Abatis and Financial Institutions

ABSTRACT

This whitepaper explores the unique capabilities of Abatis, a cybersecurity solution that moves beyond traditional "detect, respond, and mitigate" models to offer proactive, deterministic protection. Supporting all operating systems from Windows NT4 to Windows 11 (including servers) and all Linux variants, Abatis addresses critical security challenges for financial institutions, including the cadence patch gap, immutability - the need to protect systems from unauthorised changes, and AI-driven threat acceleration. With its lightweight footprint, energy efficiency, and ability to prevent malware persistence, Abatis provides a scalable, zero-maintenance solution for diverse IT environments. Real-world use cases demonstrate its value in application servers, vendor appliances, ATMs, and more.

Alexander Rogan | CEO

FS-ISAC | AFFILIATE

CONTENTS

EXECUTIVE SUMMARY

In today's rapidly evolving threat landscape, financial institutions are grappling with significant cybersecurity challenges. The emergence of AI and Large Language Models (LLMs) has accelerated the development of Exploits against known vulnerabilities (published CVE's), threatening to outpace traditional defence mechanisms. This makes it crucial for organisations to adopt proactive and innovative solutions. Key challenges include the cadence patch gap, where institutions struggle to promptly patch vulnerabilities, vendor-enforced updates that can destabilise systems or make them entirely unavailable, and the complexity of managing legacy and hybrid systems. In this context, the unique capabilities of Abatis, a cybersecurity solution that moves beyond traditional 'detect, respond, and mitigate' models to offer proactive, deterministic protection, become particularly relevant.

The Abatis solution addresses these challenges by providing a proactive, deterministic, and immutable security framework that ensures operational integrity. Key features include:

- **Operating System Immutability:** Prevents unauthorised changes and malware persistence while enabling secure pre-production patch testing.
- **Proactive Threat Neutralisation:** Instantly blocks AI-driven threats and weaponised vulnerabilities, ensuring rapid responses to emerging attacks.
- **Empirical Data and SOC Optimisation:** Logs only genuine events, reducing noise and streamlining operations within Security Operations Centres (SOCs).

With universal compatibility across various operating systems, Abatis enhances security with minimal performance impact and improves operational efficiency. Institutions can expect reduced energy consumption by 20%, aligning with environmental and sustainability goals.

Additionally, integrating Abatis with Aegis provides a unified cybersecurity stack that protects data and endpoints without traditional encryption, effectively addressing emerging threats in the post-quantum era.

Proven results demonstrate Abatis' capacity to neutralise malware across diverse environments while significantly simplifying SOC operations and reducing operational stress. This innovative approach equips financial institutions to navigate the complexities of the cybersecurity landscape and strengthen their defences against evolving threats.

THE GROWING CYBERSECURITY CHALLENGES FOR FINANCIAL INSTITUTIONS

AI AND LLM-DRIVEN THREAT ACCELERATION

The emergence of AI and Large Language Models (LLMs) has drastically reduced the time required for bad actors to weaponise vulnerabilities. Proof-of-concept exploits, intended to aid defence, are now operationalised within hours, outpacing traditional detect-and-respond models.

THE CADENCE PATCH GAP

Financial institutions often struggle to patch systems promptly, exposing vulnerabilities for weeks. Secure patch testing in pre-production environments is critical to maintaining operational integrity.

Vendor-Enforced Updates

Mandatory vendor updates can destabilise systems, leading to operational disruptions like Blue Screen of Death (BSOD) events, often creating additional security vulnerabilities.

Legacy and Hybrid Systems

Institutions must secure a complex mix of legacy and modern systems, ensuring compatibility while addressing unique vulnerabilities.

THE ABATIS SOLUTION: PROACTIVE, DETERMINISTIC, AND IMMUTABLE

Operating System Immutability

- Prevents unauthorised changes to operating systems, ensuring immutability and resilience against malware persistence.
- Supports secure patch testing in pre-production environments before live deployment, mitigating risks from untested updates.
- Enables zero trust architectures by enforcing a default-deny policy at the endpoint level.

Proactive Threat Neutralization

- Neutralizes threats deterministically, stopping malware and unauthorised changes in nanoseconds.
- Blocks AI-accelerated, weaponised vulnerabilities before they can impact systems.

Empirical Data and SOC Optimization

- Logs only actual events, with no false positives or negatives, reducing SOC workloads and storage needs by an order of magnitude.
- Provides real-time alerts on blocked threats, removing the need for traditional downstream threat hunting.

Universal Compatibility

Supports all Windows operating systems from NT4 to Windows 11 (including servers) and all Linux variants, ensuring seamless integration across diverse environments.

Energy Efficiency

Reduces energy consumption and costs by 20%, aligning with ESG goals and lowering operational expenses.

USE CASES FOR FINANCIAL INSTITUTIONS

- **Windows Application Servers:** Ensures integrity by preventing unauthorised executable content post-build.
- **Vendor Appliances and Turnkey Systems:** Adds a lightweight security layer to vendor-managed systems without impacting performance or requiring updates.
- **ATM Systems:** Provides file-system-level protection, complementing existing controls to secure critical financial endpoints.
- **Abatis as a Sensor:** Operates in "learn mode" to log policy violations and integrates with tools like Tanium for advanced threat visibility and control.
- **Legacy Communication (SMBv1):** Secures critical interoperability between legacy and modern systems without increasing attack surfaces.
- **Memory-Only Attacks:** Extends protection to in-memory threats, mitigating vulnerabilities not covered by traditional endpoint solutions.
- **Real-Time Threat Reporting:** Neutralises threats instantly, providing real-time visibility and reducing response times.

BENEFITS FOR FINANCIAL INSTITUTIONS

SECURITY

- AI-Resilient Protection: Stops rapidly weaponised vulnerabilities, neutralising AI and LLM-driven threats.
- Immutable Endpoints: Prevents malware persistence and unauthorised changes.
- Zero Trust Enablement: Enforces a strict deny-all policy, ensuring system integrity.

OPERATIONAL EFFICIENCY

- Streamlined Patching: Solves the cadence patch gap by supporting confident pre-production testing.
- SOC Optimization: Reduces logging noise and eliminates unnecessary processes, saving resources and significantly reducing operational stress, providing a sense of reassurance to decision-makers.
- Cost Efficiency: Low maintenance and lightweight footprint lead to reduced hardware upgrades and overall savings.

ENVIRONMENTAL SUSTAINABILITY

- Energy Savings: Demonstrated a 20% reduction in energy consumption across 2,000 servers.
- ESG Alignment: Supports environmental and sustainability goals.

COMPLEMENTING ABATIS WITH AEGIS

POST-QUANTUM DATA SECURITY

Aegis protects files and databases without traditional encryption, addressing vulnerabilities in the post-quantum era.

UNIFIED CYBERSECURITY STACK

Abatis and Aegis provide comprehensive endpoint and data protection, future-proofing institutions against emerging threats and making the audience feel secure and prepared for future challenges.

PROVEN RESULTS

Validated Use Cases

- Proven to secure Windows servers and Linux endpoints, neutralising malware in diverse IT environments.
- Demonstrated energy savings of 20% during testing on 2,000 servers.

SOC Impact

Reduced logging noise and workload by an order of magnitude, simplifying SOC operations.

Real-Time Blocking

Stops attacks in nanoseconds, providing instant alerts and negating the need for post-event investigations.

CONCLUSION

Abatis provides a proactive and deterministic solution to cybersecurity challenges faced by financial institutions. Its unique ability to render systems immutable, lightweight design, broad compatibility, and sustainability benefits make it an ideal choice for securing both legacy and modern environments. Combined with Aegis, Abatis offers a future-proof defence that addresses today's threats while preparing for tomorrow's challenges.