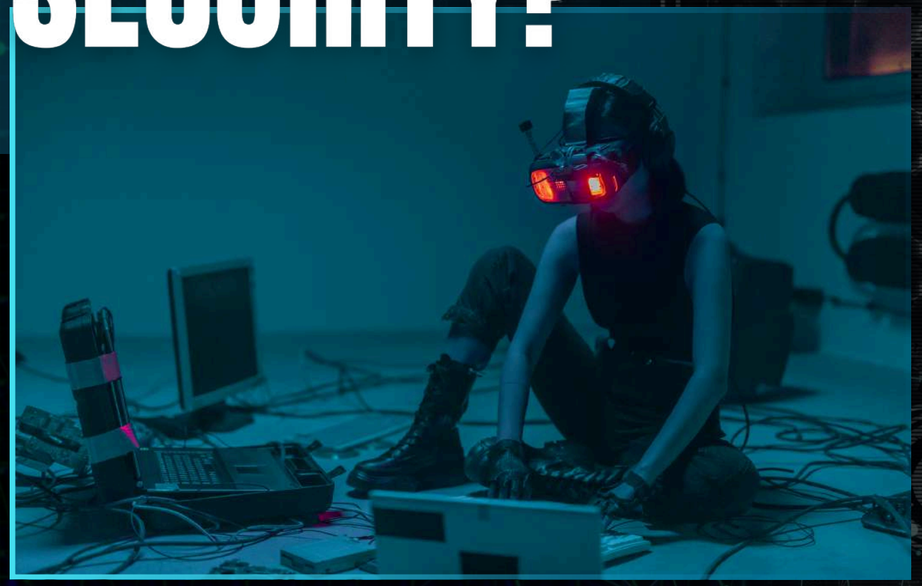
CYBER SECURITY

www.novatech-global.com

Novatech

WHAT IS CYBER SECURITY?



Cybersecurity is the practice of protecting computers, networks, systems, and data from digital attacks, unauthorized access, and malicious activities. It encompasses various technologies, processes, and practices designed to safeguard both organizations and individuals online.

Key aspects include network security, application security, information security, operational security, and disaster recovery. As cyber threats evolve, from ransomware to phishing attacks and data breaches, cybersecurity measures must continuously adapt to counter new risks.

Strong cybersecurity requires multiple layers of protection, including firewalls, antivirus software, encryption, and security awareness training. It's crucial for protecting sensitive information like financial data, intellectual property, and personal information from cybercriminals.

In today's interconnected world, cybersecurity is essential for maintaining privacy, trust, and business continuity in the digital age.

THREAT TYPES

Physical threats involve unauthorized physical access to systems, theft of devices, or damage to infrastructure. These can include break-ins, vandalism, or natural disasters.

Network threats target system connectivity and communication. Examples include DDoS attacks, man-in-the-middle attacks, and packet sniffing.

Software threats exploit vulnerabilities in applications and operating systems. These include malware, viruses, ransomware, and zero-day exploits.

Social engineering threats manipulate people into revealing sensitive information or granting access. Common tactics are phishing, pretexting, and baiting.

Insider threats come from within an organization, whether malicious employees or negligent staff who accidentally compromise security.

Configuration threats arise from misconfigurations in systems and networks that create security gaps. These often result from human error or poor security practices.

MANAGED SOC

The escalating complexity of cybersecurity threats has driven the need for greater visibility, resulting in an overwhelming volume of data and fragmented technology stacks. This fragmentation makes it challenging for security analysts to efficiently analyze, prioritize, and address vulnerabilities across multiple tools.

Novatech's Managed SOC solutions integrate real-time threat detection and response, advanced security analytics, and comprehensive endpoint protection into a unified platform. This streamlined approach provides organizations with a holistic, unobstructed view of their security posture, enhancing threat visibility and response capabilities.

Core capabilities

1. Consolidate and optimize your entire security toolset.
2. Minimize alert fatigue and prioritize critical threats.
3. Enhance your internal capabilities with expert cybersecurity support.
4. Gain a comprehensive, 360-degree view of your security posture.

SIEM

Designed for network-wide threat monitoring and forensic analysis.

XDR

Delivers a holistic view of security across all IT layers.

MDR

Enhances threat detection and response with Managed Detection and Response.

SOC

Optimized for full operational visibility and efficient incident management.

Endpoint Detection and Response

Novatech's Endpoint Threat Detection and Response solutions provide swift threat identification and mitigation by centralizing critical attack data within an intuitive, interactive interface.

Our platform visualizes the full attack timeline, traces malware propagation across processes and users, and consolidates all related communications. This comprehensive approach enables faster, more precise threat detection, response, and remediation.

CORE OUTCOMES

1. Continuously monitor endpoints to instantly detect suspicious activity and potential threats.
2. Gain full visibility with integrated remediation tools.
3. Identify security breaches in real-time by detecting anomalous behavior, eliminating reliance on periodic scans.
4. Accelerate response times and contain threats with automated response capabilities.
5. Leverage our team of experts to strengthen your threat detection and response.
6. Develop and apply detection rules across Windows, macOS, and Linux environments.
7. Reduce downtime, data loss, and financial impact from security breaches.

Endpoint Threat Analytics

Novatech's Endpoint Threat Analytics transforms endpoint security by delivering deep insights into endpoint behavior.

Our advanced analytics strengthen cyber threat protection, enhance overall security, and optimize endpoint defenses—empowering your organization to remain secure and resilient.

CORE OUTCOMES

1. Enhance incident response by rapidly assessing attack scope, identifying affected systems, and implementing targeted remediation.
2. Achieve real-time, comprehensive visibility into endpoint activities to detect anomalies and potential breaches.
3. Collect and store detailed endpoint data for in-depth forensic investigations and attack reconstruction.
4. Continuously refine security strategies based on evolving threats and actionable insights from endpoint data.

Network Threat Detection

Novatech's Network Threat Detection delivers deep visibility into network traffic, offering unmatched insights into network behavior.

Our advanced analytics strengthen cybersecurity defenses, enhance security measures, and optimize overall network performance.

CORE OUTCOMES

1. Quickly detect and block brute force attacks by identifying and restricting malicious IP addresses.
2. Prevent unauthorized access by blocking connections from unapproved geographic locations.
3. Identify and mitigate distributed denial-of-service (DDoS) attacks launched by botnets.
4. Monitor bandwidth usage to identify the causes of spikes or disruptions.
5. Diagnose and address network-related application performance issues.
6. Utilize historical data to create predictive models for optimal network expansion and upgrades.

MANAGED RISK

Novatech's Managed Risk solutions offer a proactive strategy designed to identify and neutralize cybersecurity risks effectively. Combining cutting-edge technology with expert guidance, this service ensures your organization stays resilient and secure by continuously monitoring, evaluating, and addressing potential vulnerabilities in your security posture.

Core capabilities

1. Assess the risk landscape throughout your entire organization.
2. Leverage advanced tools and technologies to detect threats before they cause significant damage.
3. Apply a risk-based strategy to strategically mitigate vulnerabilities.
4. Strengthen your first line of defense while fostering a cyber-aware workforce.

Vulnerability Management

Vulnerability management provides a comprehensive security approach, including regular reports and expert guidance to develop a prioritized action plan for addressing vulnerabilities.

Human Risk Management

Human Risk Management focuses on reducing risks linked to human factors within your organization. It offers a premium service with seamless implementation, on-demand training, role-specific programs tailored to different positions, and real-time feedback.

Vulnerability Management

For true cyber resilience, security and risk management leaders must ensure that risk is effectively measured and managed.

Novatech's Vulnerability Management solutions deliver the expertise, methodologies, technology, and support necessary to establish a practical risk appetite framework that prioritizes critical risks in alignment with your business needs.

CORE SERVICES

1. MONTHLY VULNERABILITY SCANNING

Internal and external vulnerability scans identify and prioritize security weaknesses specific to your organization.

- Uncover hidden threats across your entire attack surface.
- Surpass industry standards for vulnerability scanning effectiveness.
- Continuously enhance security measures to stay ahead of evolving threats.

2. PENETRATION TESTING + BREACH AND ATTACK SIMULATIONS

Expert-led simulated cyberattacks that identify vulnerabilities and validate your cyber resilience.

- Assess the likelihood of vulnerability exploits with monthly penetration testing.
- Gain insights into external threat perception through reputation scanning.
- Evaluate preparedness for real-world attacks.

3. SECURITY REPUTATION MONITORING

Gain an external perspective on how your organization's security is perceived, allowing for proactive action.

- Understand how hackers view your organization's security posture.
- Actively search for and eliminate global threats.
- Make informed decisions based on data collected by cybersecurity experts.

Human Risk Management

Managing human risk is a critical component of any risk management strategy.

Novatech's Human Risk Management solutions are designed to influence user behavior, foster a proactive approach to cyber risks, enhance overall cybersecurity awareness, and equip employees with the skills needed to quickly identify and mitigate cyber threats.

CORE SERVICES

1. CYBERSECURITY AWARENESS TRAINING

Cultivate a cyber-aware workforce through tailored education, testing, and reinforcement of cyber hygiene best practices.

- Customize training to your organization's needs.
- Use gamification and personalized content for better retention.
- Provide real-time feedback to correct mistakes.
- Access metrics and reports to identify high-risk employees.
- Integrate with Active Directory or via .csv for easy setup.

2. PHISHING SIMULATION EXERCISES

Phishing simulations are key to building cyber awareness. Novatech's services deliver realistic phishing attack scenarios to strengthen your organization's resilience and improve cyber awareness.

- Customize simulations to mirror daily scenarios for better engagement.
- Run regular, advanced phishing tests with minimal effort.
- Boost learning and phishing defense skills with instant educational feedback.

3. PHISHING REMEDIATION

Novatech's Phishing Remediation service streamlines phishing threat management. With Email Quarantine Automation (EQA), easily search, locate, and isolate malicious emails across all mailboxes with one click.

- Integrate seamlessly with top enterprise SaaS email platforms.
- Respond quickly to new and emerging email threats.
- Access a complete, end-to-end phishing defense solution.

MANAGED STRATEGY

Novatech's Managed Strategy combines customized cybersecurity services that are closely aligned with your business's strategic objectives. This solution offers an innovative approach to cyber resilience, emphasizing scalability, flexibility, and ongoing enhancement to address evolving digital threats.

Core capabilities

1. Align your cybersecurity strategy with business objectives and priorities.
2. Continuously adapt your strategy to emerging threats.
3. Develop a strategic roadmap designed for long-term growth.
4. Leverage the expertise of seasoned cybersecurity professionals.
5. Effortlessly navigate the regulatory compliance landscape.

vCISO

A vCISO provides the strategic direction and leadership of a Chief Information Security Officer in a virtual and more accessible format. This service is essential for businesses needing expert guidance without the resources for a full-time executive position.

InfoSec Advisor

Focusing on future-proofing your information security policies, InfoSec Advisory services ensure your strategy is customized to address current challenges while remaining flexible to adapt to future needs.

vCISO

Novatech's vCISO service offers the vision and guidance necessary to navigate today's complex threat landscape. Combining extensive expertise with strategic foresight, this service provides a tailored approach to cybersecurity leadership.

Take a proactive approach to digital resilience by equipping your organization with the tools and insights needed to confidently address current challenges and stay resilient against future threats.

CORE SERVICES

1. RISK ASSESSMENT

Risk assessments provide a deep dive into your organization's resilience, helping you identify and mitigate potential disruptions while ensuring strong business continuity.

- Comprehensive organization-wide risk evaluation.
- Detailed reporting on key findings and liabilities.
- Strategic recommendations for risk mitigation and planning.

2. POLICY DEVELOPMENT

Novatech's Policy Development service creates a resilient cybersecurity framework tailored to your organization's needs, going beyond compliance to integrate security into your company culture.

- Develop customized cybersecurity policies aligned with your business goals
- Ensure policies meet and exceed industry standards and regulations
- Promote a cyber-aware workforce, strengthening your first line of defense

3. CYBERSECURITY PROGRAM DEVELOPMENT

Develop your cybersecurity program with Novatech's vCISOs, avoiding full-time executive costs. Tailored strategies ensure alignment with business goals and long-term cyber resilience.

- Modernize your approach to security program management.
- Address current cybersecurity challenges effectively.
- Build an agile foundation ready to adapt to evolving threats.

InfoSec Advisory

InfoSec Advisory services provide a comprehensive evaluation of your security posture's maturity, uncovering hidden gaps and vulnerabilities.

Going beyond traditional advisory services, this offering delivers a data-driven, in-depth perspective on your cybersecurity risks, empowering you to strategically enhance and evolve your security posture.

CORE SERVICES

1. BUSINESS IMPACT ANALYSIS

Novatech's analysis identifies critical processes and resources, ensuring resilience and continuity.

- Define project scope with Novatech experts
- Analyze key functions and resources
- Receive tailored advice and next steps in a strategy meeting

2. SECURITY POSTURE ASSESSMENT

Novatech's assessment evaluates your security controls, providing actionable insights to enhance maturity and ensure ongoing protection.

- Define security goals with experts
- Evaluate security infrastructure
- Review findings in a detailed report

3. CYBERSECURITY PROGRAM DEVELOPMENT

Novatech's services prepare your organization for cyber threats by simulating real-world scenarios, ensuring swift and effective response.

- Develop incident response plans with experts
- Participate in interactive cyber-attack simulations
- Receive feedback and improvement strategies post-exercise

ZERO TRUST ARCHITECTURE

Adopt a modern Zero Trust security framework that eliminates implicit trust and ensures least privilege access. Assess your security maturity, implement strong authentication, network segmentation, and continuous monitoring to protect users, devices, and applications. Strengthen security for remote access and hybrid environments with strict controls and intelligent policies.

Zero Trust Architecture

A modern security framework that eliminates implicit trust, ensuring strict identity verification and least privilege access across all users, devices, and applications.

CORE SERVICES

1. ZERO TRUST MATURITY ASSESSMENT
   Evaluate your current security posture and develop a roadmap to implement a Zero Trust model tailored to your business needs.
2. IDENTITY & ACCESS MANAGEMENT (IAM)
   Enforce secure authentication, multi-factor authentication (MFA), and least privilege access to protect user identities and prevent unauthorized access.
3. MICROSEGMENTATION & NETWORK SECURITY
   Restrict lateral movement within your network by segmenting access based on user identity, device, and security policies.
4. CONTINUOUS MONITORING & LEAST PRIVILEGE ACCESS
   Implement real-time monitoring and dynamic access controls to ensure users only have the minimum permissions required for their roles.
5. ZERO TRUST ENDPOINT & APPLICATION SECURITY
   Protect endpoints and applications with strict access controls, behavioral analytics, and zero-trust enforcement policies.
6. SECURE ACCESS SERVICE EDGE (SASE)
   Integrate network security and cloud security to provide secure, identity-based access to applications from any location.
7. ZERO TRUST FOR REMOTE WORKFORCES
   Secure remote users with identity-driven access controls, endpoint security, and encrypted communication to prevent unauthorized access.

FUTURE TRENDS

1. AI IN SECURITY

AI automates threat detection and response, analyzing data to identify anomalies quickly. This technology enhances proactive defense, reducing cyberattack mitigation time and safeguarding digital assets effectively.

2. QUANTUM ENCRYPTION

Quantum encryption uses quantum mechanics for secure data transmission, making interception nearly impossible. It ensures robust security with quantum keys, vital as quantum computing advances.

3. ADVANCED THREATS

Cyber threats evolve with sophisticated tactics like ransomware and supply chain attacks. A multi-layered approach combining traditional defenses and innovative tech is crucial for protecting critical assets.

YOUR TRUSTED PARTNER

ALL SYSTEMS SECURE

Novatech delivers cutting-edge cybersecurity services to protect organizations against evolving digital threats. Our expert team specializes in vulnerability assessments, penetration testing, security audits, and incident response.

Our comprehensive approach includes advanced threat detection, 24/7 security monitoring, and tailored security awareness training for employees. We help businesses strengthen their security posture through state-of-the-art technologies and industry best practices.

We understand that each organization faces unique security challenges. Our customized solutions ensure compliance with international security standards while maintaining operational efficiency.

From ransomware protection to cloud security, we safeguard your digital assets and maintain your business continuity.

GET IN TOUCH WITH US!

info@novatech-global.com

320 Boston Post Rd Suite 180, Darien
CT 06820 | United States