Suites
- Cyber Resiliency and Business Continuity
- Security Program Strategy
- Risk optimization
- Building Coordinated Protection
- Enterprise Incident Management
- Hybrid Cloud Security
- Secure and Compliant Cloud adoption
- Secure Cloud Migration
- Industrial and IoT security

-Pen Testing -Ethical Hacking -Vulnerability Assessment

CYBERFALCON will assess the overall network security including the network perimeter devices residing on network segments and the Internet for potential vulnerabilities that could expose critical organizational systems and applications; customer information; organization information, and financial assets.

This assessment will be conducted combining the tools and techniques used by malicious "hackers" with disciplined scientific procedures to provide unique insight into the state of security in the customer Information Systems environment. During the Penetration testing we will use our own software licenses (shown below in applicable sections). Penetration Testing will provide a diagnosis of network vulnerabilities from an external hacker perspective (from the Internet into customer internal network) and from the internal provided connection. Network devices including firewalls, routers, switches, servers, printers, remote-access devices, mainframes, middleware, and backend services connected to the Internet (DMZ and LAN in case of internal penetration test) will all be assessed.

Incident Response

The objective of this service is to help the customer in the first place to conduct Incident Forensics & Response, Ransomware recovery, assess and improve overall Security posture to mitigate any other potential entry points for attackers (Security Hardening service) to ensure the network, infrastructure and data is safe. Our professionals will work with the IT/Security team of the customer on-site to implement all required cybersecurity best practices in the company and to confirm that security remediation has prevented further breaches likely to be. We will employ both Offensive and Defensive teams at different stages of the project to meet the clients requirements and provide the best of the breed results in a limited time frame.

CONTACT INFORMATION

ENTERPRISE CYBER RESILIENCY SERVICES

Email: bizdev@cyberfalcon4u.com

Phone: 888-206-6120

Visit Us: https://cyberfalcon4u.com