**Fidelity Personas**

**Persona 1: Application Security Analyst**

Goals:

* Ensure software and apps developed internally are secure by design.
* Reduce the risk of exploitable vulnerabilities in financial products.
* Improve secure development lifecycle practices (e.g., shift-left security).

Primary Responsibilities:

* Perform code reviews and security testing (SAST/DAST).
* Work closely with DevOps/Engineering to integrate security tools into CI/CD pipelines.
* Define and maintain secure coding standards.
* Evaluate third-party libraries and APIs for security risks.

Tools & Technologies:

* Tools: Checkmarx, Veracode, GitHub Advanced Security, SonarQube, OWASP ZAP
* Languages: Python, Java, JavaScript (for reviewing code)
* Frameworks: OWASP Top 10, NIST Secure SDLC

Influences/Key Collaborators:

* Software engineers
* DevOps teams
* Product managers
* Internal auditors or compliance

Communication Style:

* Prefers structured updates in Jira or Confluence
* Wants to be looped in early for new features/releases
* Appreciates evidence-based, risk-prioritized discussions

What Success Looks Like:

* Zero critical vulnerabilities in production code
* Reduced time to patch vulnerabilities
* Strong developer adoption of secure coding best practices

**Persona 2: Threat Intelligence Analyst**

Goals:

* Stay ahead of emerging cyber threats that could impact financial data, infrastructure, or brand.
* Translate external threat intel into actionable insights.
* Build and maintain comprehensive threat models and attack surface assessments.

Primary Responsibilities:

* Monitor threat intel feeds, dark web chatter, and APT activity.
* Collaborate with incident response, SOC, and security engineering.
* Correlate threat activity to internal vulnerabilities or exposures.
* Support tabletop exercises, red team/blue team ops, and security awareness.

Tools & Technologies:

* Tools: MISP, ThreatConnect, Recorded Future, MITRE ATT&CK, Splunk, Elastic
* Feeds: FS-ISAC, CISA Alerts, commercial intel providers
* Frameworks: MITRE, Kill Chain Model, STIX/TAXII

Influences/Key Collaborators:

* Security operations center (SOC)
* Risk management teams
* Legal & compliance (esp. during threat disclosures or breaches)
* Cloud & infrastructure security

Communication Style:

* Clear, concise briefs or dashboards
* Appreciates priority flags (e.g., “urgent + relevant to financial services”)
* Comfortable presenting threat models to exec leadership or board

What Success Looks Like:

* Early detection of targeted threats
* Improved threat-to-risk mapping across assets
* Timely and actionable alerts that prevent or mitigate incidents

**Persona 3: DLP / Insider Threat Analyst**

Goals:

* Detect and prevent unauthorized access, transfer, or misuse of sensitive company or customer data.
* Monitor employee behavior and access patterns to identify potential insider threats.
* Build and enforce data classification and protection policies.

Primary Responsibilities:

* Configure and monitor DLP systems to flag risky activity (e.g., large data transfers, USB use, email exfiltration).
* Correlate user behavior with potential insider threat indicators (UBEA/UEBA).
* Work closely with HR and Legal on sensitive investigations.
* Develop policies around data handling, privileged access, and shadow IT.

Tools & Technologies:

* Tools: Microsoft Purview DLP, Symantec DLP, Proofpoint Insider Threat, Varonis, Splunk, Forcepoint
* Integrations: Identity & Access Management (IAM), CASB, SIEM
* Methods: UEBA (User & Entity Behavior Analytics), data fingerprinting

Influences/Key Collaborators:

* HR & Legal (especially for investigations)
* IT Admins & Identity teams
* Compliance (e.g., FINRA, GLBA)
* Endpoint management/security

Communication Style:

* Highly discreet and confidential
* Prefers secure channels and formal documentation trails
* Investigative mindset — values context-rich data and pattern logs

What Success Looks Like:

* No major data exfiltration events
* Accurate early detection of insider risk behaviors
* Strong collaboration with HR/legal on risk mitigation and escalation

**Persona 4: Malware Analyst**

Goals:

* Analyze, reverse engineer, and understand malware affecting financial systems.
* Stay ahead of malware campaigns targeting banking, payment, and trading platforms.
* Build signatures and indicators of compromise (IOCs) for threat detection tools.

Primary Responsibilities:

* Reverse engineer malware using static/dynamic analysis techniques.
* Create YARA rules and custom detections for advanced malware variants.
* Work with SOC to identify malware infections and response plans.
* Track trends in malware targeting financial institutions (banking trojans, ransomware, etc.).

Tools & Technologies:

* Tools: IDA Pro, Ghidra, Wireshark, Cuckoo Sandbox, YARA, PEStudio
* Threat Intel: VirusTotal, Any.Run, Hybrid Analysis
* Languages: Assembly, Python, C/C++

Influences/Key Collaborators:

* Incident Response (IR) team
* Threat Intelligence
* Endpoint Detection & Response (EDR) teams
* Security Operations Center (SOC)

Communication Style:

* Detailed technical reports with IOCs, hashes, and TTPs
* Comfortable briefing security teams or sharing de-obfuscation guides
* Less concerned with flashy presentations — more focused on accuracy and clarity

What Success Looks Like:

* Fast turnaround time on malware dissection
* Early identification of malware campaigns targeting the org
* EDR systems proactively blocking malware variants based on internal signatures

**Role Based Summary**

|  |  |  |
| --- | --- | --- |
| **Analyst Role** | **What to Look for in Articles/Publications** | **Key Keywords** |
| **Application Security Analyst** | Emerging secure coding practices, vulnerability trends in development frameworks, and real-world exploit examples. | OWASP Top 10, zero-day, buffer overflow, code injection, secure coding, SSRF, CI/CD, SAST, DAST |
| **Threat Intelligence Analyst** | Evolving threat actor TTPs, especially those targeting financial systems, to enhance threat modeling and early detection. | APT, TTPs, MITRE ATT&CK, initial access, supply chain attack, lateral movement, C2, FS-ISAC, FIN groups |
| **DLP / Insider Threat Analyst** | Trends in insider data misuse, policy failures, and behavioral indicators that inform monitoring and prevention. | data exfiltration, insider threat, UEBA, privilege misuse, shadow IT, file transfer, USB, DLP policy |
| **Malware Analyst** | Technical breakdowns of new malware strains, obfuscation techniques, payload behavior, and IOCs. | ransomware, trojan, payload, YARA, reverse engineering, IOC, obfuscation, command and control, Ghidra |