FRENOS

Proactive Defense Framework for Critical Infrastructure

Co-Authored by: Harry Thomas & Alex Waitkus

FRENOS • White Paper • December 2024

I. Executive Summary

Critical infrastructure organizations face increasingly sophisticated cyber-attacks that can have devastating consequences on essential services and operations. This framework presents a comprehensive approach to proactive defense, moving beyond traditional reactive security measures to implement an intelligence-driven security strategy that anticipates and prevents threats before they materialize.

The primary purpose of this framework is to systematically reduce the attack surface of critical infrastructure systems through a multi-faceted approach that combines threat intelligence, simulation-based validation, and continuous improvement. By shifting from a reactive to a proactive security posture, organizations can identify and remediate potential security gaps before they can be exploited by adversaries.

Our framework addresses four key objectives that are essential for maintaining robust security in critical infrastructure environments:

First, we focus on decreasing the mean time to detection and response through enhanced monitoring capabilities and streamlined incident response procedures. This reduction in response time is crucial for minimizing the potential impact of security incidents and preventing them from escalating into major breaches.

Second, the framework emphasizes the importance of validating security controls effectiveness through regular testing and assessment. This validation ensures that defensive measures perform as intended and provide meaningful protection against real-world threats.

Third, we establish methodologies for identifying and remediating potential attack paths within the infrastructure. This process involves comprehensive mapping of system interconnections and access points, allowing organizations to understand and address vulnerabilities before they can be exploited.

Finally, the framework guides organizations in implementing intelligence-driven controls that adapt to emerging threats. By leveraging current threat intelligence and attack pattern analysis, security measures can be continuously updated to address new and evolving attack methodologies.

The success of this framework is measured through quantifiable risk reduction metrics, allowing organizations to demonstrate concrete improvements in their security posture. These metrics include reductions in vulnerable attack paths, improvements in detection rates, and decreased incident response times.

Through the implementation of this framework, critical infrastructure organizations can move beyond passive defense to actively identify and address security challenges, ultimately building a more resilient and secure operational environment.

II. Threat Intelligence for Proactive Defense

The foundation of an effective proactive defense strategy lies in the systematic collection, analysis, and operationalization of threat intelligence. Critical infrastructure organizations must develop robust intelligence gathering capabilities that extend beyond traditional indicator sharing to encompass comprehensive understanding of adversary tactics, techniques, and procedures (TTPs).

Intelligence Collection and Analysis

Modern threat intelligence programs require diverse information sources to build a complete picture of the threat landscape. Organizations should actively participate in Information Sharing and Analysis Centers (ISACs) and maintain strong relationships with government partners such as CISA to receive sector-specific threat information. This collaborative approach ensures access to timely, relevant intelligence about emerging threats targeting critical infrastructure.

Of particular importance is the analysis of known adversary TTPs, such as those employed by sophisticated threat actors like Volt Typhoon and Sandworm. Understanding these TTPs allows organizations to anticipate potential attack methodologies and implement appropriate defensive measures before attacks occur. This analysis should be complemented by robust vulnerability intelligence programs that track both known vulnerabilities (like the CISA known, exploited vulnerability - KEV database) and emerging zero-day threats that could impact critical systems.

Intelligence-Driven Defense Planning

The true value of threat intelligence lies not in its collection, but in its practical application to defense planning. Organizations must establish systematic processes for mapping identified threats to their critical assets and infrastructure. This mapping process should consider both direct threats to specific systems and potential cascade effects that could impact interconnected infrastructure components.

By analyzing high-risk attack vectors identified through threat intelligence, organizations can prioritize their defensive measures more effectively. This prioritization should consider both the likelihood of specific attack methodologies being employed and the potential impact of successful attacks on critical operations. The resulting defensive measures should be proactive rather than reactive, focusing on preventing attacks by addressing vulnerabilities and attack paths before they can be exploited.

Continuous Threat Assessment

The threat landscape facing critical infrastructure is constantly evolving, necessitating a dynamic approach to threat assessment. Organizations must implement real-time threat monitoring capabilities that can quickly identify and analyze new attack patterns as they emerge. This monitoring should encompass both technical indicators of compromise and broader strategic intelligence about adversary intentions and capabilities.

To support effective decision-making, organizations should implement risk scoring and prioritization frameworks that quantify the relative importance of different threats. These frameworks should consider factors such as:

- The criticality of potentially affected assets
- The sophistication of threat actors
- The current state of defensive controls
- The potential consequence to operations

Regular reassessment of these risk scores ensures that defensive priorities remain aligned with the most pressing threats facing the organization. This continuous assessment process should feed directly into the organization's broader security program, driving updates to defensive controls and security policies as needed.

Through this comprehensive approach to threat intelligence, organizations can move beyond reactive security measures to implement truly proactive defense strategies. By understanding and anticipating threats before they materialize, critical infrastructure operators can better protect their essential systems and services from increasingly sophisticated cyber-attacks.

III. Attack Path Validation Through Simulation

The effectiveness of any proactive defense strategy ultimately depends on its ability to withstand real-world attacks. Attack path validation through simulation provides organizations with a structured methodology to identify and remediate potential vulnerabilities before they can be exploited by adversaries. This approach combines rigorous analysis with practical testing to ensure that defensive measures are both comprehensive and effective.

Attack Path Mapping

A thorough understanding of potential attack paths begins with comprehensive network topology analysis. Organizations must document and understand not only their network architecture but also the complex interactions between different systems and components. This analysis should pay particular attention to critical assets, which serve as likely targets for sophisticated adversaries. By mapping these assets and their interconnections, organizations can better understand how attackers might move through their infrastructure to reach high-value targets.

The documentation of access paths serves as a crucial component of this analysis. Every potential route to critical assets must be identified and evaluated, including both direct network connections and indirect paths that might leverage intermediate systems or trust relationships. This detailed mapping allows organizations to identify choke points – critical junctions where multiple attack paths converge. These choke points often represent optimal locations for implementing defensive controls, as they allow organizations to maximize the impact of their security investments.

Simulation Scenarios

The development of effective simulation scenarios requires a deep understanding of both adversary capabilities and organizational vulnerabilities. Rather than relying on generic attack scenarios, organizations should develop custom scenarios that reflect their specific threat landscape. These scenarios should incorporate known adversary TTPs, particularly those identified through threat intelligence as being relevant to their sector or organization.

Beyond specific TTPs, scenarios should also encompass common attack patterns that have proven successful against similar organizations or infrastructure. These patterns often represent well-understood and frequently exploited vulnerabilities that must be addressed. Industry-specific scenarios are particularly valuable, as they reflect the unique challenges and attack methodologies relevant to critical infrastructure environments.

Custom attack chains should be developed to test specific concerns or vulnerabilities identified through risk assessment processes. These chains should combine multiple techniques and approaches to simulate sophisticated, multi-stage attacks that better reflect real-world threats. The complexity and sophistication of these scenarios should increase over time as basic security controls are validated and improved.

Validation Methodology

The validation process must be systematic and thorough to provide meaningful results. Starting with paper-based scenario testing allows organizations to identify obvious gaps and inefficiencies before committing resources to live testing. This initial phase helps refine scenarios and identify potential safety concerns that need to be addressed before moving to active testing.

Live scenario execution represents the most critical phase of validation. During this phase, organizations can observe how their defenses perform against simulated attacks in real-time. This testing should be carefully controlled to prevent unintended impacts on critical systems while still providing realistic validation of security controls. The measurement of control effectiveness during these exercises provides quantitative data that can guide future improvements.

Gap identification through validation testing often reveals unexpected vulnerabilities or control failures that weren't apparent during theoretical analysis. These findings should be thoroughly documented and prioritized based on the potential impact to critical operations. The validation process should be iterative, with identified gaps feeding back into the defense planning process to drive continuous improvement in security controls.

Through systematic attack path validation, organizations can move beyond theoretical security models to develop proven, effective defenses. This approach provides concrete evidence of security control effectiveness while identifying areas requiring additional attention or investment. The resulting improvements in defensive capabilities directly enhance the organization's ability to protect critical infrastructure against sophisticated cyber-attacks.

IV. Breach and Attack Simulation (BAS)

While traditional penetration testing provides valuable insights into security posture, the dynamic nature of modern threats demands a more continuous and automated approach to security validation. Breach and Attack Simulation (BAS) addresses this need by providing organizations with automated, consistent, and repeatable testing capabilities that can be executed.

BAS Implementation

The foundation of an effective BAS program lies in its automation framework. Unlike manual testing approaches, automated platforms enable organizations to conduct frequent, comprehensive security assessments without straining resources or introducing human error. These platforms should be carefully configured to emulate real-world attack scenarios while maintaining strict controls to prevent impact on production systems.

Modern BAS frameworks must go beyond simple vulnerability scanning to provide true attack emulation. This involves executing actual adversarial techniques, albeit in a controlled manner, to validate the entire security stack – from preventive controls through detection and response capabilities. The framework should support continuous validation, allowing organizations to quickly identify when changes in their environment may have introduced new vulnerabilities or weakened existing defenses.

Control effectiveness measurement represents a critical component of the BAS framework. Each simulated attack should generate detailed telemetry about which controls detected or prevented the attack, as well as any controls that failed to perform as expected. This data provides concrete metrics for evaluating security investments and identifying areas requiring improvement.

Comprehensive Testing Scope

Network segmentation validation stands as a primary focus area for BAS testing. In critical infrastructure environments, proper network segmentation often represents the last line of defense against lateral movement and escalation. BAS scenarios should actively test segmentation boundaries, attempting to identify paths between network zones that should remain isolated. This testing should include both obvious direct connections and subtle trust relationships that might be exploited by sophisticated attackers.

Access control testing through BAS extends beyond simple authentication checks to validate the entire chain of trust relationships and permissions. Simulated attacks should attempt to exploit misconfigurations, over-privileged accounts, and weak points in identity management systems. This testing should cover both human and machine identities, as automated systems often hold privileged access to critical infrastructure components.

Detection capability assessment represents perhaps the most valuable aspect of BAS testing. By executing known attack techniques, organizations can validate whether their internal network security monitoring (INSM) systems can effectively identify malicious activity. This testing should evaluate not just the technical detection capabilities but also the effectiveness of alert prioritization and correlation systems. False positive rates should be measured alongside detection rates to ensure that security teams can effectively separate genuine threats from background noise.

Results Analysis and Continuous Improvement

The true value of BAS lies not in the testing itself but in the systematic analysis of results. Success and failure metrics should be tracked over time to identify trends and patterns in security control effectiveness. These metrics should be granular enough to identify specific control failures while also providing high-level views of overall security posture improvement.

Gap identification through BAS should feed directly into the organization's security improvement lifecycle. When control failures are identified, root cause analysis should determine whether the issue stems from technical misconfigurations, process deficiencies, or fundamental architectural weaknesses. This analysis helps ensure that remediation efforts address underlying issues rather than just symptoms.

Remediation prioritization must balance multiple factors including:

- The criticality of affected systems or data
- The likelihood of exploitation
- The complexity of required fixes
- The potential impact on operations
- Resource availability and constraints

Organizations should establish clear thresholds for acceptable risk and required remediation timeframes based on these factors. High-risk findings that could directly impact critical infrastructure operations should trigger immediate response, while lower-risk issues might be addressed through planned improvement cycles.

Through consistent execution of BAS programs, organizations can maintain continuous visibility into their security posture while validating the effectiveness of their defensive investments. This approach provides the empirical data needed to make informed decisions about security improvements while ensuring that critical infrastructure remains protected against evolving threats. and indirect paths that might leverage intermediate systems or trust relationships. This detailed mapping allows organizations to identify choke points – critical junctions where multiple attack paths converge. These choke points often represent optimal locations for implementing defensive controls, as they allow organizations to maximize the impact of their security investments.

V. Control Implementation and Validation

The successful execution of a proactive defense framework ultimately depends on the effective implementation and continuous validation of security controls. While previous sections outlined the intelligence gathering and testing methodologies necessary to identify security requirements, this section focuses on the practical aspects of deploying and maintaining defensive measures within critical infrastructure environments.

Risk-Based Control Selection

The selection and implementation of security controls must be driven by a comprehensive understanding of organizational risk. Rather than adopting a one-size-fits-all approach, organizations should carefully evaluate how different control types address their specific threat landscape. Network segmentation enhancements, for instance, should be designed to create logical boundaries between critical systems while maintaining necessary operational workflows. This might involve implementing zero-trust architectures that enforce strict access controls at every network junction, or deploying advanced monitoring solutions at key network choke points identified during attack path analysis.

Access control optimization represents another crucial aspect of the control framework. Organizations must move beyond simple role-based access control to implement attribute-based systems that can make dynamic access decisions based on multiple factors including user identity, device status, network location, and current threat levels. This granular approach to access control helps prevent lateral movement while ensuring that legitimate users maintain necessary system access.

The enhancement of monitoring capabilities should focus on achieving full visibility across the infrastructure while minimizing alert fatigue. This requires careful tuning of detection systems to focus on high-priority threats identified through threat intelligence, while implementing automated triage systems to help analysts focus on the most critical alerts. Organizations should also invest in response capability strengthening, developing automated playbooks for common scenarios while maintaining flexibility to address novel threats.

Strategic Implementation Approach

The deployment of new security controls in critical infrastructure environments requires careful planning to prevent operational disruption. A prioritized deployment strategy should be developed based on risk assessment findings, with critical vulnerabilities addressed first while maintaining a balance with operational requirements. This prioritization should consider both the potential impact of security incidents and the complexity of implementing specific controls.

A phased implementation approach often proves most effective, allowing organizations to validate each control's effectiveness before moving to subsequent deployment phases. This methodology provides opportunities for fine-tuning and adjustment based on real-world performance, while limiting the scope of potential issues that might arise during deployment. Each phase should include comprehensive testing and validation to ensure that new controls integrate properly with existing security measures and operational systems.

Measuring Success

The ultimate measure of control effectiveness lies in concrete, measurable improvements to organizational security posture. Primary metrics should include quantifiable reductions in attack surface, measured through regular vulnerability assessments and attack path analysis. Organizations should track improvements in detection rates, focusing particularly on the detection of sophisticated attack techniques identified through threat intelligence.

Response times provide another crucial metric, with organizations working to continuously decrease the interval between initial detection and threat containment. This improvement in response capabilities should be measured across different types of incidents, with particular attention paid to scenarios that could impact critical infrastructure operations.

Enhanced resilience represents the culmination of these efforts, demonstrated through the organization's ability to maintain critical operations even when faced with sophisticated cyber-attacks. This resilience should be regularly tested through scenarios that combine multiple attack vectors and techniques, validating the organization's comprehensive defensive capabilities.

Through careful attention to control implementation and validation, organizations can build and maintain robust defenses against evolving cyber threats. This systematic approach ensures that security investments deliver measurable improvements in protection while supporting, rather than hindering, critical infrastructure operations.

VI. Attack Path Prioritization Using Frenos

Building upon the foundational elements of threat intelligence and breach simulation outlined in previous sections, effective attack path prioritization represents the crucial bridge between identifying potential vulnerabilities and implementing targeted defensive measures. The integration of Frenos into this framework provides organizations with sophisticated capabilities for automated attack path discovery and prioritization, enabling more efficient allocation of security resources.

Automated Attack Path Analysis

Frenos brings automation to the complex task of understanding how attackers might move through an organization's infrastructure. Through continuous network analysis, Frenos maps the relationships between assets, permissions, and trust relationships to generate comprehensive attack graphs. These graphs reveal potential paths that attackers could exploit to reach critical assets, including subtle chains of trust relationships that might be overlooked in manual analysis.

The system's reachability analysis goes beyond simple network connectivity to consider the full spectrum of potential attack vectors, including misconfigurations, weak credentials, and trust relationships between systems. This comprehensive approach ensures that organizations understand not just direct attack paths but also complex, multi-stage attack sequences that sophisticated adversaries might employ.

Risk-Based Prioritization

The true value of attack path analysis lies in the ability to prioritize remediation efforts effectively. Frenos implements a sophisticated risk scoring system that considers multiple factors when evaluating the criticality of identified attack paths. Path complexity scoring examines the technical sophistication required to exploit each path, while asset criticality weighting ensures that paths leading to the most critical infrastructure components receive appropriate attention.

Exploitation likelihood assessment incorporates current threat intelligence to evaluate the probability of specific attack paths being targeted. This assessment considers factors such as known adversary capabilities, current attack trends, and the availability of exploit tools or techniques. When combined with business impact analysis, these factors produce a comprehensive risk score that guides prioritization decisions.

Integration with Breach and Attack Simulation

Frenos enhances the effectiveness of BAS programs by automatically generating test scenarios based on discovered attack paths. This integration ensures that simulation efforts focus on validating the most critical and likely attack vectors rather than testing arbitrary scenarios. The system maintains a continuous feedback loop between attack path discovery and validation testing, ensuring that new paths are quickly identified and assessed.

The platform's control validation mapping provides clear visibility into which security controls protect against specific attack paths. This mapping helps organizations understand gaps in their defensive coverage and validate the effectiveness of existing controls. Real-time monitoring of control effectiveness ensures that changes in the environment that might impact security are quickly identified and addressed.

Continuous Improvement Process

Frenos enhances the effectiveness of BAS programs by automatically generating test scenarios based on discovered attack paths. This integration ensures that simulation efforts focus on validating the most critical and likely attack vectors rather than testing arbitrary scenarios. The system maintains a continuous feedback loop between attack path discovery and validation testing, ensuring that new paths are quickly identified and assessed.

The platform's control validation mapping provides clear visibility into which security controls protect against specific attack paths. This mapping helps organizations understand gaps in their defensive coverage and validate the effectiveness of existing controls. Real-time monitoring of control effectiveness ensures that changes in the environment that might impact security are quickly identified and addressed.

Remediation Planning and Execution

Effective remediation planning requires more than just identifying problems – it requires actionable guidance on how to address them. Frenos's control recommendation engine analyzes identified attack paths and suggests specific defensive measures that would be most effective in mitigating the risk. These recommendations consider both the technical requirements for remediation and the potential operational impact of proposed changes.

Implementation prioritization is guided by a comprehensive understanding of risk and resource constraints. The system helps organizations develop realistic remediation timelines that balance security requirements with operational considerations. A structured validation workflow ensures that remediation efforts effectively address identified risks while maintaining system functionality.

Measuring Effectiveness

The ultimate measure of any security program lies in its ability to demonstrate concrete improvements in security posture. Frenos provides comprehensive metrics that track both coverage of potential attack paths and the effectiveness of remediation efforts. Path coverage metrics show what percentage of potential attack vectors are protected by current controls, while risk reduction tracking quantifies the impact of security improvements over time.

Time to resolution metrics help organizations understand and optimize their security operations, while broader security posture improvement measurements demonstrate the overall effectiveness of the program. These metrics provide the quantitative evidence needed to justify security investments and demonstrate progress to stakeholders.

Through the integration of Frenos into their proactive defense framework, organizations can move beyond reactive security measures to implement truly predictive and preventive security controls. This systematic approach to attack path analysis and remediation ensures that security resources are focused where they will have the greatest impact in protecting critical infrastructure from sophisticated cyber-attacks.

VII. Conclusion:
Moving from Reactive to Proactive Defense

The increasing sophistication of cyber-attacks against critical infrastructure demands a fundamental shift in how organizations approach cybersecurity. Traditional reactive security measures, while still necessary, are no longer sufficient to protect essential services and operations from determined adversaries. This framework demonstrates how organizations can implement a truly proactive defense strategy that anticipates and prevents attacks before they can impact critical systems.

The integration of comprehensive threat intelligence with practical validation through simulation creates a powerful feedback loop that drives continuous security improvement. By understanding and analyzing current threats through industry partnerships and intelligence sharing, organizations can anticipate likely attack vectors and implement targeted defensive measures. This intelligence-driven approach ensures that security resources are focused where they will have the greatest impact in preventing successful attacks.

Breach and Attack Simulation (BAS) provides the crucial validation layer that transforms theoretical security models into practical, proven defenses. Through automated, continuous testing, organizations can verify that their security controls actually deliver the expected protection against real-world attack techniques. This validation process helps identify and eliminate gaps in coverage before they can be exploited by adversaries, while providing quantitative metrics that demonstrate security program effectiveness.

The incorporation of advanced attack path analysis through Frenos represents a significant evolution in proactive defense capabilities. By automatically discovering and prioritizing potential attack paths, organizations can more effectively allocate their security resources to address the most critical vulnerabilities. This systematic approach to understanding and eliminating attack vectors helps prevent the sophisticated, multi-stage attacks that often target critical infrastructure.

Perhaps most importantly, this framework emphasizes the need for continuous adaptation and improvement in security measures. The threat landscape facing critical infrastructure continues to evolve rapidly, with adversaries constantly developing new attack techniques and capabilities. Through the implementation of automated testing, continuous validation, and dynamic priority adjustment, organizations can ensure that their defensive capabilities keep pace with emerging threats.

Success in protecting critical infrastructure ultimately depends on the ability to demonstrate measurable improvements in security posture. This framework provides the metrics and validation methodologies needed to quantify risk reduction and control effectiveness. These measurements not only guide ongoing security improvements but also help justify security investments to stakeholders and demonstrate compliance with regulatory requirements.

The future of critical infrastructure security lies not in merely responding to attacks, but in proactively identifying and eliminating attack vectors before they can be exploited. By implementing this comprehensive framework, organizations can build robust, resilient defenses that protect essential services while adapting to meet new security challenges as they emerge. As cyber threats continue to evolve, this proactive approach to defense will become increasingly crucial for maintaining the security and reliability of critical infrastructure systems.