



0101
1001
0110

cybertorch™

OVERVIEW

About Quzara Cybertorch™



Cybertorch offers full stack security and threat visibility.



Cybertorch's helps businesses meet Vulnerability Management & Security Monitoring requirements for FedRAMP, CMMC/NIST, and FISMA Compliance with inheritable controls.



Cybertorch is a turn-key solution addressing all facets of Vulnerability Management and Security Monitoring without hardware or staffing.

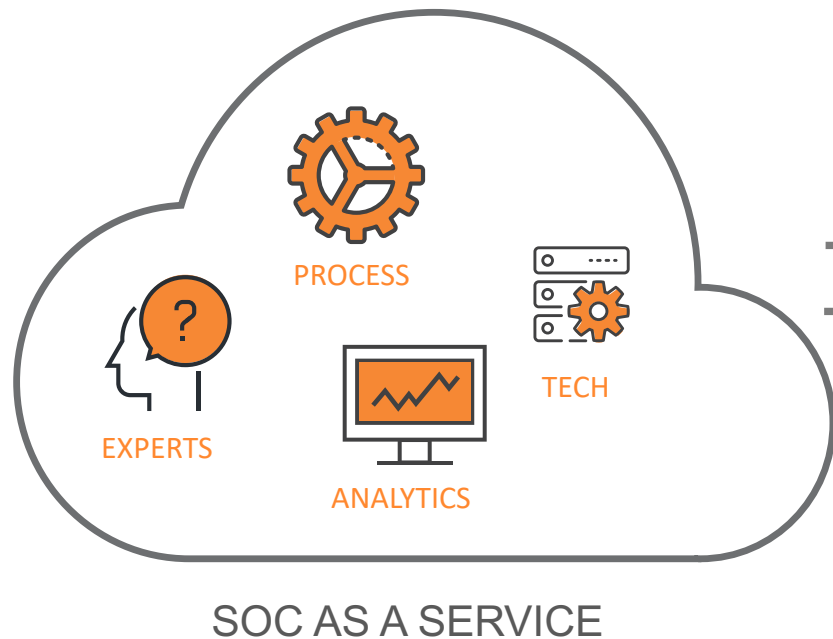


The Cybertorch information security team is available 24x7x365 to assist with rapid remediation to threats and vulnerabilities.



The monthly subscription service includes a dedicated portal for communication, alerts, reports and dashboards.

We Deliver Security Operations Capabilities



Ready-to-use services,
continuously updated

Economies of scale
for efficient
protection

SPEED

Actionable insights in days

- No staff to hire and train
- No tools to buy
- No data to clean and normalize
- No content to build and update

VALUE

Inherited compliance controls

Cybertorch™

Services Overview



Cybertorch delivers an industry leading Managed Security Operations Service.



Cybertorch develops customer configurations to collect and store data within customers boundary.



Cybertorch conducts data correlation to detect and investigate potential security incidents.

Cybertorch can deliver, and support, full end to end security coverage with in-house highly skilled security analysts along with leading edge security solutions utilizing Artificial Intelligence engines detect potential threats for deeper analysis by Cybertorch security experts.

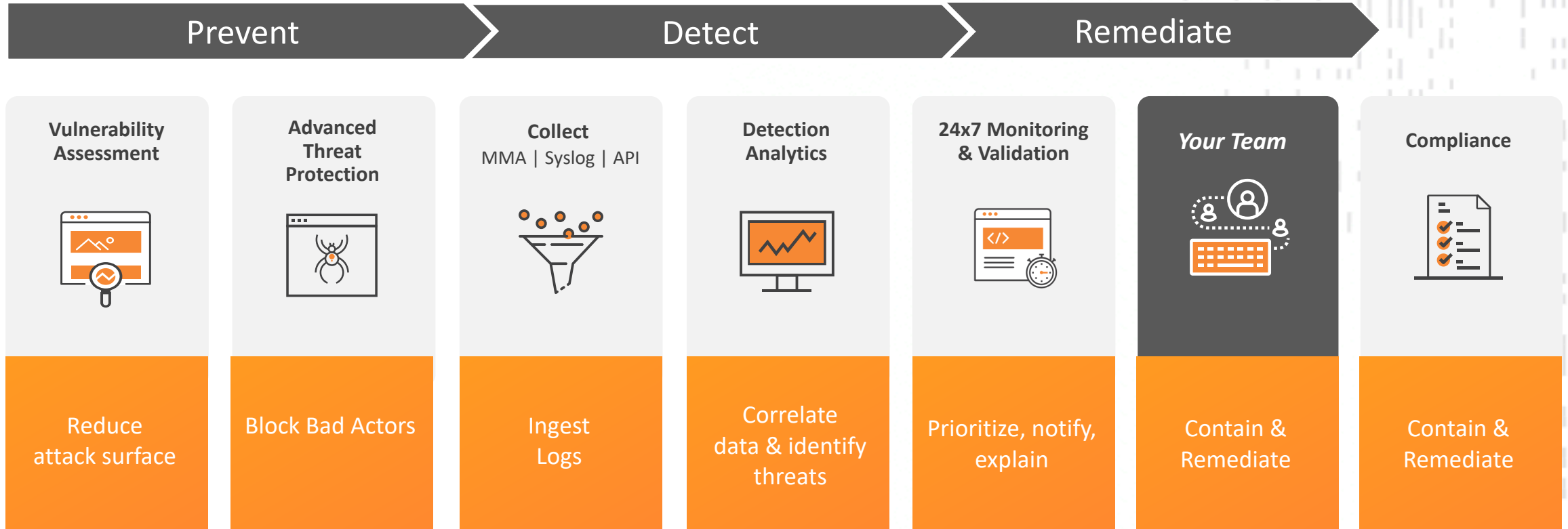
- ✓ **Enhanced protection of data security**
- ✓ **Automation processes to increase efficiency**
- ✓ **Faster detection of threats**
- Flexible and scalable technology**

Cybertorch™ Platform Overview

	PRODUCT CATEGORIES	KEY CAPABILITIES	MANAGED SERVICE
Applications	Office 365	Adaptive learning engine Compliance coverage (FedRAMP, NIST, CMMC, etc.)	SOC as a Service
Networks	MMA API	Powerful analysis for security logs Simple, intuitive search interface All your data accessible online, all the time	SOC as a Service
Systems	Firewall Intrusion Detection Vulnerability Assessment	Context aware threat identification Integrated vulnerability scanning PCI Approved Scanning Vendor certified	SOC as a Service

Cybertorch™ Solution

END TO END SECURITY & COMPLIANCE



Cybertorch Features



Increased Visibility & Analysis of Threats

- Threat detection
- Rule development
- Event source ingestion
- Event Triage (manual review)



Reporting and Configuration Review

- Review event source health/visibility
- Alert reports and review with customer
- Customer compliance & Incident dashboards



Additional Services

- Threat Hunting
- Forensic Investigation
- Vulnerability Analysis
- Automated response

Addressing Compliance Requirements

CYBERTORCH SOLUTIONS

	FedRAMP	800-171	CMMC
Level 1	<p>RA-5 Information System Vulnerability scanning</p> <p>RA-5(5) Privileged access authorization information system component for vulnerability scanning.</p>	<p>3.11.2 Information System Vulnerability scanning</p> <p>3.11.3 Provide remediation to vulnerabilities in accordance with patches.</p>	<p>RM.2.142 Information System Vulnerability scanning</p> <p>SA.3.169 Cyber Threat Intelligence tracking and response</p>
Level 2	<p>IR-2 Incident Response Training</p> <p>RA-03 Information System Risk Assessment</p> <p>SI-4 Information System Boundary Monitoring</p> <p>SI-5(1) Provides Organizations with Security alert and advisory information</p>	<p>3.4.7 Restrict/disable/prevent the use of nonessential programs, functions, ports, protocols and services.</p> <p>3.6.1 Track/report incidents to designated personnel to the organization.</p>	<p>AU.5.055 Identify Assets not reporting audit logs</p> <p>IR.5.108 A 24x7 Cyber Incident Response Team</p> <p>SI.5.223 Continuous monitoring Information system components</p>
Level 3	<p>SA-11(8) Dynamic Code Analysis to identify flaws</p> <p>SI-4(4) Maintain IDS/IPS to monitor and alert personnel;</p> <p>SI-4(16) Correlate Monitoring information for reveal otherwise unseen attack patterns</p> <p>SI-4(23) Host-based monitoring</p>	<p>3.13.13 Control and monitor the use of mobile code.</p>	<p>RM.4.150 Threat Intelligence to System Development Life Cycle</p> <p>SC.3.188 Control and monitor the use of mobile code</p> <p>SI.5.222 Detect execution of normal system commands and scripts the indicate malicious actions</p>

Cybertorch™ Security Operations Center providing Monitoring, Protection, and Reporting

Addressing Compliance Requirements

CYBERTORCH SOLUTIONS

	PCI DSS	SOX	HIPAA & HITECH
Level 1	<p>6.5.d Have processes in place to protect applications from common vulnerabilities such as injection flaws, buffer overflows and others</p> <p>6.6 Address new threats and vulnerabilities on an ongoing basis by installing a web application firewall in front of public-facing web applications.</p>	<p>DS 5.10 Network Security</p> <p>AI 3.2 Infrastructure resource protection and availability</p>	<p>164.308(a)(1) Security Management Process</p> <p>164.308(a)(6) Security Incident Procedures</p>
	<p>10.2 Automated audit trails</p> <p>10.3 Capture audit trails</p> <p>10.5 Secure logs</p> <p>10.6 Review logs at least daily</p> <p>10.7 Maintain logs online for three months</p> <p>10.7 Retain audit trail for at least one year</p>	<p>DS 5.5 Security Testing, Surveillance and Monitoring</p>	<p>164.308 (a)(1)(ii)(D) Information System Activity Review</p> <p>164.308 (a)(6)(i) Login Monitoring</p> <p>164.312 (b) Audit Controls</p>
Level 3	<p>5.1.1 Monitor zero-day attacks not covered by anti-virus</p> <p>6.2 Identify newly discovered security vulnerabilities</p> <p>11.2 Perform network vulnerability scans quarterly by an ASV or after any significant network change</p> <p>11.4 Maintain IDS/IPS to monitor and alert personnel; keep engines up to date</p>	<p>DS5.9 Malicious Software Prevention, Detection and Correction</p> <p>DS 5.6 Security Incident Definition</p> <p>DS 5.10 Network Security</p>	<p>164.308 (a)(1)(ii)(A) Risk Analysis</p> <p>164.308 (a)(1)(ii)(B) Risk Management</p> <p>164.308 (a)(5)(ii)(B) Protection from Malicious Software</p> <p>164.308 (a)(6)(iii) Response & Reporting</p>

Managed Security Services

CYBERTORCH™ PLATFORM OVERVIEW



APPLICATION SECURITY MONITORING

Our RASP Sensors provide deep visibility to source code, library risks. We also provide live threat detection and protection for your application.



VULNERABILITY MANAGEMENT

Dedicated security operations team who install, monitor and triage security scan reports and risks. Remediation reporting for actionable responses to meet risk and regulatory compliance needs.



CLOUD SECURITY MANAGEMENT

Monitor Cloud Identity, Virtual Machines, API Access and other vulnerabilities. Manage risk to authorized assets and services.



O365 + AZURE








We leverage Native Azure Cloud stack, with Azure Sentinel, AIP, ATP and Security Center to identify real-time risks to O365 and Azure workloads.



NETWORK SECURITY MONITORING

Real-time threat detection for your network. We use active and passive scanning techniques for Cloud and On-Prem Network Infrastructure.

Cybertorch™ Platform Overview

CATEGORY	DESCRIPTION	OUTCOMES	CHARGE MODEL
 MANAGED VULNERABILITY MANAGEMENT	We deploy Tenable scan solutions inside the Azure boundary. Configuring the scan engine, plugin updates, and provide reporting monthly.	2 weeks Vulnerability solution deployment, Custom Audits, Installation of container monitoring, Integration with JIRA or email, New Sensor installs.	Set –up + monthly Engineering Service Charge
 MANAGED FULL STACK SCANS	Monthly we perform Application, Database, and Operating systems security scans & quarterly compliance scans. Includes 4 hours of SME support.	Monthly risk-prioritized scans, Quarterly compliance scan reports for Application & Operating systems, SME support.	Monthly Service Charge[[
 MANAGED COMPLIANCE SCANS	Quarterly Compliance Scans of Operating Systems & Compliance-mandated services for DISA/CIS L1	Quarterly Compliance Scans for Application & Operating System. SME Support over 24 business hours.	[Monthly Service Charge
 DYNAMIC WEB APPLICATION SCANS	Scans of external facing customer web services & perimeter services.	Weekly risk-prioritized scan reports for external public assets in-scope. Authenticated scans for web applications. SME Support.	One-Time Charge
 PENETRATION STUDIES	Penetration studies for customers based on scope of environment.	Testing launched from Cybertorch™ Environment. Custom testing report – does not include attestation services.	Monthly Service Charge
 PATCH MANAGEMENT SERVICES RETAINER	Includes coordination between Cybertorch™ Information System Owner and End-Customer. Analysts provides support for remediation guidance.	SME Support, Research & Ticketing Support, Hours are tracked on weekly basis for billing	One-Time Charge
 MANAGED SOURCE CODE SCANS	We provide source code scans & IDE integrations for Customer Static Code Analysis. Customer gets access to a Source Code Dashboard & Ticketing integrations.	2 weeks IAST Sensor Deployment, 10 IDE Integrations included in pricing, 1 ticketing system (JIRA), Scan reports sent via email on weekly basis.	Monthly Service Char

0101
1001
0110

cybertorch™

THANK YOU

1-800-218-8528

info@quzara.com

www.quzara.com

8521 Leesburg Pike,
Suite #250,
Vienna, VA 22182



@QuzaraTech



/Quzara