

Today, organizations utilize numerous security products; most are **standalone, complex, and too slow to catch modern day attacks**. Hackers are also relying more on “living-off-the-land” strategies: leveraging existing IT technologies and user accounts for malicious purposes. As a result, detecting and analyzing hacker tradecraft often takes significant time, technical expertise, and resources.

SNAP-Defense security operations and incident response platform is a **gamechanger**; it excels at monitoring and catching modern hacking tradecraft, delivering real-time alerts, and allowing for immediate threat response.

CAPABILITIES



LIVE ASSET
VISIBILITY



MULTI-POINT THREAT
DETECTION



LATERAL SPREAD
DETECTION



PRIVILEGED ACCOUNT
MONITORING



IMMEDIATE THREAT
RESPONSE



REMOTE ACCESS
MONITORING



INSIDER THREAT
VISIBILITY



3RD PARTY
INTEGRATIONS



RISK AND COMPLIANCE
REPORTING

AVAILABLE AS:

MANAGED DETECTION + RESPONSE (MDR)

Our team monitors SNAP-Defense for you

KEY BENEFITS:

- PATENTED LATERAL MOVEMENT DETECTION
- THREAT HUNTING CAPABILITIES
- REAL-TIME THREAT DETECTION AND RESPONSE
- REPORTING AND COMPLIANCE MODULE
- INTEGRATED NON-TRADITIONAL IT ASSET VISIBILITY AND THREAT DETECTION

- Internet of Things (IoT)
- Operational Technology (OT)
- Building Automation Systems (BAS)
- Industrial Control Systems (ICS)

SNAP-Defense enables security teams to quickly identify modern hacking tradecraft and take immediate response.

MANAGED DETECTION AND RESPONSE (MDR)

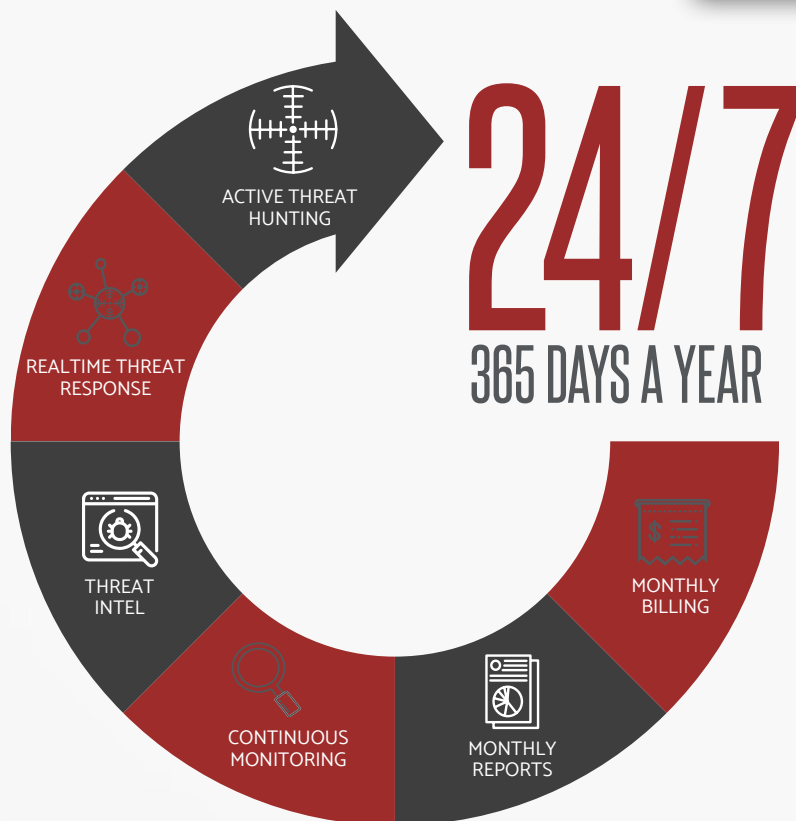
POWERED BY **SNAP** DEFENSE



networkdoctor
IT SOLUTIONS & SERVICES

CONTINUOUS CYBER PROTECTION

Our 24x7 MDR service uses its patented SNAP-Defense platform, NICOS network tap, and 3rd party integrations.



WHAT IS MDR?

The next evolution of managed security service with a focus on **real-time threat detection, threat hunting, and active response.**

WHY MDR?

Prevention and perimeter protection is no longer sufficient to detect and stop cyberattacks. Neither is expensive, resource-intensive log analysis. Finally, organizations need **response, not just recommendations.**

Gartner

"IT security leaders should use managed detection and response (MDR) services to augment existing security monitoring capabilities to address gaps in advanced threat detection and incident response before investing in more security monitoring tools (e.g., security information and event management [SIEM], network, and host-threat detection), and associated staff and expertise."

Gartner, "Market Guide for Managed Detection and Response (MDR) Services", May 2016, Bussa, Lawson, Kavanagh

Competitive Pricing

Our SNAP-Defense platform and MDR service are competitively priced and offer significantly more capabilities and value than competing solutions:

Network Visualization | Real-time Monitoring | Real-time Threat Detection | Real-time Response | Compliance | Reporting | Notifications | Endpoint Protection | and more!

Our MDR service is significantly more cost-effective and efficient than if an organization was to build and operate its own 24x7 SOC.

Protection Options

Extend SNAP-Defense with additional enhanced capabilities:

+ A/V (Webroot) | Bundled with SNAP-Defense

(Anti-malware, Pre-execution Behavior Analysis, Web Security, Download Reputation)

+ Sophos Intercept-X | Bundled with SNAP-Defense

(Deep Learning Anti-malware, Ransomware File Protection, Man-in-the-browser Protection, Disk & Boot Record Protection, Credential Theft Protection, Process Privilege Escalation, Malicious Process Migration, Asynchronous Procedure Calls Protection)

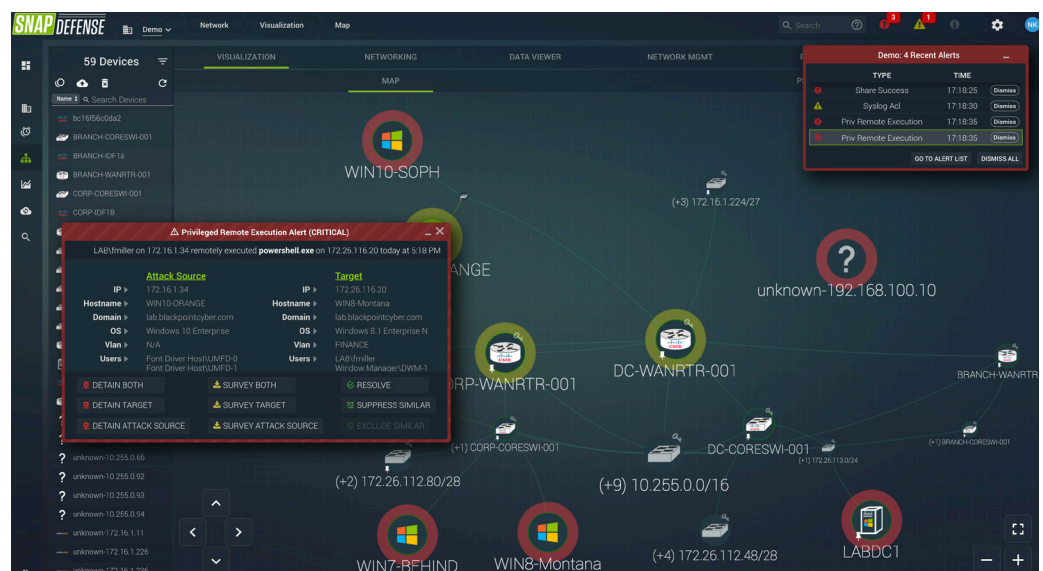
+ 365 Defense | Bundled with SNAP-Defense

24/7 Microsoft 365 Security Add-on

+ NICOS | Integrates with SNAP-Defense

(Network-based Asset Discovery, Monitoring, Threat Detection, Remote Access Auditing)

IMMEDIATE
THREAT
RESPONSE



MONTHLY REPORTING



— See the Value we Bring

— Detailed Metrics

— Summary of Service Activity



PROVIDED SECURITY VALUE

24/7 cyber security monitoring and response is critical to defend against today's cyber threats. Our 24/7 Managed Detection and Response service provides the following value to your organization.

\$42,000

REPORTING PERIOD VALUE

\$252,000

PAST 12 MONTHS VALUE

The provided value is based on the approximate costs to setup and run a 24/7 MDR operation over the reporting period for an organization similar to Your Client

LABOR	+	RENT + UTILITIES	+	HOSTING + EQUIPMENT	+	MDR TECH
\$50,000		\$7,000		\$1,000		\$XXX

Note: all amounts in USD

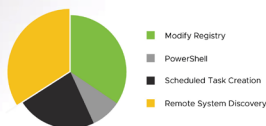
November 2020 — December 2020

Prepared for: Your Client

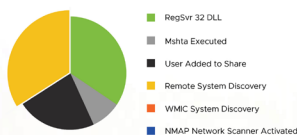
SECURITY ANALYSIS: THREAT TECHNIQUES

During the report period, we evaluated **19 suspicious events** detected by **7 specific rules** covering **11 unique threat techniques**.

Events by Top 10 Techniques



Events by Top 10 Rules



- ✓ Good security practices and IT hygiene significantly reduce your cyber risk
- ✓ Keep software and devices updated and patched
- ✓ Backup regularly and ensure backups work
- ✓ Investigate suspicious events as soon as possible

Threat detection rules define events and behavior that may indicate malicious activity. Our threat intelligence team updates and adds new rules based on emerging tactics and techniques. These rules are grouped into threat technique categories to help identify patterns. Your MDR service works around-the-clock to detect and notify you of valid threats.

Your Events Past 12 Months



November 2020 — December 2020

Prepared for: Your Client

SECURITY ANALYSIS: SUMMARY

REPORTING PERIOD

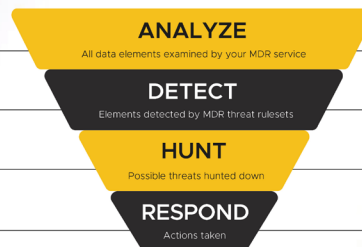
600,000

32,000

108

2

3 Rule Detections



PAST 12 MONTHS

3,200,000

132,000

640

24

2 Threat Techniques

1 Privilege Remote Activity Events

1 365 Defense Events

0 Anti-virus Events

1 MITRE ATT&CK® Framework Events

November 2020 — December 2020

Prepared for: Your Client