WHITE ROCK CYBERSECURITY

NJECC
Leading, Inspiring, & Transforming Education through Technology

Bitdefender

Bitdefender Managed Detection & Response PLUS (MDR, SOC)

Your organization's most important assets may be for sale on the dark web. **Bitdefender Managed Detection and Response PLUS** gives you all the protections of Bitdefender MDR and then seamlessly integrates comprehensive dark web detection, response and more into your service. A specialized Cyber Intelligence Fusion Cell (CIFC) unit gathers, synthesizes, and analyzes global intelligence data to provide complete protection outside your environment. A dedicated Security Account Manager (SAM) and Professional Services onboarding provide additional, personalized service.

Bitdefender MDR PLUS includes:

All the benefits of Bitdefender MDR are included

24x7 Security Account Manager – Dedicated SAM is your single point-of-contact, there to address your questions or concerns and provide a quarterly business review (QBR).

Professional Service On-boarding - Professional services team provides detailed support and guidance to quickly and accurately on-board your organization onto the service

Global Threat Intelligence Feeds & Analysis – Cyber Intelligence Fusion Cell (CIFC) utilizes the threat intelligence lifecycle to research cyber threats, geopolitical activity, and industry-specific data trends and then apply this knowledge to your organization.

Dark Web Monitoring - Continuously monitor the dark web to detect leaked or stolen organizational data, including domains, credentials, intellectual property (IP), brand references and typo-squatting, technology stack, and industry and geography concerns.

Security Baselining and Tailored Threat Modeling - Collect and process information about your organization, including your business, users, and known threats, to model and monitor your specific threat landscape.

Brand and IP Protection - Continuously monitor your most valuable assets to detect and notify you of what is being shared or sold on the dark web.

High Priority Target Monitoring - Continuously monitor high-value employees for information that may have been stolen or leaked.

Comprehensive reporting intelligence hunts, Quicklooks (dark web report), Tippers (industry-specific research and recommendations), and Requests for Information (customer requested)

Beginning on November 21, 2024, Bitdefender will add the new Bitdefender MDR Cybersecurity Breach Warranty coverage to our Bitdefender MDR and Bitdefender MDR PLUS service subscriptions, in partnership with Cysurance, at no additional charge for all current and future MDR and MDR PLUS customers.

Customers are eligible for up to $100,000 for MDR, and up to $1,000,000 for MDR PLUS or MDR customers with 1000+ endpoints, in financial assistance in the event of a security incident.

MDR: Ransomware event $100,000
MDR PLUS: Compliance event $200,000; Ransomware event & BEC event $200,0000; Cyber Legal Liability event $500,000; Business Income event $100,000

Odessa Criales-Smith | odessa@wrsecure.com | 214-613-1568

Bitdefender

Service Component	MDR	MDR Plus
Industry leading security platform	☐	☐
24x7 SOC	☐	☐
Pre-approved Actions (PAAs)	☐	☐
Threat Hunting	☐	☐
Expert Recommendations	☐	☐
Incident Root Cause & Impact Analysis	☐	☐
MDR Portal & Reporting	☐	☐
24x7 Security Account Manager (Customer Success)		☐
Professional Services On-boarding		☐
Global Threat Intelligence Feeds and Analysis		☐
Dark Web Monitoring		☐
Security Baselining and Tailored Threat Modeling		☐
Brand & IP Protection		☐
High Priority Target Monitoring		☐
XDR Sensors	Add-ons	Add-ons

Bitdefender Penetration Testing

Bitdefender Pen testing scans vulnerabilities to identify potential security gaps, for instance, misconfigured systems or flawed applications. Testers then use the tactics of actual attackers to penetrate further into the system, which can reveal the extent of potential damage and test the resilience of existing security measures. Sometimes, the assessments go even beyond digital vulnerabilities, like examining physical security protocols and the effectiveness of staff training against social engineering tactics. A professional pen test offers a detailed report with the discovered vulnerabilities, the methods employed to exploit them, and strategic recommendations for remediation.

Types of Pen Testing

Pen testers assume various perspectives in the attack scenario - from anonymous attackers to insiders with full access, and from this point of view, the following types have emerged:

Black-box Testing (also known as Closed-box Testing): In this scenario, attackers have no background information other than the target's name, so the pen test simulates an external attacker with no internal system knowledge, typically limited to the target URL or IP addresses.

Grey-box Testing: This method blends external and internal attack perspectives, offering testers partial system information, such as user credentials or system documentation.

White-box Testing (also referred to as Open-box Testing): Grants testers extensive system information, including source code and architecture diagrams. This deep dive into the system's security uncovers vulnerabilities that are not apparent to external or less-informed attackers.

WHITE ROCK CYBERSECURITY

NJECC
Leading, Inspiring, & Transforming Education through Technology

Bitdefender

Various Pen Testing Classifications:

Automated vs. Manual Pen Testing: The approach to uncovering vulnerabilities can vary significantly, using both automated and manual testing methods. Automated testing relies on software tools to scan for known vulnerabilities across a wide range of systems quickly, while manual testing involves targeted exploration by testers to identify complex security issues that automated tools may not detect.

Internal vs. External Penetration Testing: Penetration testing can be categorized based on the attacker's perspective. External penetration testing simulates attacks that could be initiated from outside the organization, aiming to identify vulnerabilities in publicly accessible assets like websites, web applications, and external network services. Internal penetration testing focuses on the potential threats from within the organization's network. It evaluates what an insider attack could achieve or the damage an external attacker could cause once they've bypassed the initial external defenses.

Based on the IT environment's specific components that are tested, the common types include:

Web Application Penetration Testing targets applications interfacing with user data to uncover exploits within the app's functions, APIs, and data flow.

Network Penetration Testing focuses on interconnected systems and devices within an organization.

Web Service Penetration Testing examines web services that are essential for application interactions so that it can identify security risks in data handling and schemas.

Wireless Penetration Testing evaluates wireless network security for risks associated with public network access points.

Mobile Application Penetration Testing concentrates on mobile apps' vulnerabilities that could expose user data.

IoT Penetration Testing targets Internet of Things (IoT) devices, which are increasingly targeted in cyberattacks for their potential to compromise networks.

Thick Client Penetration Testing reviews applications with local and server-side components for common vulnerabilities like XSS and SQL Injection.

Contact Odessa for an NJECC-discounted quote or to request a demo:

White Rock Cybersecurity

odessa@wrsecure.com | 214-613-1568

Bitdefender annual subscriptions

NJECC Bitdefender Enterprise w/ EDR $11.89 each
NJECC Bitdefender MDR $25.49 each
NJECC Bitdefender MDR Plus $61.89 each
NJECC Bitdefender Patch Mgm $6 each
NJECC Bitdefender Full Disk Encryption $3 each

Bitdefender Pen Testing annual subscriptions

NJECC Perimeter Network, small $2500
NJECC Perimeter Network, medium $3750
NJECC Perimeter Network, large $5000
NJECC Internal Network, small $2500
NJECC Internal Network, medium $6250
NJECC Internal Network, large $12,500

*Call for pricing on Server Security Assessment, Grey-Box Web Application Pen Testing and more!