SECURITY INCIDENT ANALYSIS REPORT

Acme Financial Services - Multi-Stage Cyberattack Investigation

Analyst: Metehan Güven | Date: November 8, 2025 | Incident: October 15, 2024

EXECUTIVE SUMMARY

Splunk SIEM analysis of 82 events revealed coordinated multi-stage attack exploiting documented vulnerabilities. Impact: 3 compromised employees, 16 customer accounts accessed, 245KB data exported, 8-hour detection gap.

OWASP Top 10 2021 Mapping:

- A01:2021 Broken Access Control - API IDOR exploitation (16 accounts)
- A03:2021 Injection - SQL injection with WAF bypass
- A07:2021 Authentication Failures - No MFA (50% phishing success)
- A09:2021 Logging Failures - No real-time alerting

Root Cause: Documented API vulnerability ("may not verify account ownership" - API Docs p.3) remained unpatched.

Methodology: Data validation → temporal analysis → anomaly detection → threat hunting → timeline reconstruction.

Key Finding: Attacker IP (203.0.113.45) within scheduled pentest range (203.0.113.0/24) but attack preceded scheduled test by 5 days, indicating compromised test infrastructure.

INVESTIGATION PROCESS

Data Validation

Four log sources (82 events total) successfully ingested into Splunk SIEM.

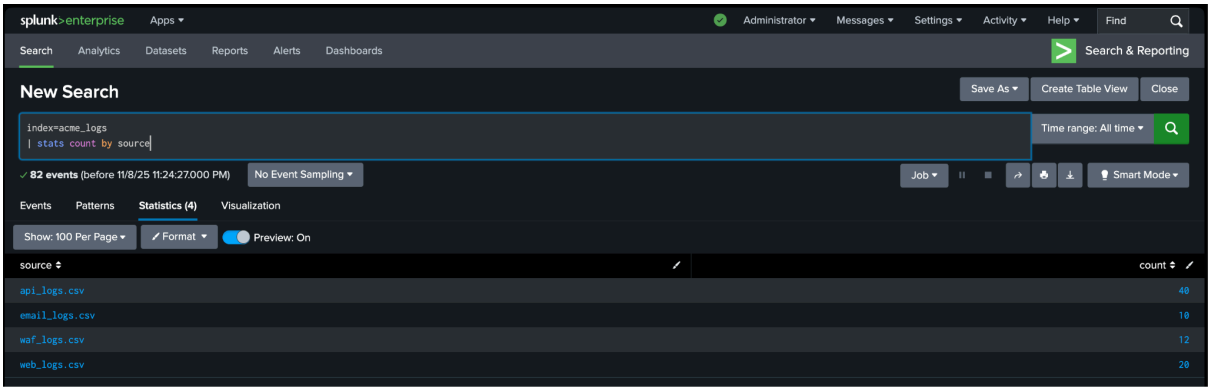


Figure 1: Email (10), WAF (12), web (20), API (40) events validated.

Temporal analysis revealed 09:00 UTC attack spike and 01:30 UTC off-hours activity.

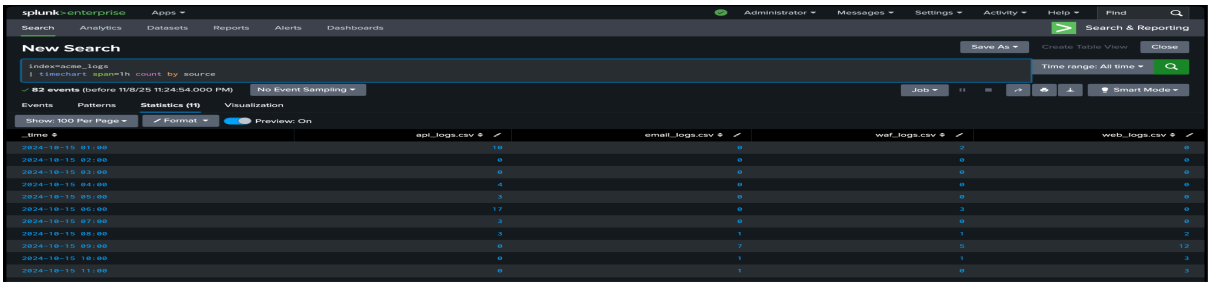


Figure 2: Timeline showing attack concentration. 01:30 activity matches scheduled Tuesday scan.

Phishing Discovery

Email logs revealed URGENT messages from fraudulent sender (security@acme-finance.com).

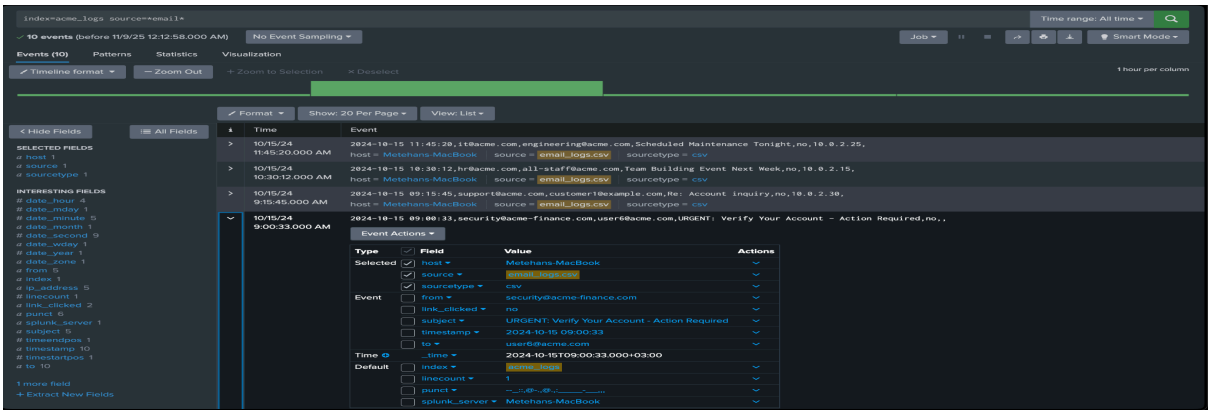
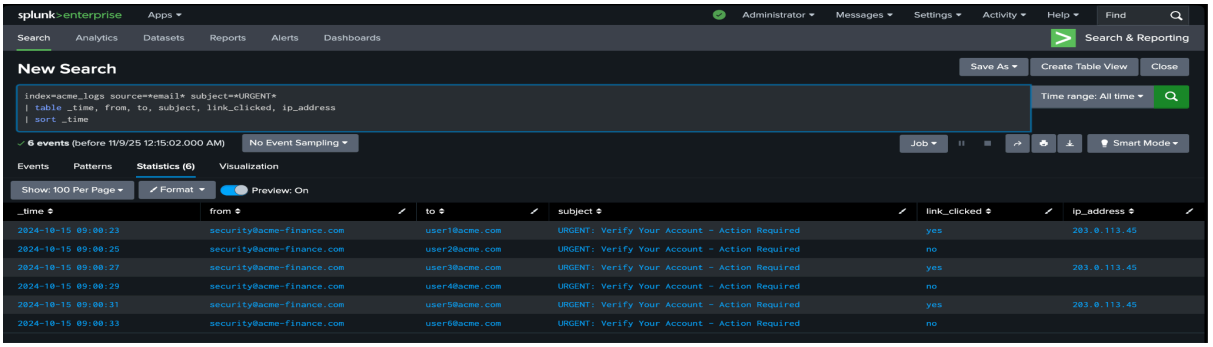


Figure 3: Raw email log - external sender, urgent subject, link tracking enabled.

Query confirmed 6 targets, 3 clicked (50% success). All from IP 203.0.113.45.



_time	from	to	subject	link_clicked	ip_address
2024-10-15 09:00:23	security@acme-finance.com	user1@acme.com	URGENT: Verify Your Account - Action Required	yes	203.0.113.45
2024-10-15 09:00:25	security@acme-finance.com	user2@acme.com	URGENT: Verify Your Account - Action Required	no	
2024-10-15 09:00:27	security@acme-finance.com	user3@acme.com	URGENT: Verify Your Account - Action Required	yes	203.0.113.45
2024-10-15 09:00:29	security@acme-finance.com	user4@acme.com	URGENT: Verify Your Account - Action Required	no	
2024-10-15 09:00:31	security@acme-finance.com	user5@acme.com	URGENT: Verify Your Account - Action Required	yes	203.0.113.45
2024-10-15 09:00:33	security@acme-finance.com	user6@acme.com	URGENT: Verify Your Account - Action Required	no	

Figure 4: Phishing victims (user1, user3, user5) and attacker IP. IP within pentest range but timing suspicious.

TECHNICAL FINDINGS

SQL Injection & WAF Bypass

Following credential compromise, attacker attempted SQL injection against web application. Raw WAF log inspection revealed multiple injection patterns.

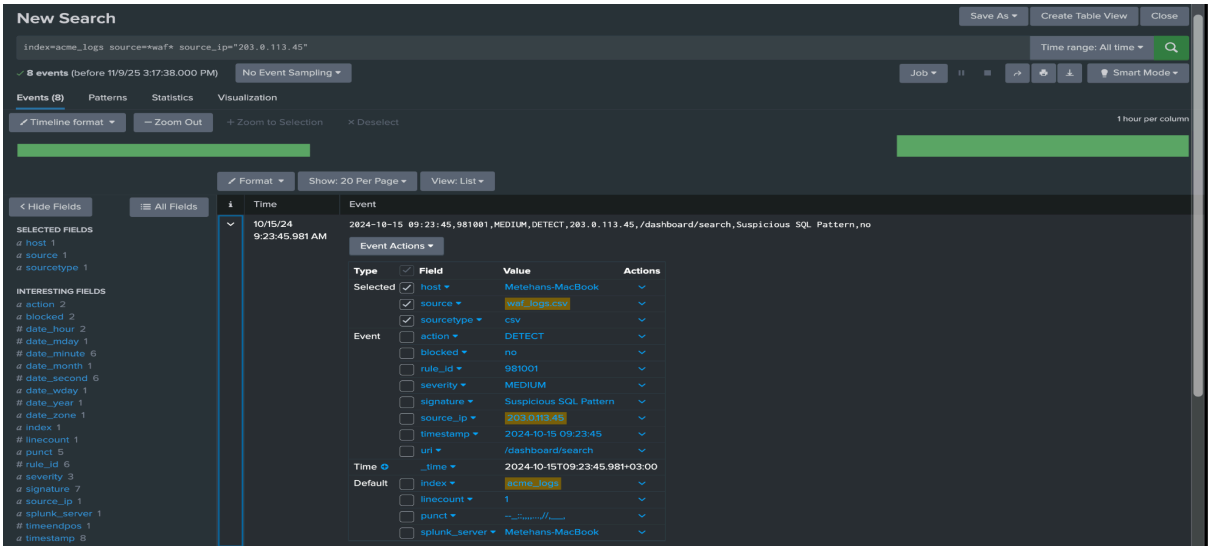


Figure 5: Raw WAF log showing SQL injection detection.

Four attempts (09:20-09:23): 3 blocked, 1 bypassed via pattern obfuscation.

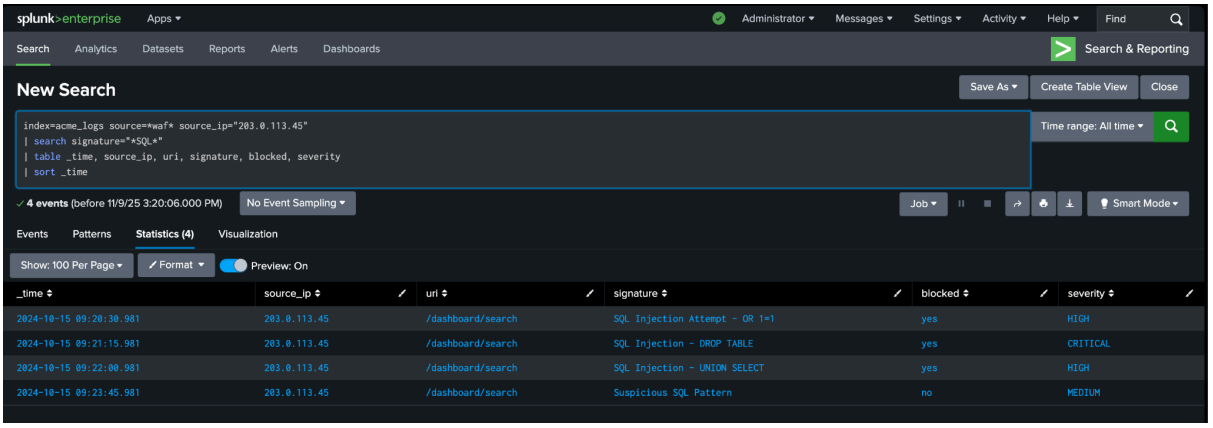


Figure 6: Three blocked (OR 1=1, DROP TABLE, UNION SELECT), one bypassed (Suspicious SQL Pattern, 09:23:45).

API Broken Access Control

Sequential enumeration of 16 accounts (1523-1538), all returning 200 OK. Confirms documented vulnerability: "may not verify account ownership" (API Docs p.3).

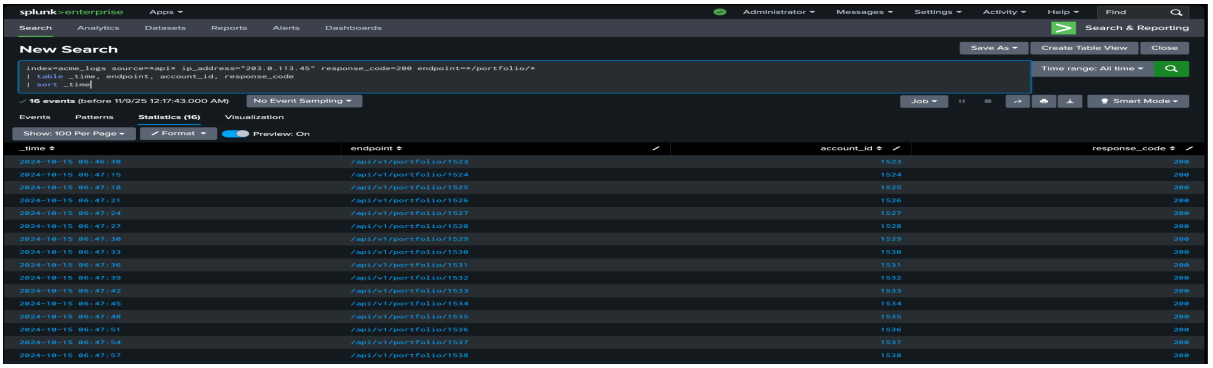


Figure 7: All 16 API requests succeeded - IDOR vulnerability confirmed.

Internal IP 192.168.1.100 at 01:30 matches scheduled scan. Admin activity (245KB export at 08:55) requires investigation - timing 3 hours before phishing.

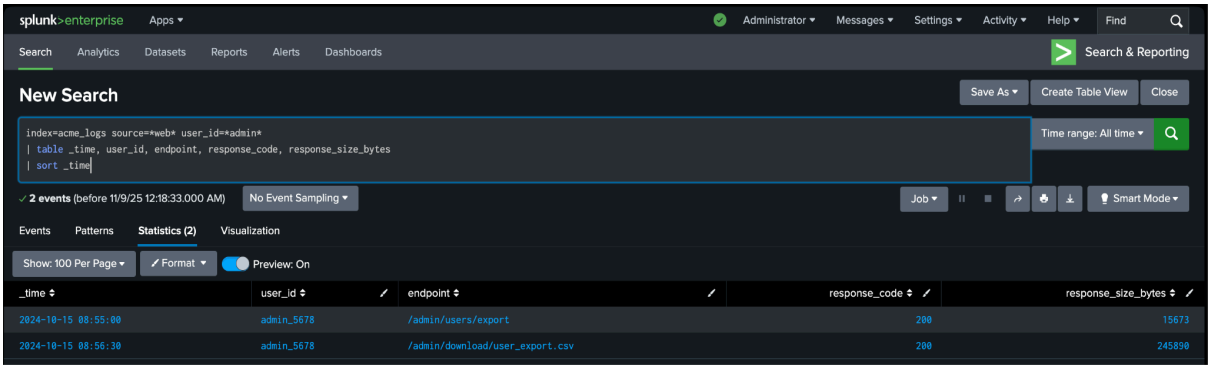


Figure 8: Admin exported 245KB user data before attack.

ARCHITECTURE ANALYSIS

Current Architecture Vulnerabilities

Analysis of existing architecture identified critical security gaps enabling the attack:

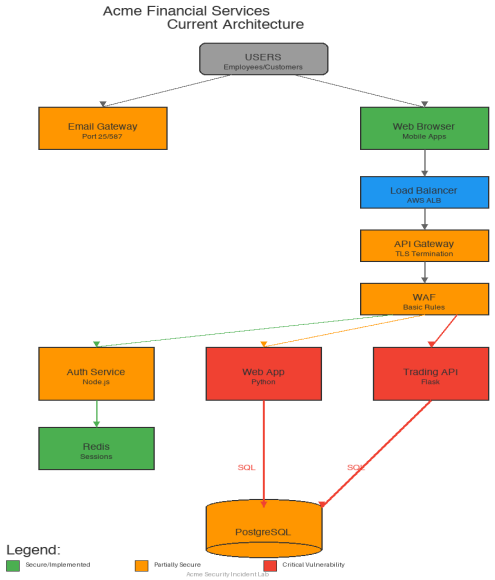


Figure 9: Current architecture showing critical vulnerabilities.

- WAF: Basic signature rules bypassed via obfuscation
- API Gateway: No authorization validation on portfolio endpoints
- Web App: Direct SQL queries, no parameterization
- Email Gateway: No SPF/DMARC enforcement
- Monitoring: No real-time alerting, 8-hour detection gap
- Authentication: No MFA implementation

Improved Security Architecture

Proposed defense-in-depth architecture addresses identified weaknesses:

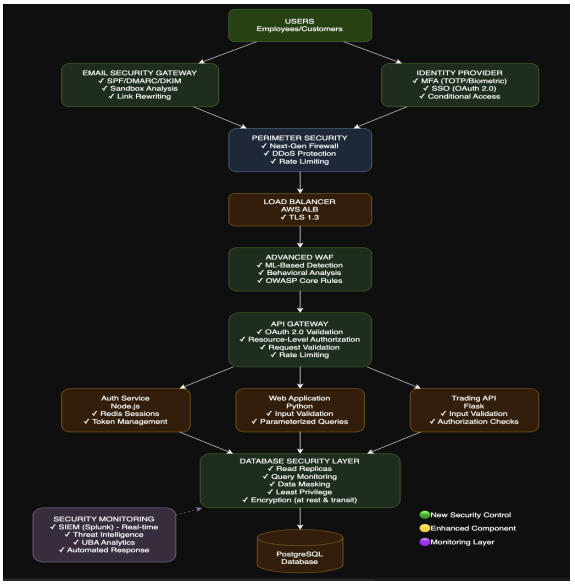


Figure 10: Improved security architecture implementing defense-in-depth strategy. Green components represent new security controls addressing identified vulnerabilities. Key enhancements include email security gateway (anti-phishing), MFA enforcement, ML-based WAF, resource-level API authorization, and real-time SIEM monitoring.

RESPONSE AND REMEDIATION

Attack Timeline

New Search

Save As | Create Table View | Close

```
index=acme_logs
| eval stage=case(
    source="api_logs.csv" AND response_code=401, "1-Recon",
    source="api_logs.csv" AND response_code=200 AND match(endpoint, "portfolio"), "2-API Enumeration",
    source="web_logs.csv" AND user_id="admin_5678", "3-Admin Export",
    source="email_logs.csv" AND link_clicked="yes", "4-Phishing",
    source="waf_logs.csv" AND match(signature, "SQL"), "5-SQL Injection",
    1=1, "Other"
)
| search stage!="Other"
| eval attacker_ip=coalesce(ip_address, source_ip)
| table _time, stage, attacker_ip, endpoint, signature, response_code
| sort _time
```

Time range: All time

✓ 39 events (before 11/9/25 3:20:51.000 PM) | No Event Sampling | Job | Smart Mode

Events | Patterns | Statistics (39) | Visualization

Show: 100 Per Page | Format | Preview: On

_time	stage	attacker_ip	endpoint	signature	response_code
2024-10-15 01:30:15.000	1-Recon	192.168.1.100	/api/v1/portfolio/1000		401
2024-10-15 01:30:16.000	1-Recon	192.168.1.100	/api/v1/portfolio/1001		401
2024-10-15 01:30:17.000	1-Recon	192.168.1.100	/api/v1/portfolio/1002		401
2024-10-15 01:30:18.000	1-Recon	192.168.1.100	/api/v1/portfolio/1003		401
2024-10-15 01:30:19.000	1-Recon	192.168.1.100	/api/v1/portfolio/1004		401
2024-10-15 01:45:10.000	2-API Enumeration	10.0.0.50	/api/v1/portfolio/5001		200
2024-10-15 01:45:15.000	2-API Enumeration	10.0.0.50	/api/v1/portfolio/5002		200
2024-10-15 01:45:20.000	2-API Enumeration	10.0.0.50	/api/v1/portfolio/5003		200
2024-10-15 01:45:25.000	2-API Enumeration	10.0.0.50	/api/v1/portfolio/5004		200
2024-10-15 01:45:30.000	2-API Enumeration	10.0.0.50	/api/v1/portfolio/5005		200
2024-10-15 04:16:15.000	2-API Enumeration	98.213.45.122	/api/v1/portfolio/2347		200
2024-10-15 05:31:30.000	2-API Enumeration	172.89.15.67	/api/v1/portfolio/3891		200
2024-10-15 06:46:30.000	2-API Enumeration	203.0.113.45	/api/v1/portfolio/1523		200
2024-10-15 06:47:15.000	2-API Enumeration	203.0.113.45	/api/v1/portfolio/1524		200

Figure 11: Chronological attack timeline showing: reconnaissance (01:30), test enumeration (01:45), random probes (04:16-08:21), attacker's targeted enumeration (06:46-06:47, 16 accounts), admin export (08:55, 245KB), phishing (09:00, 3 victims), SQL injection (09:20-09:23, 1 bypass). Primary threat actor: 203.0.113.45.

Immediate Actions (0-24h)

- Revoke compromised credentials (user1, user3, user5) + force password reset with MFA
- Block attacker IP 203.0.113.45, isolate accounts 1523-1538
- Deploy emergency WAF rules, investigate admin_5678 activity
- Audit pentest infrastructure security - verify test credentials not stolen
- Review all access to test IP range 203.0.113.0/24

Short-Term (1-2 weeks)

- Implement API authorization middleware, parameterized queries
- Configure SPF/DMARC/DKIM email security
- Enable real-time SIEM alerts, phishing awareness training

Long-Term (1-3 months)

- ML-based WAF, zero-trust architecture, database security layer - Threat intelligence integration, automated response - Quarterly pentesting, SOC 2 compliance preparation

MITRE ATT&CK Mapping

T1566.002 (Phishing), T1078 (Valid Accounts), T1190 (Exploit Public-Facing App), T1087 (Account Discovery), T1530 (Data Exfiltration)

Compliance: Incident requires disclosure under breach notification laws (GDPR, PCI-DSS).