

Application Analysis with ModSecurity



Michael Edie

SENIOR SECURITY ENGINEER

@tankmek blog.edie.io



modsecurity

Open Source Web Application Firewall



modsecurity

Open Source Web Application Firewall

Creator: “Ivan Ristić”

ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx that is developed by Trustwave's SpiderLabs. ModSecurity provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring, logging and real-time analysis.





An open-source web application firewall (WAF) that filters, monitors, and blocks HTTP traffic to a web application.

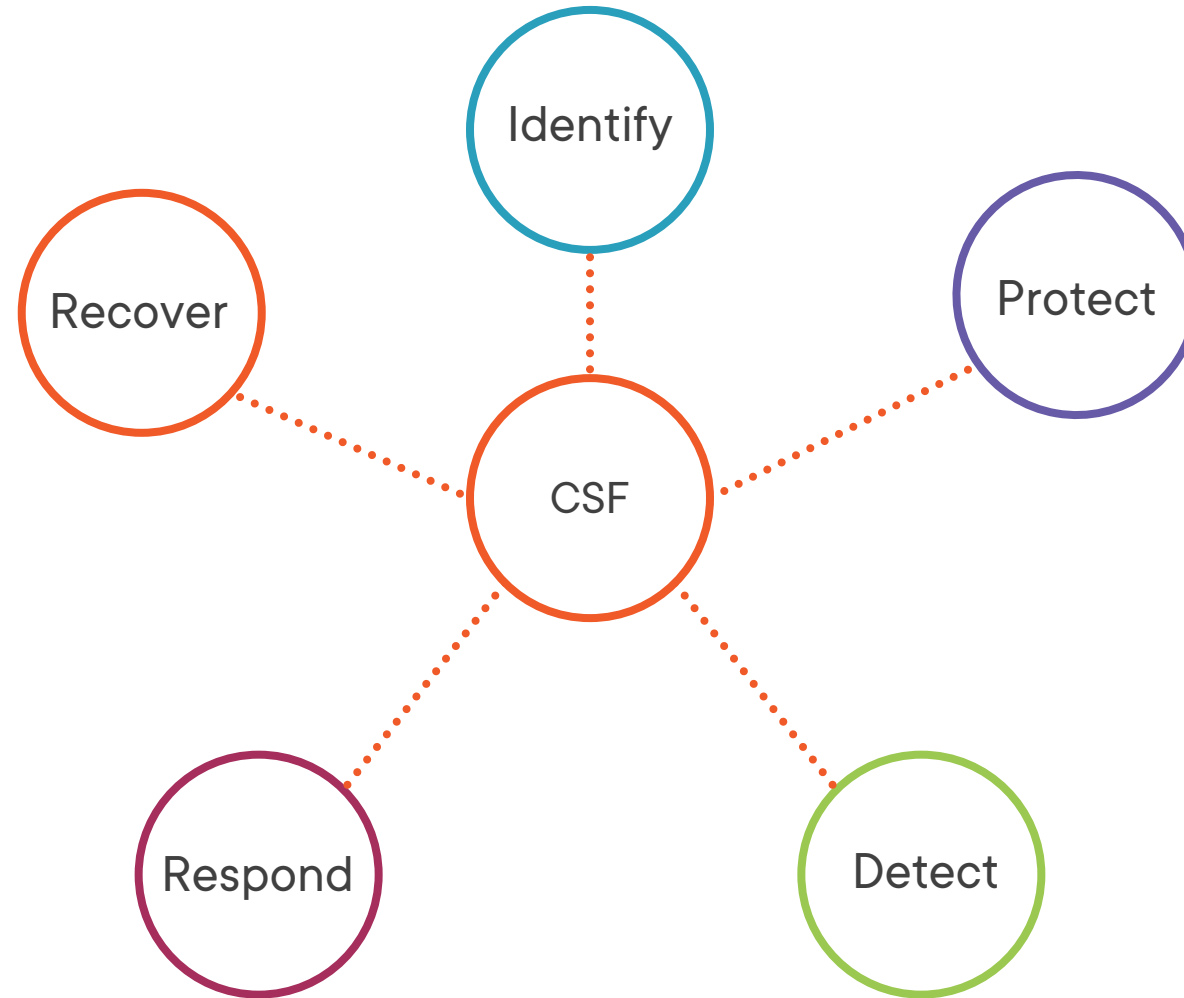
Can be accessed from:

<https://github.com/SpiderLabs/ModSecurity>

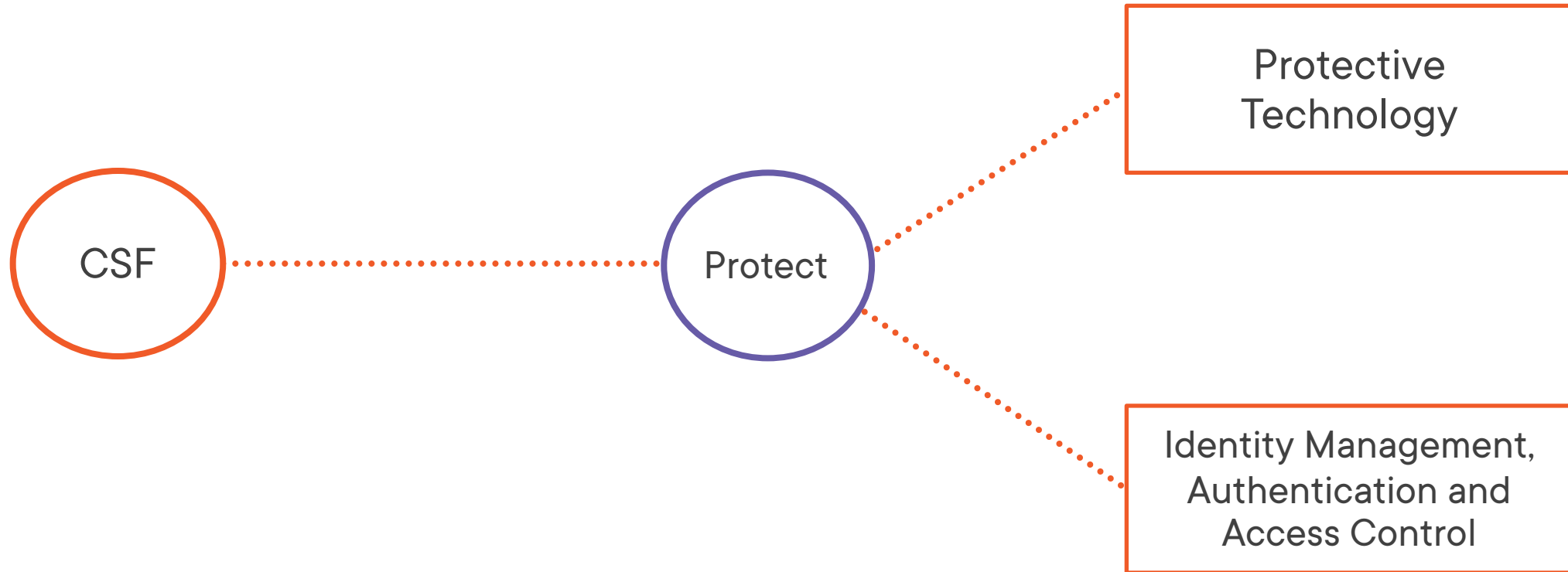
Provides support for Apache, Nginx, and IIS. Helps harden web applications against malicious attacks. It can be used embedded or as a reverse proxy. PCI DSS Requirement 6.6 compliance.



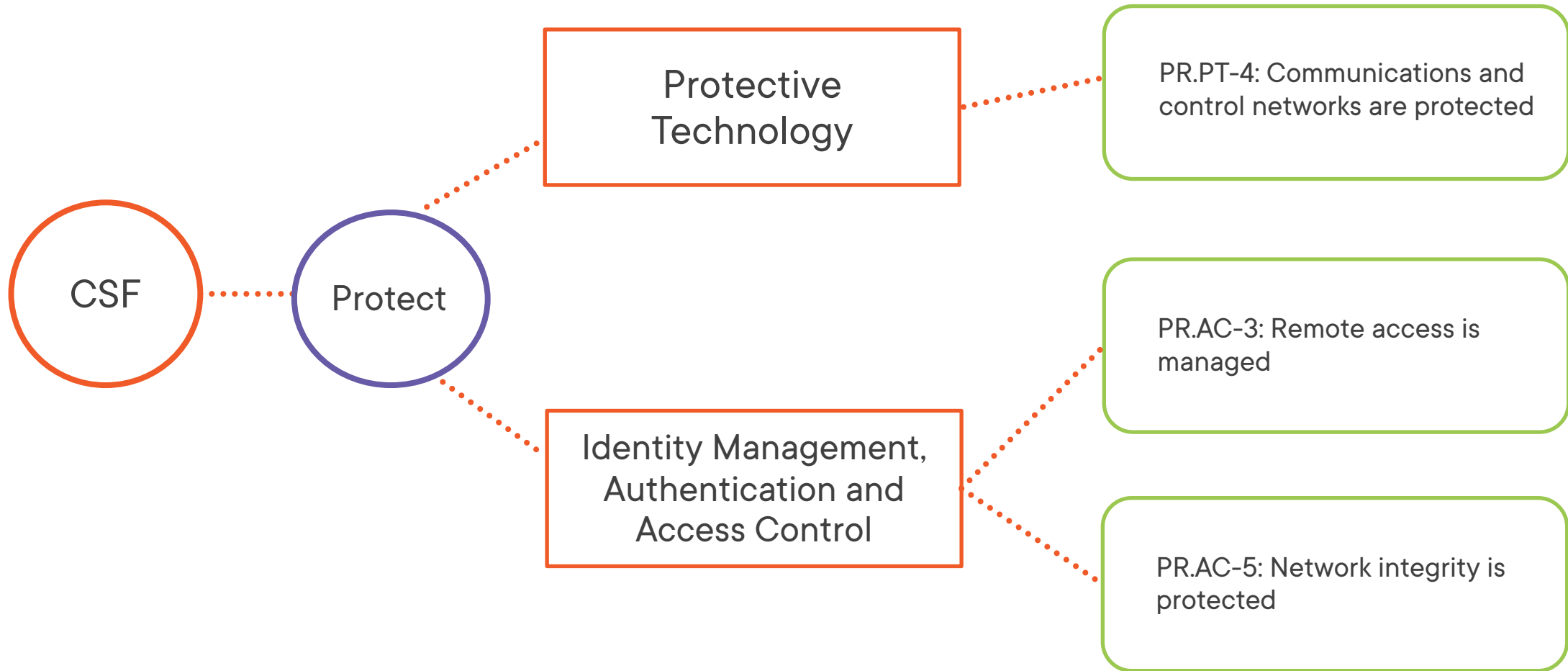
NIST Cybersecurity Framework



NIST Cybersecurity Framework



NIST Cybersecurity Framework



MITRE ATT&CK

Data Analysis Type

Network Analysis

OS Analysis

Application Analysis

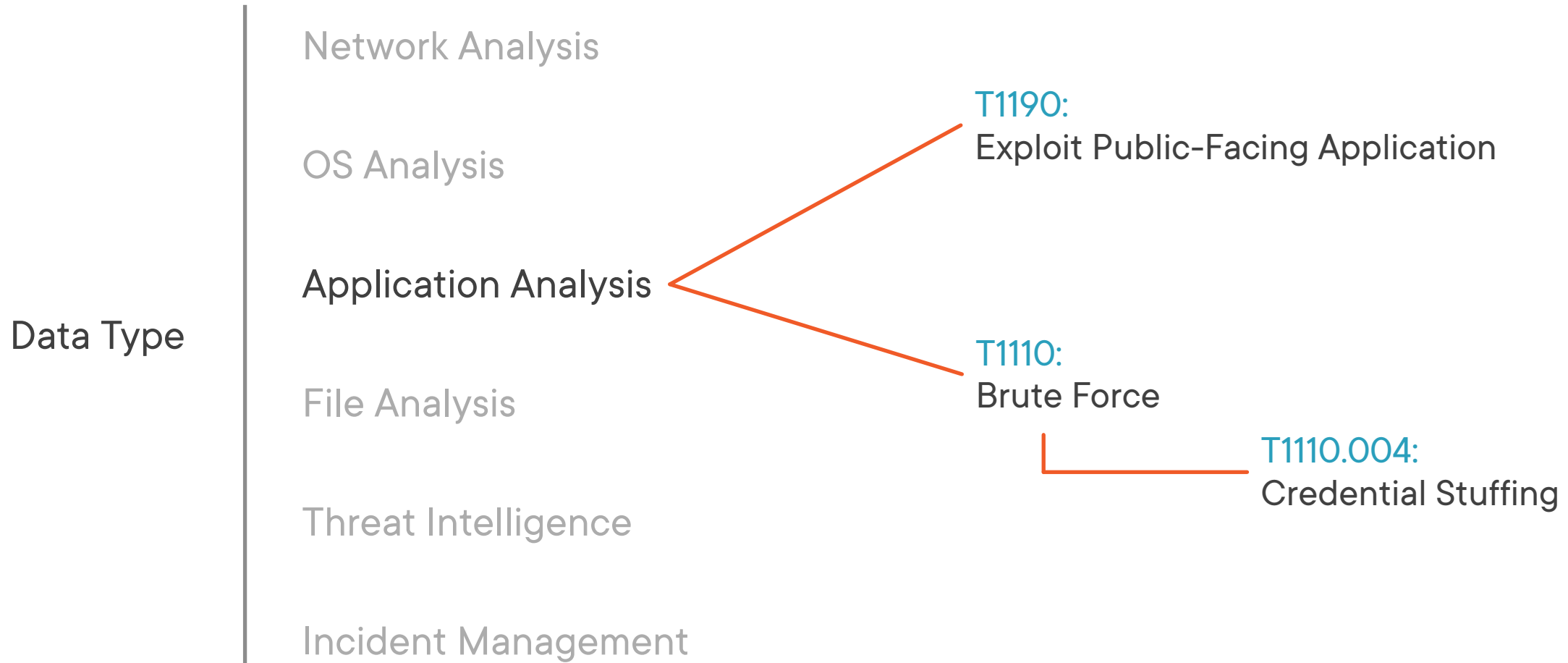
File Analysis

Threat Intelligence

Incident Management



MITRE ATT&CK



modsecurity

Open Source Web Application Firewall

