

Digital Defense Strategies: A Proactive Approach



Christos Bakomitros



Presales Engineer



Data-Ally



C.Bakomitros@data-ally.com +357 22 441514




data.ally

Introduction

"The Dynamic Cyber Threat Landscape"



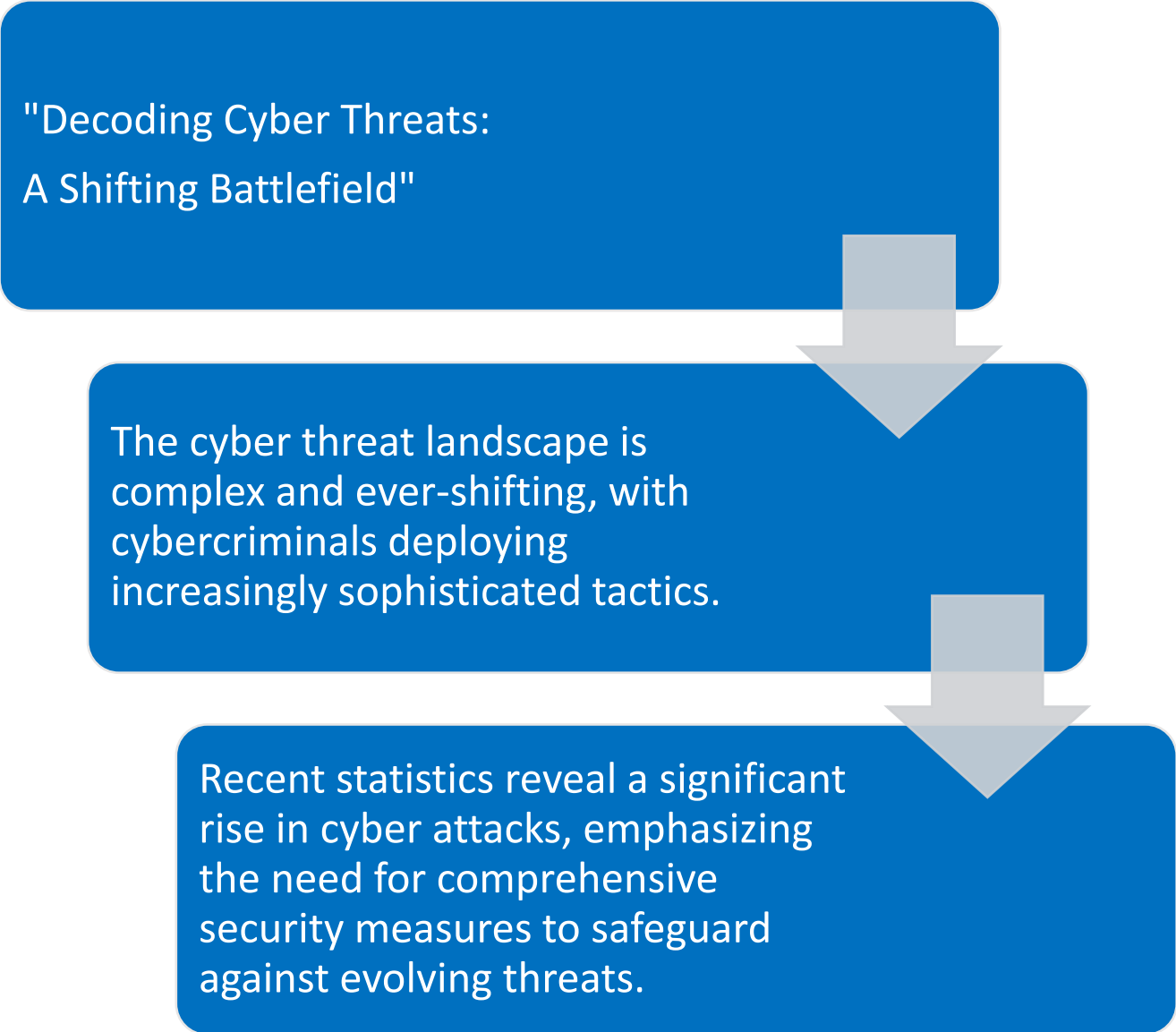
From sophisticated phishing attempts to advanced malware, the challenges are diverse and require proactive measures for effective defense.



In the ever-evolving world of cybersecurity, companies face a multitude of dynamic threats that demand constant attention and vigilance.

Understanding the Threat Landscape

"Decoding Cyber Threats:
A Shifting Battlefield"



The cyber threat landscape is complex and ever-shifting, with cybercriminals deploying increasingly sophisticated tactics.

Recent statistics reveal a significant rise in cyber attacks, emphasizing the need for comprehensive security measures to safeguard against evolving threats.




Challenges Faced by Companies

"Navigating Challenges in the Cyber Battlefield"

Companies encounter various challenges in the cyber battlefield, including data breaches, ransomware attacks, and intellectual property theft.

Real-world examples highlight the impact of cyber threats on businesses, emphasizing the urgency for robust cybersecurity solutions.



The Proactive Approach



"REDEFINING SECURITY: A PROACTIVE STANCE"



SHIFTING FROM A REACTIVE TO A PROACTIVE CYBERSECURITY APPROACH IS PARAMOUNT. A PROACTIVE STANCE INVOLVES ANTICIPATING POTENTIAL THREATS AND TAKING PREVENTIVE MEASURES.



COMPANIES MUST STAY AHEAD OF CYBER ADVERSARIES, STRATEGICALLY PLANNING THEIR DEFENSE TO MITIGATE RISKS BEFORE THEY ESCALATE.

The Need for Continuous Testing

- "Continuous Testing: Safeguarding Your Digital Frontier"
- Continuous testing stands as a foundational pillar in cybersecurity resilience, offering a proactive approach to identifying and mitigating vulnerabilities.
- This methodology allows organizations to stay ahead of potential threats, ensuring a robust defense against an ever-changing threat landscape.

The image features a stylized graphic of a hand holding a glowing blue digital waveform. The hand is rendered in a light, semi-transparent style, with the fingers curled around the waveform. The waveform itself is composed of multiple parallel, wavy lines that create a sense of motion and energy. The background is a light gray color with a pattern of golden-brown circuit traces and small white dots, suggesting a digital or technological environment. In the upper left quadrant, there is a small blue square containing a white circle, with the binary code '10110101' written in white next to it.

Introducing SecPoint Penetrator

- "SecPoint Penetrator: Your Strategic Cyber Ally"
- Enter SecPoint Penetrator, a cutting-edge cybersecurity solution designed to fortify your digital defenses.
- This powerful tool goes beyond traditional security measures, offering comprehensive features to ensure continuous testing and threat detection.

Product

Protector™ UTM firewall
appliance



Penetrator™ vulnerability
scanner and assessment



SECPPOINT[®]
www.secpoint.com

Portable Penetrator™ WIFI
pen testing



Cloud Penetrator™



Vulnerability Scanner & WiFi Pen Testing Report

SAMPLE VULNERABILITY SCANNING Summary Report



Scan Summary Report

Confidential

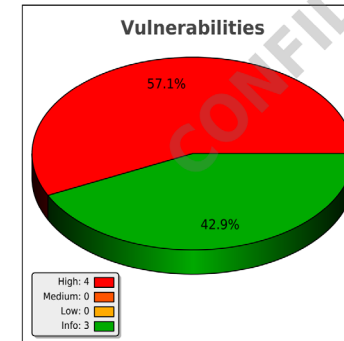
Scan Name		Audited on	2023-05-23 17:00:00
Scan Profile	Best Scan		
Scan Engine	SecPoint	Firmware Version	1.0.0
Audited Targets			

Overall Risk Level: High (Critical Level). Your system security level is dangerously low. It is possible for intruders to fully penetrate the system which can result in loss of private and sensitive data. It is recommended that you take immediate action to improve the security level.

Compliance result: ❌ **The Scan is Not Compliant**

Vulnerabilities: 7 potential vulnerabilities identified, with the following risk levels:

High: 4
Medium: 0
Low: 0
Information: 3



If you wish to view a detailed report of your scan or change your scan details, you can login to your SecPoint® Penetrator

Vulnerability Scanner

You can choose between 19 different vulnerability scanning profiles.



Profile can help you to perform quick and fast scans that will give a brief overview of vulnerabilities. You can also perform the recommended Normal Scan or more intensive Full Firewall Scan which are safe to run in production environments. If you need to test the strength of your firewall and systems the Aggressive Scan profile can help with that. We also have several compliance scanning profiles that can be deployed.



If you are not sure which scanning profile is best in your network security environment just feel free to contact us to get support

Profile 1 - Best Scan - Popular Ports

Profile 2 – Lethal HTTPS Web Attack Scan

Profile 3 – SSL & CMS Web Scan – Wordpress – Joomla

Profile 4 – Wordpress Web Scan

Profile 5 – Quick Scan

Profile 6 – Full Scan

Profile 7 – Firewall Scan

Profile 8 – Aggressive Scan

Profile 9 – OWASP 10 2021 Scan

Profile 10 – PCI-DSS Preparation for Web Applications

Profile 11 – HIPAA Policy Scan for Compliance

Profile 12 – SCADA ICS PLC IoT

Profile 13 – CWE 2011 Compliance

Profile 14 – ISO 27001 Compliance

Profile 15 – NIST 800-53/FISMA Compliance

Profile 16 – Controls v8.0 Compliance

Profile 17 – GLBA Integrity Compliance

Profile 18 – SSL Security Checks

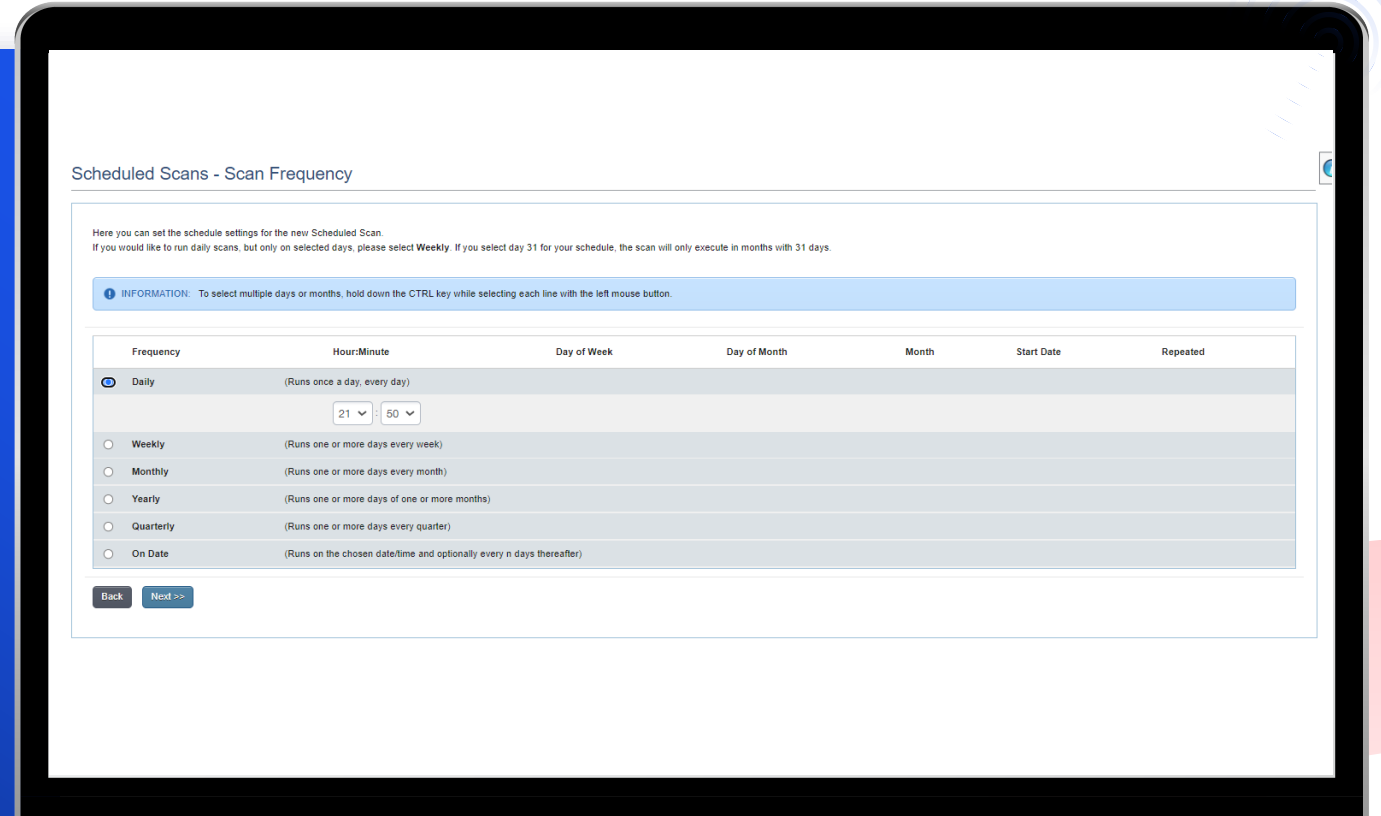
Profile 19 – VoIP Devices

Schedule



Easy to setup scheduled scanning they can choose based on compliance

- Daily
- Weekly
- Monthly
- Yearly
- Quarterly
- on specific dates



Node Scanning

The screenshot shows the SecPoint Penetrator web interface. The left sidebar contains navigation options: Home, Vulnerability Scanner (10), Schedule, Node Scanning (selected), Autonomous Sonar Robot, AI Machine Learning Robot (2), Statistics (2), Tickets (3), WiFi Pen Test (15), Firewall, Multi User (6), System (16), Network Setup, Update (4), Support (18), and Privacy. The main content area is titled 'Node Scanning' and has tabs for 'Main Penetrator' and 'Node Penetrator'. Below the tabs, there is an informational message: 'Here you can configure this Penetrator as a Main of one or more Node Penetrators. When a Main-Node environment has been configured, it's possible to launch a Vulnerability scan on the Node units.' A 'License and Node Scanning' button is visible. An 'INFORMATION' box states: 'For this feature to work, it is necessary that port 443 is reachable on the remote Penetrator and not blocked by a firewall.' Below this is a table for 'Node Penetrators' with columns for 'IP Address or CIDR', 'Hostname', and 'Description'. A 'Delete' button is located below the table. At the bottom of the interface, there is a diagram showing a central node connected to several other nodes, representing a distributed scanning environment. The footer of the interface reads '© 1998-2023 SecPoint®. All rights reserved - Disclaimer'.



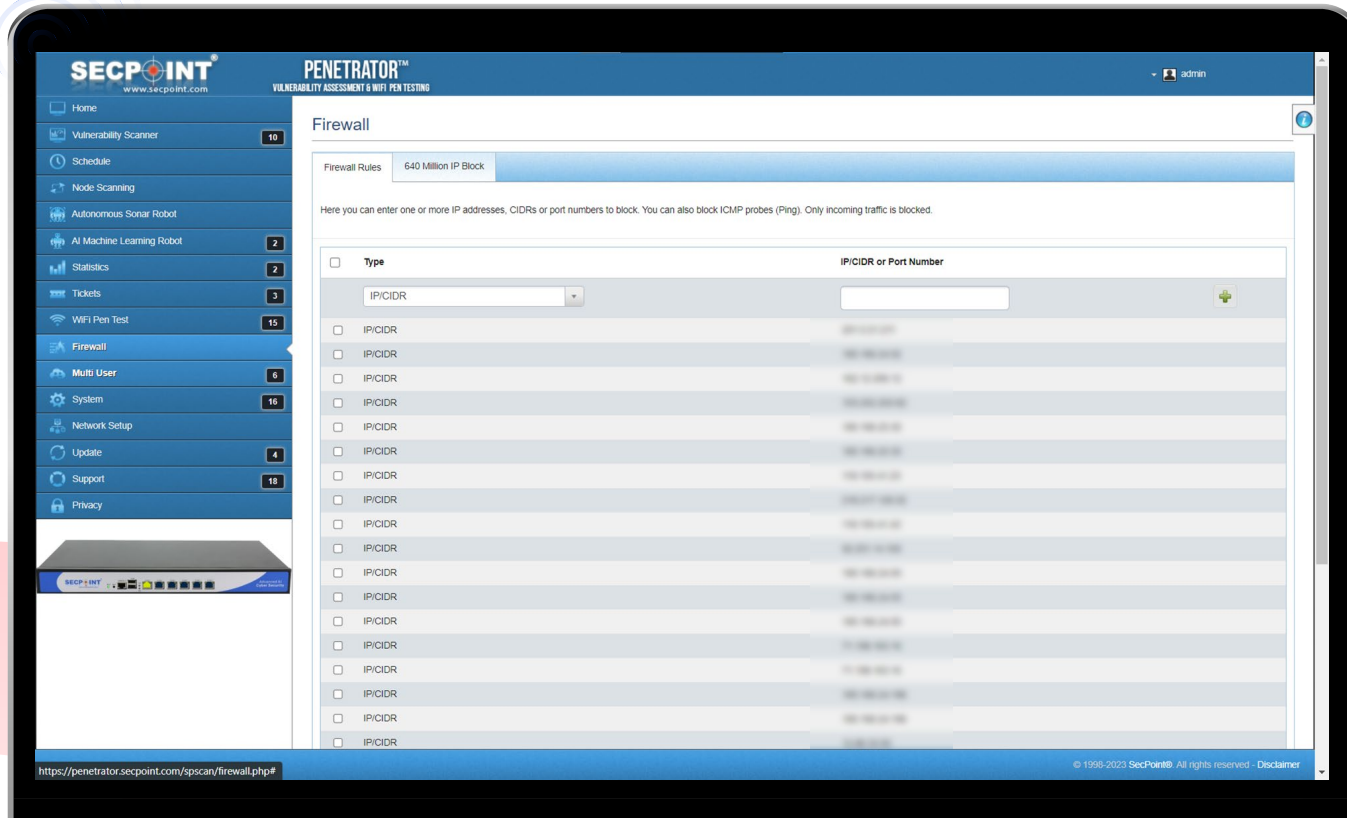
Allows to connect multiple software or appliances together in a distributed manner and do the scanning centralized.



Then all data and reporting will be centralized and allows for easy control from the admin



Firewall



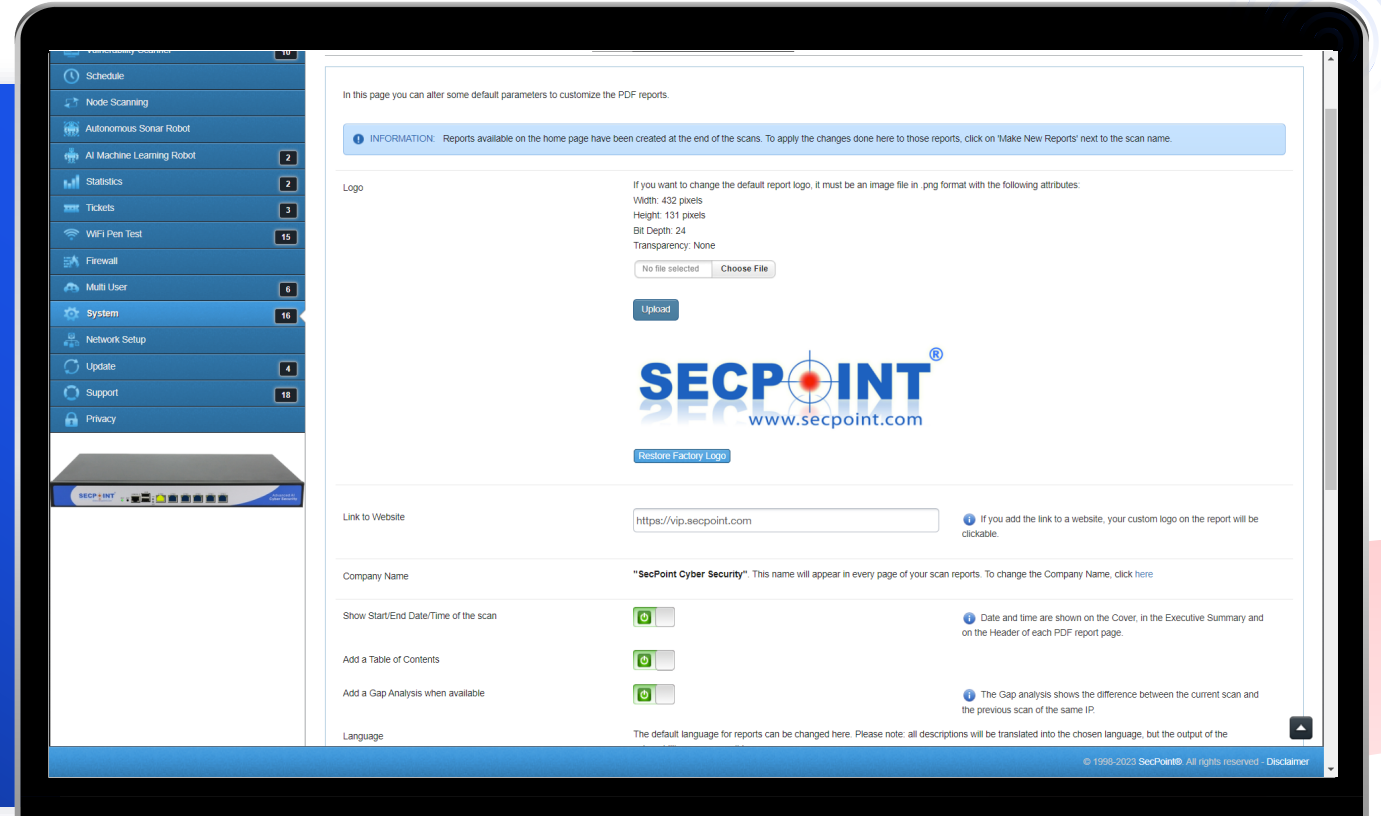
Penetrator™ has strong onboard firewall system to block attacks, toxic IPS to connect, specific attacks such as brute force , SQL injection, command execution and more




Whitelabeling



It is possible on the Penetrator™ to rebrand reports with company name, logo, watermark and specific text



Key Features of SecPoint Penetrator

- "Empowering Your Defense: Unveiling SecPoint Penetrator"
 - Automated Vulnerability Scanning: Identifies potential weaknesses in your network infrastructure.
 - Threat Intelligence Integration: Leverages real-time threat intelligence to enhance proactive defense.
 - Advanced Penetration Testing: Simulates cyber attacks to uncover vulnerabilities before malicious actors do.
 - Continuous Monitoring: Ensures ongoing security, adapting to the evolving threat landscape.
- 

Customer Benefits

- "SecPoint Penetrator: Delivering Tangible Benefits"
- Real-time Threat Prevention: Proactively identifies and prevents cyber threats in real-time.
- Cost-Efficient Security: Reduces the financial impact of potential breaches through continuous testing and threat mitigation.
- Enhanced Compliance: Helps companies meet regulatory requirements by maintaining a secure and compliant network.



Conclusion

- "SecPoint Penetrator: Safeguarding Your Future"
- In conclusion, SecPoint Penetrator provides a comprehensive solution to meet the evolving challenges of cybersecurity.
- We invite questions and discussions to explore how SecPoint Penetrator can be tailored to enhance your organization's security posture.

