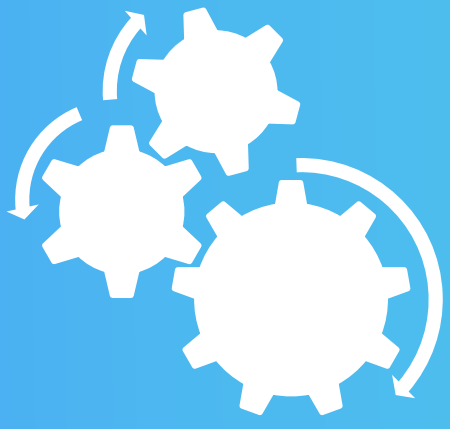
Feroot

How Feroot Aligns with Cybersecurity Frameworks

- NIST
- MITR ATT&CK
- PRE-ATT&CK
- Operations



1 NIST CYBERSECURITY FRAMEWORK (CSF)

The NIST Cybersecurity Framework (CSF) is one of the top if not the number one cybersecurity frameworks. By aligning with the NIST CSF, organizations can benefit from clear standards, guidelines, and actionable best practices to help protect your organization, reduce risk, and ensure business continuity.

For effective recovery, responders need to have the right information at hand. Feroot Access Insight analysis report provides a prioritized list of asset's state of security for a timely and complete recovery and to ensure that that all assets are operating as desired.

Feroot uses a behavior-based approach to accurately identify data assets and data ingestion touchpoints. Full asset visibility is the key to accurate risk mitigation and furthering cybersecurity program maturity.

Feroot Inspector helps you quickly perform threat hunting, containment, and remediation. Its alerts and events provide rich contextual information about the source, nature, and target of the threat. It reports key analysis including samples of data access attempts, such as keyloggers, related to the threat.

The Feroot platform provides real-time shielding and visibility into data assets within the front end of web applications and its dependencies. It enables the least privilege and zero trust operations to help ensure reliable controls are in place.

Feroot detects and blocks activities that can indicate an attack. It alerts and reports data access attempts initiated by legitimate and misconfigured application's elements, third-party and open-source dependencies, or threat actors. Feroot sends alerts and events to SIEMs, protective technologies, and other tools, saving you time by facilitating quick response and recovery.

Feroot capabilities aligns with these 18 NIST functions, categories and subcategories:

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

ID.AM-3: Organizational communication and data flows are mapped

ID.AM-2: Software platforms and applications within the organization are inventoried

ID.RA-1: Asset vulnerabilities are identified and documented

ID.RA-3: Threats, both internal and external, are identified and documented

ID.RA-4: Potential business impacts and likelihoods are identified

ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process

ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition

PR.DS-5: Protections against data leaks are implemented

PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity

PR.IP-1: A baseline configuration of information technology systems is created and maintained incorporating security principles (e.g. concept of least functionality)

PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

DE.AE-2: Detected events are analyzed to understand attack targets and methods

DE.AE-4: Impact of events is determined

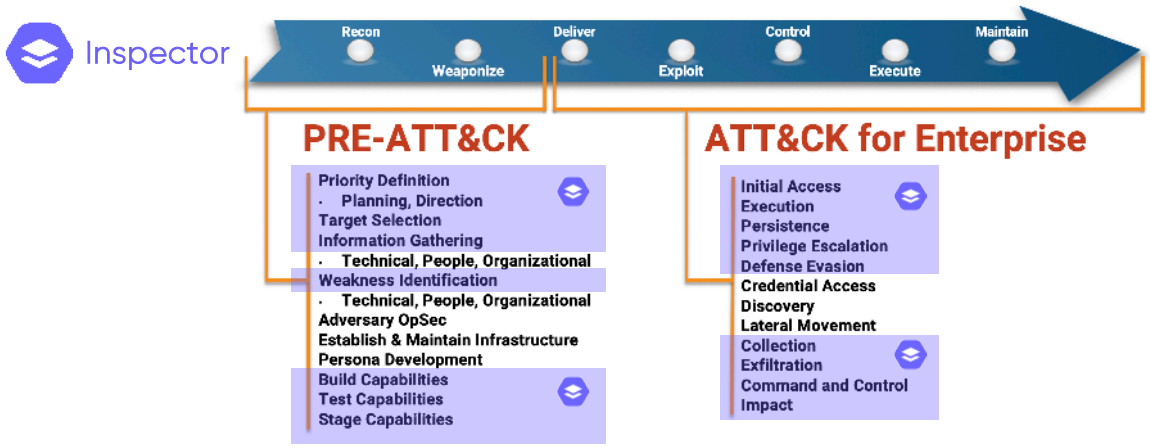
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events

RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks

2 ATT&CK AND PRE-ATT&CK

MITRE ATT&CK and PRE-ATT&CK tactics frameworks are great resources to understand gaps not only in your cybersecurity program but in your coverage and maturity as well. Knowing the attack chain, knowing the patterns enables you better craft and fine tune your program and making your Blue Team stronger. ATT&CK and PRE-ATT&CK frameworks are great final arbiters as well to look at any gaps or questions.

Feroot capabilities aligns with these 17 MITRE ATT&CK and PRE-ATT&CK Tactics:



MITRE ATT&CK™ framework - SaaS Matrix

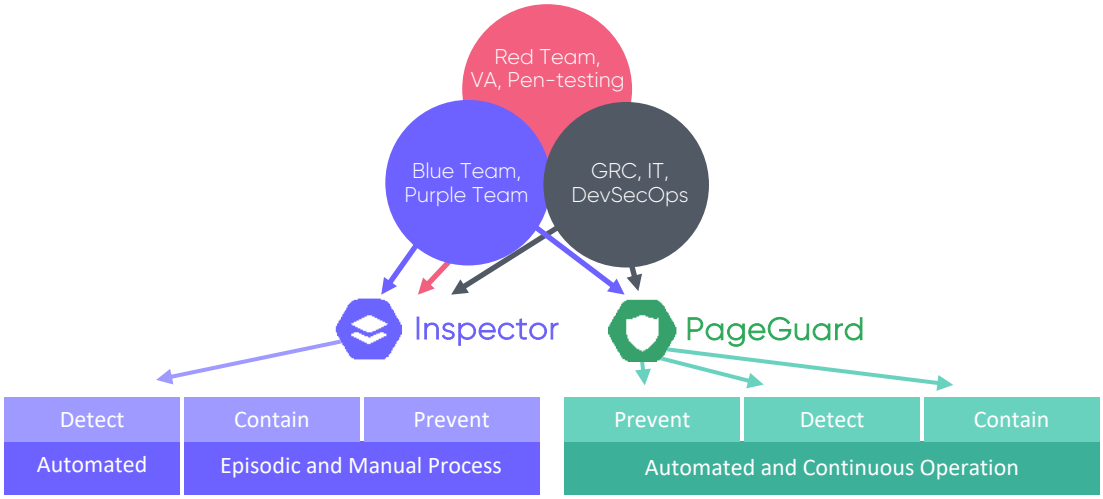
Feroot platform capabilities enable detection and/or protection against a number of tactics and technique outlined by the MITRE ATT&CK framework, including:

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
Drive-by Compromise	Redundant Access	Valid Accounts	Application Access Token	Brute Force	Cloud Service Discovery	Application Access Token	Data from Information Repositories
Spearphishing Link	Valid Accounts		Redundant Access	Steal Application Access Token		Internal Spearphishing	
Trusted Relationship			Valid Accounts	Steal Web Session Cookie		Web Session Cookie	
Valid Accounts			Web Session Cookie				

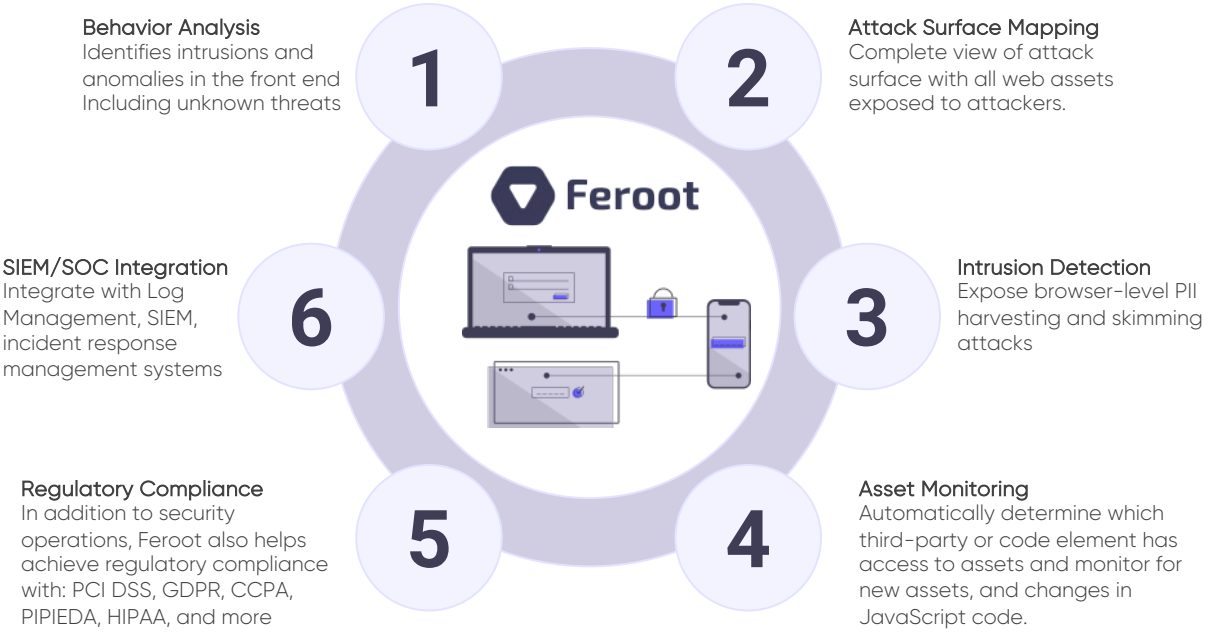
MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

3 PEOPLE AND PROCESS ALIGNMENT

Feroot platform secures the front end [client-side] of web applications and websites protecting the digital user experience against today's and tomorrow's threats. Feroot dashboards and reports providing a consolidated view of findings for security, GRC, and technology operations teams.



Feroot provides run-time in-app protection capabilities that harden the front end of consumer and employee-facing web applications to help prevent incidents and deter attacks.



Behavior Analysis
Identifies intrusions and anomalies in the front end Including unknown threats

Attack Surface Mapping
Complete view of attack surface with all web assets exposed to attackers.

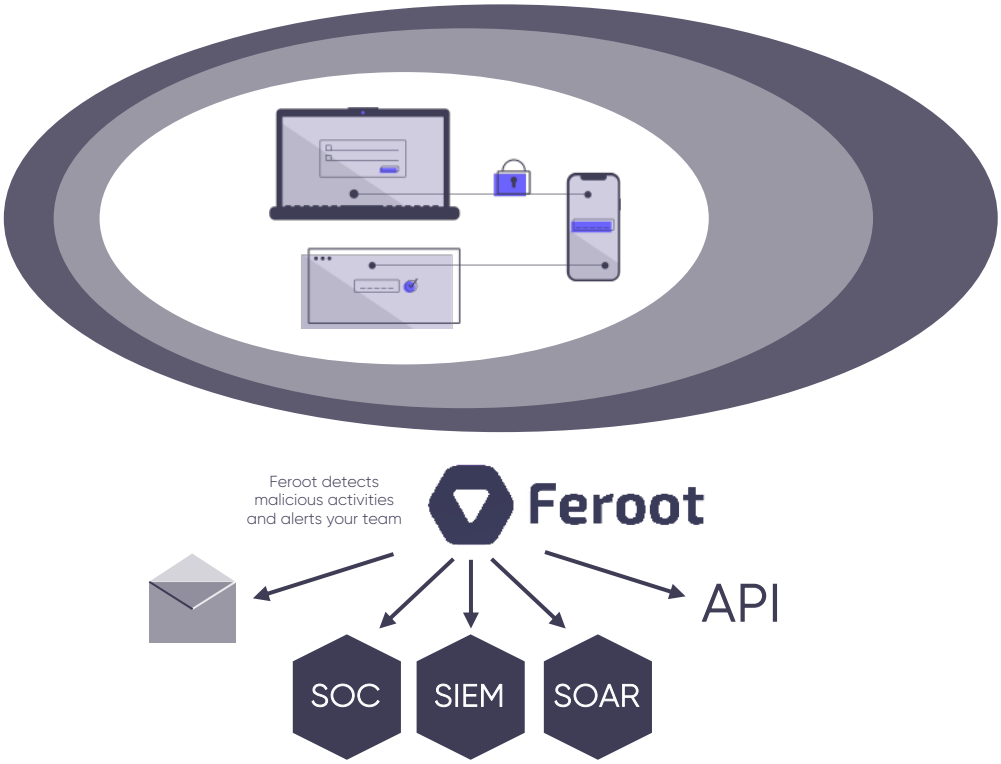
SIEM/SOC Integration
Integrate with Log Management, SIEM, incident response management systems

Intrusion Detection
Expose browser-level PII harvesting and skimming attacks

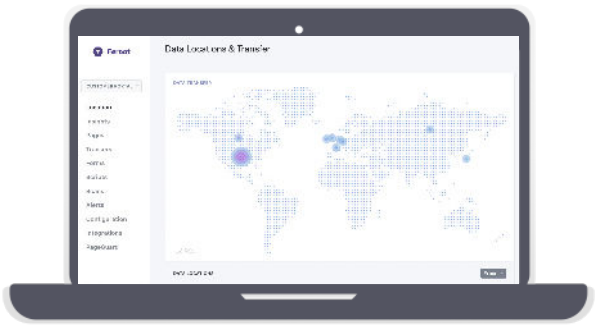
Regulatory Compliance
In addition to security operations, Feroot also helps achieve regulatory compliance with: PCI DSS, GDPR, CCPA, PIPIEDA, HIPAA, and more

Asset Monitoring
Automatically determine which third-party or code element has access to assets and monitor for new assets, and changes in JavaScript code.

4 ABOUT FEROOT



Feroot is the lock and alarm system for every backdoor that gets introduced into front end user experience of web applications. By using Feroot, companies can drive their business by introducing the best-in-breed technology and ensure that every side door is locked and watched. The platform uses integrated in-app protection and proactive threat detection to prevent incidents, not just finding risks, while easily integration into your DevSecOps, SIEM, SOC, GRC, other operational processes.



www.feroot.com