Adlumin

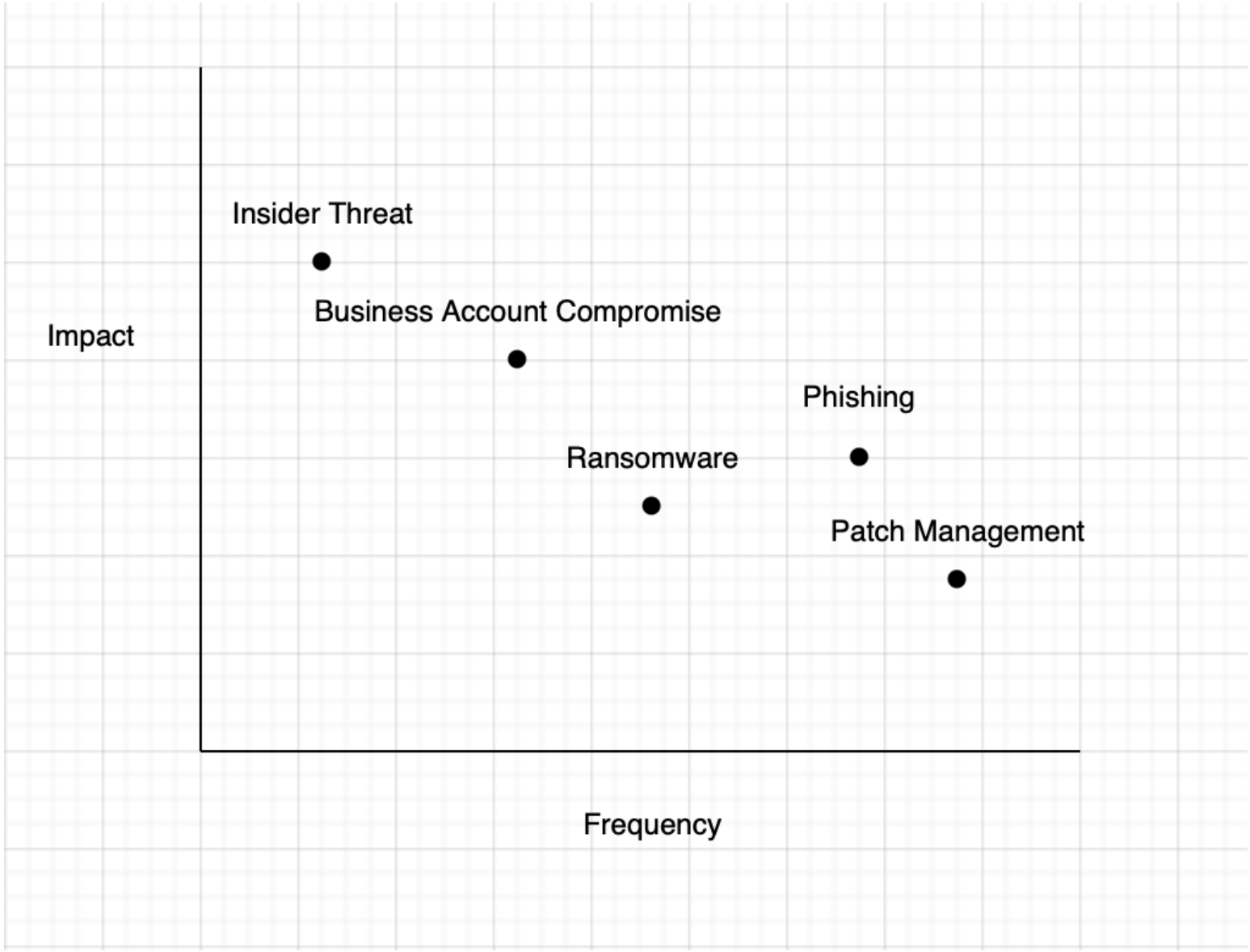
Bank Security, 2022

The command center for security operations.

SEE MORE

Top Threats

- Ransomware
- Phishing
- Business Account Compromise
- Patch Management
- Insider Threat



Adlumin

1. Ransomware

- 37% of respondents' organizations in one poll were affected by ransomware attacks in the last year
- Average requested ransom has increased from $5,000 in 2018 to nearly $200,000 in 2020
- Growth in Ransomware-as-a-Service (RaaS)
  - Creators of these tools take a percentage of each successful ransom payment
- Move from holding data for ransom to releasing data for ransom

Adlumin

THE PROBLEM

INCREASING COMPLIANCE

01

Comprehensive reporting, unique regulatory standards like FFIEC, NCUA, & CMMC compliance.

DECREASING BUDGETS

02

Adlumin offers frictionless pricing and billing models enabling the different markets we serve to perform better.

DECREASING CAPACITY

03

Zero customer configuration means a technology when implemented just works.

INCREASING THREATS

04

Our 24/7 Security Operations Center (SOC) quickly enhances organization's threat detection & response times.

Points of Focus

PROACTIVE

Take an active approach to making yourself a hard target.

Focus on collecting telemetry from external access points like VPN and Cloud Email.

Reduce opportunities for attackers to automatically propagate their attack.

DETECTION AND MITIGATION

For 99% of organizations in the mid to enterprise lite market you need to focus ONLY on three areas to prevent the worst:

1. Cloud Email
2. VPN
3. Endpoint
4. Get Managed Detection and Response

LOG MANAGEMENT

Meet both your compliance and security objectives in a single platform.

Employ a cloud native solution integrating many product capabilities into a single platform.

Breach Last Week

A significant breach of a US financial institution customer discovered and remediated by Adlumin threat research team by multiple threat actors, the most significant DEEP PANDA, which maps to the Chinese Ministry of State Security

The main issues: The customer was under resourced and didn't opt into the managed detection and response product offering. He didn't have enough time or expertise to pay attention to his patching, security products, or IT environment.

Initial infection vector was an unpatched log4j vulnerability in VmWare Horizon and Apache Tomcat.

More than 50 alerts and recommendations to respond immediately but kept clearing them as false positives. They were not.

Eventually Adlumin's threat research and hunting team, which is our backstop and last line of defense discovered and remediated. This customer is now an MDR customer.

Kaseya Breach

Compromised third-party management infrastructure delivered adverse effects on organizations across America (e.g., phone system providers, managed service providers, etc.).

organizations had no introspection into these managed systems.

Most organizations were affected by **mapped drives**. Persistently, mapped drives from the ransomware affected systems to other systems within the environment facilitated encryption of those mapped drives.

At-risk shares remain a huge problem at organizations. Often, older teller and card reading software must be installed with excessive privileges.

Adlumin's at risk program is designed to **find places where non-privileged accounts or groups have been given unnecessary privileged access to network shares** and system resources greatly increasing a organizations exposure to breaches like Kaseya.

Activate file auditing logging where possible it would have saved you a lot of pain.

organizations could not identify places in their environment where Kaseya was running.

Colonial Pipeline Breach

External access points represent the greatest threat to the Banking Industry.

Ransomware groups take leverage password reuse and Dark Web Breaches to gain access to external points of entry. **100% of organizations have dark net exposure.**

Cloud email and client VPN access are usually the next to be compromised. organizations have some visibility into cloud email but nearly no introspection into client VPN access….the deadliest.

At Adlumin we detect and prevent nearly a breach a week across cloud email and client VPN access.

Malware is the very last ball to drop and typically means a large variety of defenses and configurations have already been defeated.

Threat Research

- **Discovered & Remediated 4 Active Attacks Against Customers**
  - 2 due to external SOC failure; 2 due to targeted attacks
- **Stood up Threat Intel ingestion and data sharing platform**
  - 100k+ technical Indicators of Compromise
  - Integrating into product and automating detections
  - Non-automated usage has already detected a compromised customer
- **Developing platform for notification of spear phishing sites which mimic customer's legitimate assets.**
  - Completed modules have already detected 2 customer domains targeted

TECHNOLOGY SUMMARY

Network Health & Compliance

- Compliance Reports
- PCI DSS, NIST, HIPAA, etc.

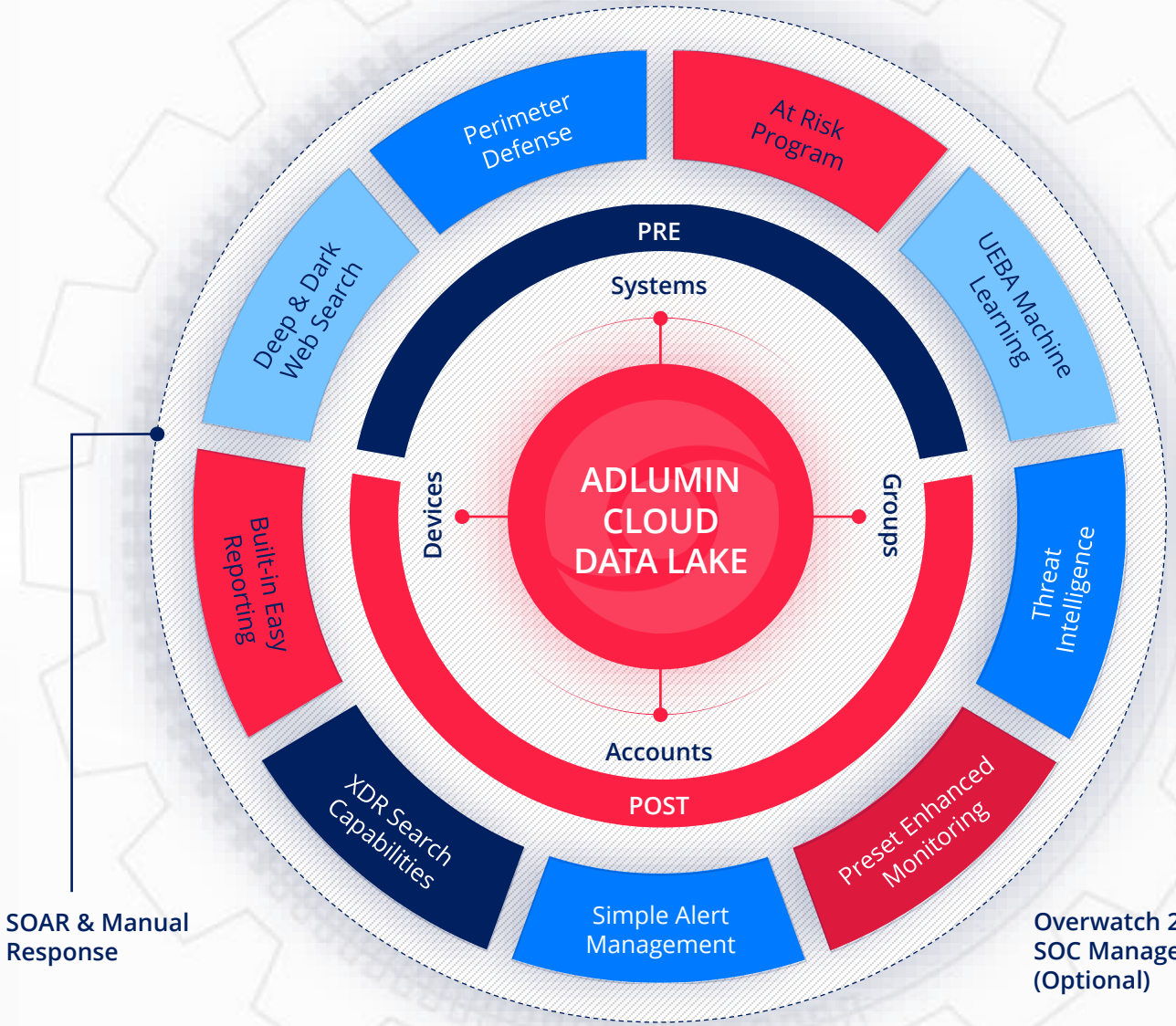
Advanced Security

- Threat Detection
- Artificial Intelligence

Data Research & Log Management

- 90-Day Storage
- Opt. 1+ Year Data Retention
- No Data Limits

OUR PLATFORM DEPLOYS IN 90 MINUTES OR LESS!



01

ADLUMIN MSP

Targeting MSP's | Utility Billing

02

ADLUMIN ENTERPRISE

Fixed Price | Per Data Source

03

TOTAL RANSOMWARE DEFENSE

EPP Augmentation

04

Continuous Vulnerability Management

Patch Management and Vulnerability Scanning

05

DARKNET EXPOSURE

OEM product providing security beyond the perimeter of the network into the open deep and dark web.

06

OVERWATCH 24/7 SOC

Managed Compliance | Detection | Response (MCDR) Service

Adlumin

THANK YOU!

QUESTIONS?

Robert Johnston
(410) 212-3907
robert.johnston@adlumin.com
www.adlumin.com