



0101  
1001  
0110

cybertorch™

# OVERVIEW

# About Quzara Cybertorch™



Cybertorch™ offers full-stack security and threat visibility.



Cybertorch™ 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.

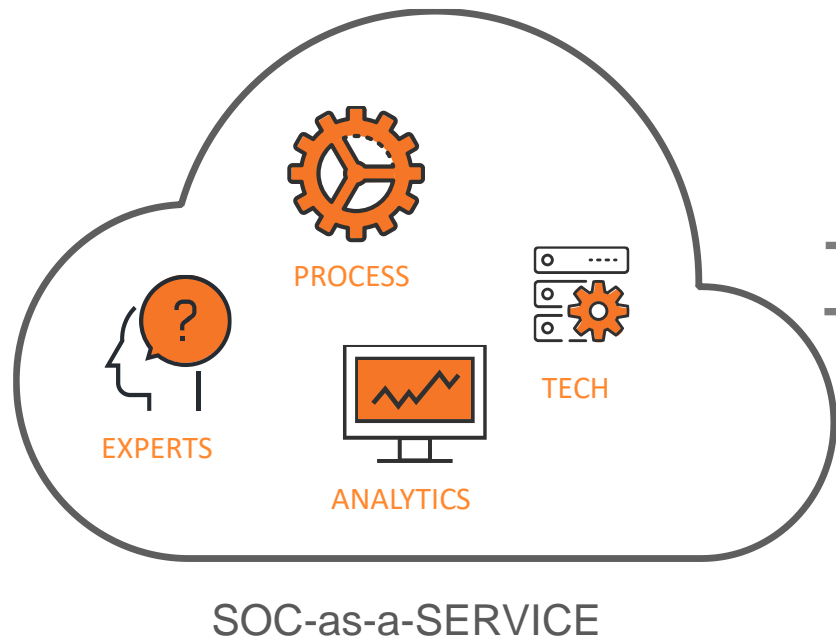


The Cybertorch™ information security team is available 24x7x365 to assist with rapid remediation to threats and vulnerabilities.



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



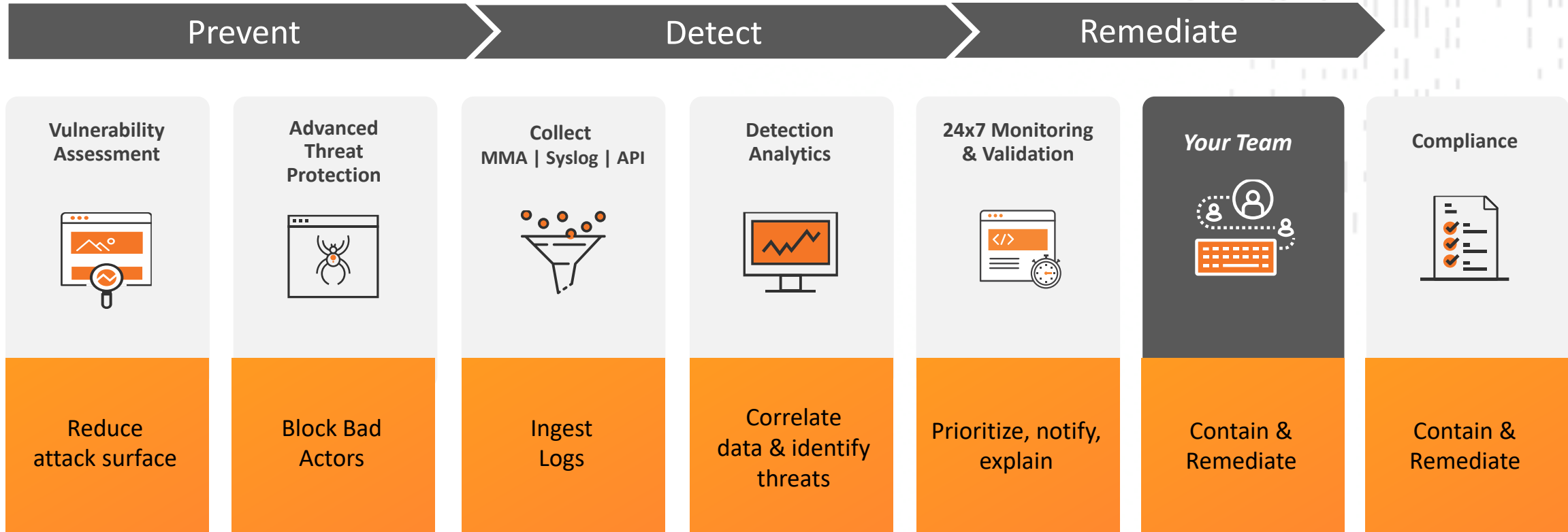
# M365 Hardening Requirements

CYBERTORCH SOLUTIONS

Scope	Hardening Services	Outcome
Email Security	<ul style="list-style-type: none"> <li>Security Configurations for EXO</li> <li>Malware Policies</li> <li>Safe Link Policies</li> <li>Message Encryption</li> </ul>	<ul style="list-style-type: none"> <li>Protect your email from SPAM/Phishing Attacks</li> <li>Protect against Malicious Attachments</li> <li>Stop Auto-forwarding of Emails</li> <li>Protect against Malware in Email</li> </ul>
Authentication	<ul style="list-style-type: none"> <li>MFA</li> <li>Password Policies</li> <li>Auditing of Password Compliance</li> <li>User Behavior Analytics</li> <li>Admin Account and Privileged Users</li> </ul>	<ul style="list-style-type: none"> <li>Protected Credentials</li> <li>Protect against Impersonation Attacks</li> <li>Tracks User Login Anomalies</li> <li>Force Compliance across user base with Password Policies</li> <li>Track/report incidents with security issues</li> </ul>
Endpoint Security	<ul style="list-style-type: none"> <li>Microsoft Endpoint Manager</li> <li>Device Compliance Policies</li> <li>Endpoint monitoring</li> </ul>	<ul style="list-style-type: none"> <li>Managed Devices</li> <li>Endpoint Detection</li> <li>Endpoint Incident Response</li> <li>Vulnerability Management on Endpoints</li> </ul>
OneDrive and SharePoint and Microsoft Defender for Cloud Apps	<ul style="list-style-type: none"> <li>External data shares</li> <li>Restricted Apps and Scored Apps</li> <li>Custom Policies for Microsoft Defender for Cloud Apps related to Data Loss</li> <li>Customer Policies Related to Cloud Usage</li> </ul>	<ul style="list-style-type: none"> <li>Enforcement of Compliance Policies</li> <li>External Drive Share Restriction</li> <li>Data Loss Protection</li> </ul>

# 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><b>RA-5</b> Information System Vulnerability scanning</p> <p><b>RA-5(5)</b> Privileged access authorization information system component for vulnerability scanning.</p>	<p><b>3.11.2</b> Information System Vulnerability scanning</p> <p><b>3.11.3</b> Provide remediation to vulnerabilities in accordance with patches.</p>	<p><b>RM.2.142</b> Information System Vulnerability scanning</p> <p><b>SA.3.169</b> Cyber Threat Intelligence tracking and response</p>
Level 2	<p><b>IR-2</b> Incident Response Training</p> <p><b>RA-03</b> Information System Risk Assessment</p> <p><b>SI-4</b> Information System Boundary Monitoring</p> <p><b>SI-5(1)</b> Provides Organizations with Security alert and advisory information</p>	<p><b>3.4.7</b> Restrict/disable/prevent the use of nonessential programs, functions, ports, protocols and services.</p> <p><b>3.6.1</b> Track/report incidents to designated personnel to the organization.</p>	<p><b>AU.5.055</b> Identify Assets not reporting audit logs</p> <p><b>IR.5.108</b> A 24x7 Cyber Incident Response Team</p> <p><b>SI.5.223</b> Continuous monitoring Information system components</p>
Level 3	<p><b>SA-11(8)</b> Dynamic Code Analysis to identify flaws</p> <p><b>SI-4(4)</b> Maintain IDS/IPS to monitor and alert personnel;</p> <p><b>SI-4(16)</b> Correlate Monitoring information for reveal otherwise unseen attack patterns</p> <p><b>SI-4(23)</b> Host-based monitoring</p>	<p><b>3.13.13</b> Control and monitor the use of mobile code.</p>	<p><b>RM.4.150</b> Threat Intelligence to System Development Life Cycle</p> <p><b>SC.3.188</b> Control and monitor the use of mobile code</p> <p><b>SI.5.222</b> 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><b>6.5.d</b> Have processes in place to protect applications from common vulnerabilities such as injection flaws, buffer overflows and others</p> <p><b>6.6</b> Address new threats and vulnerabilities on an ongoing basis by installing a web application firewall in front of public-facing web applications.</p>	<p><b>DS 5.10</b> Network Security</p> <p><b>AI 3.2</b> Infrastructure resource protection and availability</p>	<p><b>164.308(a)(1)</b> Security Management Process</p> <p><b>164.308(a)(6)</b> Security Incident Procedures</p>
	<p><b>10.2</b> Automated audit trails</p> <p><b>10.3</b> Capture audit trails</p> <p><b>10.5</b> Secure logs</p> <p><b>10.6</b> Review logs at least daily</p> <p><b>10.7</b> Maintain logs online for three months</p> <p><b>10.7</b> Retain audit trail for at least one year</p>	<p><b>DS 5.5</b> Security Testing, Surveillance and Monitoring</p>	<p><b>164.308 (a)(1)(ii)(D)</b> Information System Activity Review</p> <p><b>164.308 (a)(6)(i)</b> Login Monitoring</p> <p><b>164.312 (b)</b> Audit Controls</p>
Level 3	<p><b>5.1.1</b> Monitor zero-day attacks not covered by anti-virus</p> <p><b>6.2</b> Identify newly discovered security vulnerabilities</p> <p><b>11.2</b> Perform network vulnerability scans quarterly by an ASV or after any significant network change</p> <p><b>11.4</b> Maintain IDS/IPS to monitor and alert personnel; keep engines up to date</p>	<p><b>DS5.9</b> Malicious Software Prevention, Detection and Correction</p> <p><b>DS 5.6</b> Security Incident Definition</p> <p><b>DS 5.10</b> Network Security</p>	<p><b>164.308 (a)(1)(ii)(A)</b> Risk Analysis</p> <p><b>164.308 (a)(1)(ii)(B)</b> Risk Management</p> <p><b>164.308 (a)(5)(ii)(B)</b> Protection from Malicious Software</p> <p><b>164.308 (a)(6)(iii)</b> Response &amp; 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
 <b>MANAGED VULNERABILITY MANAGEMENT</b>	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
 <b>MANAGED FULL STACK SCANS</b>	Monthly we perform <b>Application, Database, and Operating systems security scans</b> & 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[[
 <b>MANAGED COMPLIANCE SCANS</b>	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
 <b>DYNAMIC WEB APPLICATION SCANS</b>	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
 <b>PENETRATION STUDIES</b>	Penetration studies for customers based on scope of environment.	Testing launched from Cybertorch™ Environment. Custom testing report – <b>does not include attestation services.</b>	Monthly Service Charge
 <b>PATCH MANAGEMENT SERVICES RETAINER</b>	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
 <b>MANAGED SOURCE CODE SCANS</b>	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