IMPERVA®

Correlated Attack Validation

Security Accuracy Based on Correlation of Suspicious Behavior

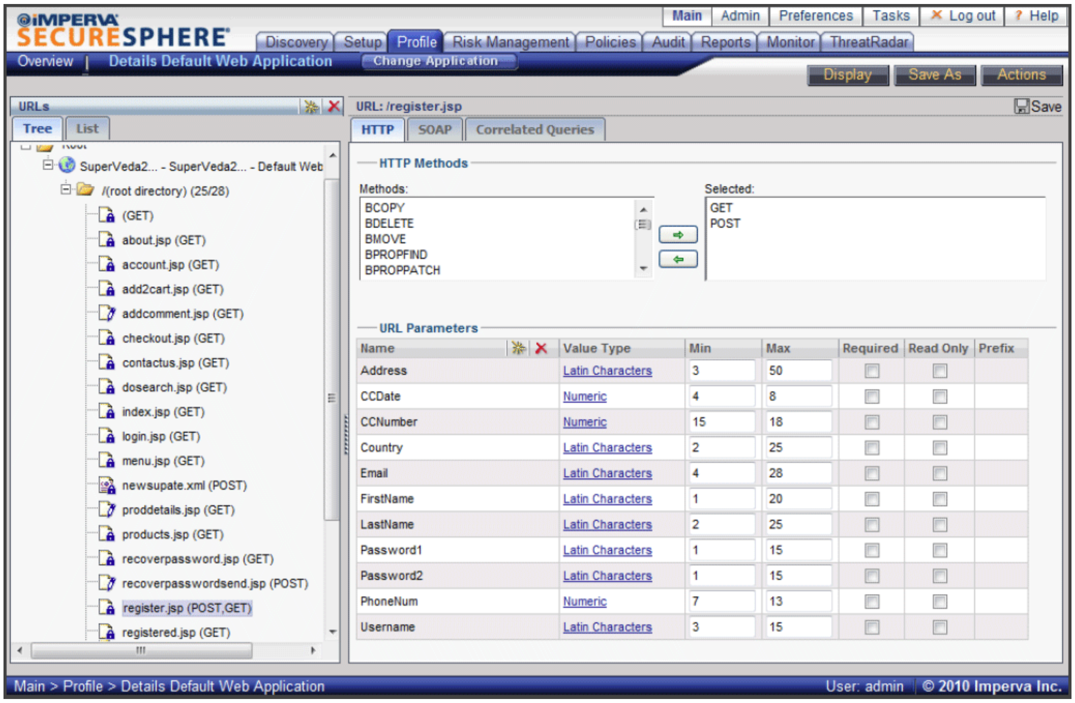
Today's security threats include advanced multi-vector attacks, persistent, and methodical reconnaissance, and automated attacks. Making a security decision based on just one factor might overlook information that would provide context and additional insight into the event Correlated Attack Validation provides SecureSphere customers with accurate protection against malicious activity by analyzing multiple data points, including protocol violations, attack signatures, data leak signatures, user reputation, and variance from past behavior. Both custom and pre-defined correlation rules deliver stronger protection against today's complex, multi-vector attacks.

Up-to-date White List and Black List Security

Imperva SecureSphere incorporates a multi-layer security architecture that enables precise attack protection without requiring burdensome manual tuning. SecureSphere's security architecture incorporates both positive (white list) and negative (black list) security models. Robust enforcement algorithms draw on these two security models to identify and block even the most sophisticated attacks.

SecureSphere's black list security model, which includes application attack signatures, live IP reputation data, and pre-defined security rules, is powered by research from the Imperva Application Defense Center (ADC). SecureSphere's attack signatures detect known attacks targeting web server, application, and operating system vulnerabilities. The Imperva ADC investigates vulnerabilities reported throughout the world and analyzes actual traffic and attacks to real websites to identify the latest threats. Signatures are automatically updated to ensure protection against current threats.

Dynamic Profiling, which is the core of Imperva's dynamic white list security model enables SecureSphere to detect any changes in application or database usage. Patented Dynamic Profiling technology automatically learns an application's elements, structure, and usage and adapts to application changes over time. Dynamic Profiling policies are designed to look for anomalies that would indicate an attack, not just Web requests that violate the white list. By focusing on attack vectors, SecureSphere eliminates the need for application profile tuning and dramatically reduces false positives.



URL: /register.jsp

SuperVeda2... - SuperVeda2... - Default Web
/(root directory) (25/28)
(GET)
about.jsp (GET)
account.jsp (GET)
add2cart.jsp (GET)
addcomment.jsp (GET)
checkout.jsp (GET)
contactus.jsp (GET)
dosearch.jsp (GET)
index.jsp (GET)
login.jsp (GET)
menu.jsp (GET)
newsupate.xml (POST)
proddetails.jsp (GET)
products.jsp (GET)
recoverpassword.jsp (GET)
recoverpasswordsend.jsp (POST)
register.jsp (POST,GET)
registered.jsp (GET)

HTTP Methods

Methods:
BCOPY
BDELETE
BMOVE
BPROPFIND
BPROPPATCH

Selected:
GET
POST

URL Parameters

Name	Value Type	Min	Max	Required	Read Only	Prefix
Address	Latin Characters	3	50	□	□	
CCDate	Numeric	4	8	□	□	
CCNumber	Numeric	15	18	□	□	
Country	Latin Characters	2	25	□	□	
Email	Latin Characters	4	28	□	□	
FirstName	Latin Characters	1	20	□	□	
LastName	Latin Characters	2	25	□	□	
Password1	Latin Characters	1	15	□	□	
Password2	Latin Characters	1	15	□	□	
PhoneNum	Numeric	7	13	□	□	
Username	Latin Characters	3	15	□	□	

Dynamic Profiling automatically builds a profile of application elements, structure and usage, including URLS, form fields, parameters, cookies and expected user input.

The positive security model also includes HTIP and SQL protocol validation. Together, SecureSphere's positive and negative security models form a complete picture of normal behavior that extends from valid network IP addresses to high-level application and database operations.

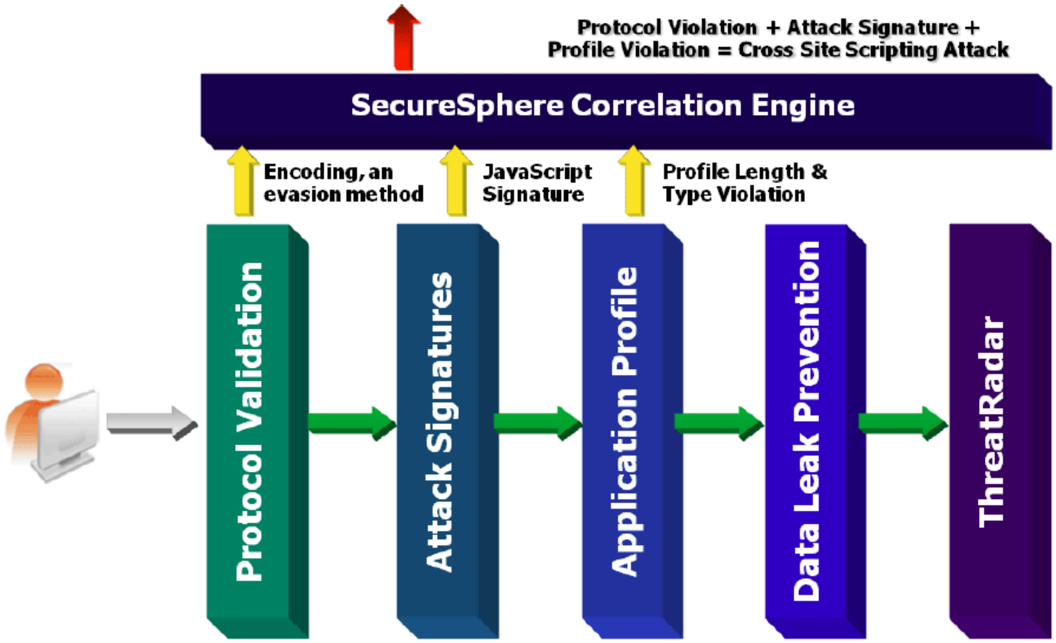
Sophisticated Signature Analysis for Granular Security

SecureSphere identifies some violations as merely suspicious while recognizing other violations as definitive indicators of an attack. Attack signatures are categorized based on attack severity and likelihood of a false positive. If an attack signature definitively detects an attack without any risk of false positives, then SecureSphere will be configured to block a Web request that contains the signature. However, if a signature has a high probability of false positives, then SecureSphere will alert but not block the request. Both signatures, though, are used by SecureSphere's correlation engines.

Multi-Layered Analysis for Accurate Decision Making

Imperva's unique Correlated Attack Validation examines multiple pieces of information at the network, protocol and application level immediately and over time to distinguish between attacks and valid user traffic. By basing decisions on multiple observations rather than a single event, Correlated Attack Validation delivers a highly accurate and completely automated defense system against application attacks and abuse.

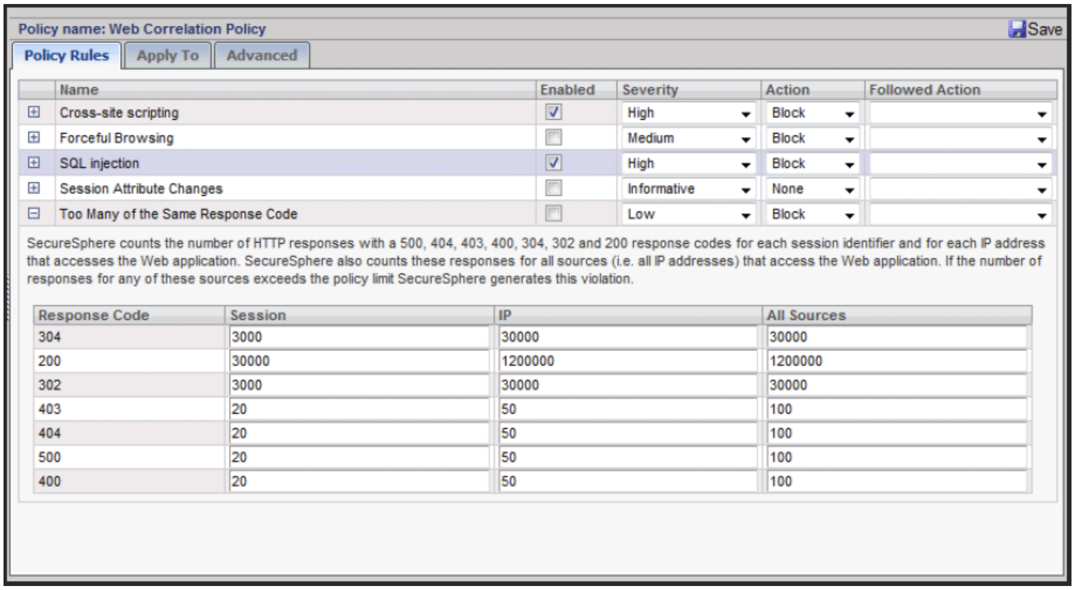
To illustrate Correlated Attack Validation in action, consider a common evasion technique: HTTP smuggling. When a hacker performs an HTIP smuggling attack, SecureSphere will detect that the Web request contains multiple Content-Length fields and correlate this information with an attack signature to accurately identify and block the attack. Analyzing multiple data security layers, in this case an HTTP protocol violation and an attack signature, enables SecureSphere to provide an unparalleled level of protection.


Protocol Violation + Attack Signature +
Profile Violation = Cross Site Scripting Attack
SecureSphere Correlation Engine
Encoding, an evasion method
JavaScript Signature
Profile Length & Type Violation
Protocol Validation
Attack Signatures
Application Profile
Data Leak Prevention
ThreatRadar

SecureSphere's Correlated Attack Validation tracks and correlates multiple events to accurately identify and block sophisticated attacks.

Correlated Attack Validation and Security Accuracy

For Imperva, delivering accurate protection without false positives has been the most important design objective. Imperva SecureSphere delivers an extremely low rate of false positives due to its Correlated Attack Validation technology, as well as its patented Dynamic Profiling and its rigorously tested security policies and signatures from the Imperva Application Defense Center. Correlated Attack Validation manifests itself in SecureSphere as pre-defined correlation rules, such as SQL injection, Cross-Site Scripting, and forceful browsing, and as custom Web Application security policies. The pre-defined correlation rules take advantage of a statistical analysis engine and severity weighting to correctly identify attacks.



Policy name: Web Correlation Policy

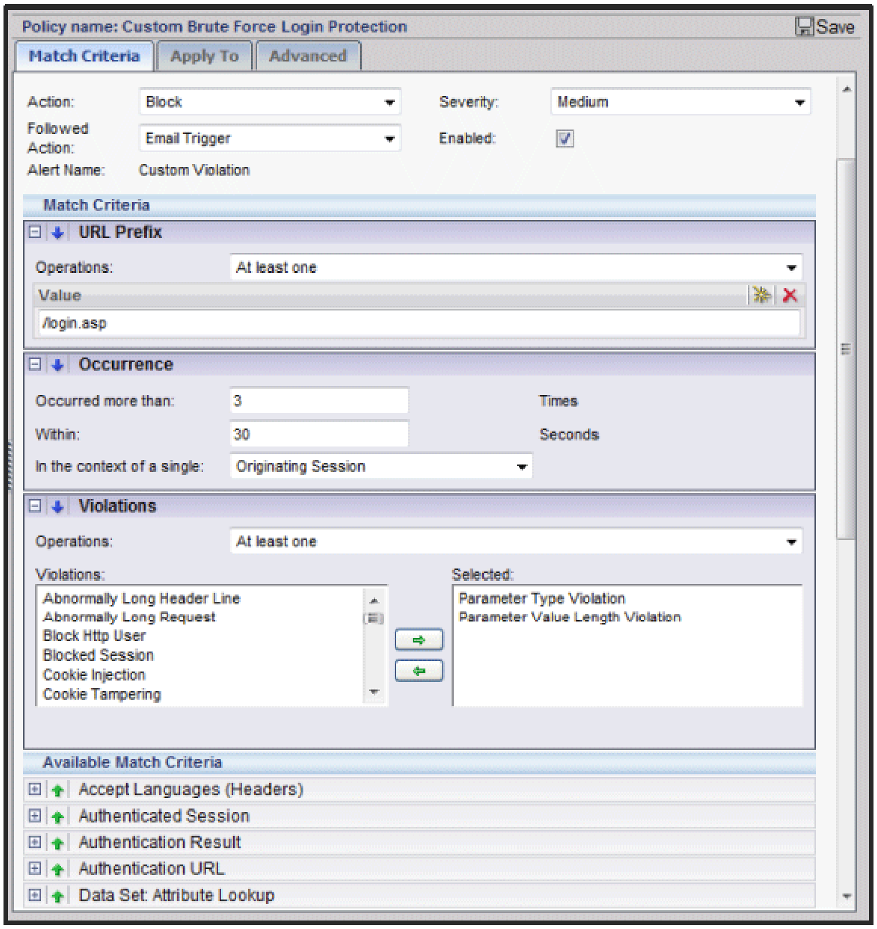
	Name	Enabled	Severity	Action	Followed Action
⊞	Cross-site scripting	☑	High	Block	
⊞	Forceful Browsing	□	Medium	Block	
⊞	SQL injection	☑	High	Block	
⊞	Session Attribute Changes	□	Informative	None	
⊟	Too Many of the Same Response Code	□	Low	Block	

SecureSphere counts the number of HTTP responses with a 500, 404, 403, 400, 304, 302 and 200 response codes for each session identifier and for each IP address that accesses the Web application. SecureSphere also counts these responses for all sources (i.e. all IP addresses) that access the Web application. If the number of responses for any of these sources exceeds the policy limit SecureSphere generates this violation.

Response Code	Session	IP	All Sources
304	3000	30000	30000
200	30000	1200000	1200000
302	3000	30000	30000
403	20	50	100
404	20	50	100
500	20	50	100
400	20	50	100

SecureSphere's pre-defined correlation rules, including advanced SQL injection and Cross-site scripting correlation engines.

Custom correlation policies allow organizations to build granular rules using over two-dozen match criteria including attack signatures, user IP address, user reputation, URL, header information, time of day, and more. SecureSphere provides custom correlation policies by out-of-the-box, including anti Google hacking, data leakage, Cross-Site Request Forgery (CSRF), and directory traversal. Custom correlation policies can be reviewed and adjusted by SecureSphere administrators.



Policy name: Custom Brute Force Login Protection

Action: Block
Severity: Medium
Followed Action: Email Trigger
Enabled: ☑
Alert Name: Custom Violation

Match Criteria

URL Prefix
Operations: At least one
Value
/login.asp

Occurrence
Occurred more than: 3 Times
Within: 30 Seconds
In the context of a single: Originating Session

Violations
Operations: At least one
Violations:
Abnormally Long Header Line
Abnormally Long Request
Block Http User
Blocked Session
Cookie Injection
Cookie Tampering
Selected:
Parameter Type Violation
Parameter Value Length Violation

Available Match Criteria
Accept Languages (Headers)
Authenticated Session
Authentication Result
Authentication URL
Data Set: Attribute Lookup

SecureSphere offers custom web application correlation policies that can be built from over two dozen match criteria. The above image shows a custom brute force policy.

Correlation Provides Industry Low Rate of False Positives and False Negatives

Hackers continually try to evade security detection by crafting attacks that look like innocent HTIP requests. Valid end users often submit requests that deviate from RFC standards or that include suspicious characters and strings. Therefore, it is imperative that a Web Application Firewall can accurately distinguish real attacks from unusual, but legitimate, behavior.

Imperva's unique Correlated Attack Validation technology correctly identifies attacks by correlating Web requests over time and by analyzing multiple request attributes. Correlating information across security layers, including Dynamic Profiling, Web attack signatures, HTTP protocol rules, Web Services security, Imperva's patented Web worm defense, and ThreatRadar reputation-based security, allows SecureSphere to protect Web applications with pinpoint precision. Its low rate of false positives and false negatives is one of the leading reasons why thousands of organizations trust SecureSphere to protect their mission critical Web applications.

www.imperva.com