Defending the Digital Core

Observability Aligned to the NIST Cybersecurity Framework

Steven Payne, CISSP
Senior Solutions Advisor, Rocket Software

STRATEGIC CONTEXT

- Why the mainframe is the enterprise's highest-value — and highest-risk — asset.

Mainframes as the Enterprise Digital Core

SHARE
EDUCATE • NETWORK • INFLUENCE

Critical Enterprise Backbone

Processes billions of daily transactions across banking, insurance, retail and government — the system of record the business runs on.

Hybrid Connectivity

Deeply integrated with cloud, distributed apps and APIs — extending its reach, and its attack surface, across the enterprise.

High-Value Data

Holds the most sensitive customer, financial and regulatory data, making it both a prime target and a compliance focal point.

Observability Foundation

Rich native telemetry — SMF, RACF, SYSLOG — provides the raw signal needed to build real security visibility.

Why Mainframes Still Matter to Business Risk

Concentrated Business Risk

A single platform underpins core revenue and customer operations, so an outage or breach here carries outsized financial and reputational impact.

Visibility Gaps

Traditional tooling treats the mainframe as a black box, leaving security teams with limited insight into who did what, and why.

Compliance & Governance

PCI DSS, SOX, GDPR and DORA demand demonstrable control and auditability over the systems that hold regulated data.

Skills & Silos

Retiring mainframe expertise and disconnected teams widen the gap between platform operations and enterprise security.

OBSERVABILITY & NIST CSF

- How a globally adopted security framework gives mainframe observability a common language.

Observability Within the NIST CSF

GV

Govern

Establish risk strategy, roles and policy that steer the security program.

ID

Identify

Inventory assets, data flows and risks across the mainframe estate.

PR

Protect

Enforce access control, hardening and safeguards on critical workloads.

DE

Detect

Surface anomalies and security events through continuous telemetry.

RS

Respond

Investigate, contain and coordinate action when incidents occur.

RC

Recover

Restore services and validate integrity to resume trusted operations.

How Observability Enables CSF Outcomes

Asset Visibility

Identify — continuous inventory of systems, users and data flows reveals exactly what must be defended.

Control Validation

Protect — telemetry proves access controls and hardening are actually enforced, not merely configured.

Anomaly Detection

Detect — behavioral baselines surface deviations that signature-based tools routinely miss.

Response & Recovery

Respond & Recover — rich forensic context speeds containment and confirms a clean, trusted restoration.

Applying CSF Principles to the Mainframe

SHARE
EDUCATE • NETWORK • INFLUENCE

Stream Native Telemetry

Forward SMF, RACF, SYSLOG, and performance records into the enterprise observability pipeline in real time.

Normalize & Correlate

Map mainframe events to the same schema as distributed logs so the estate analyzes as one.

Extend Enterprise Controls

Apply identity, access and change policy to z/OS with the same rigor as any other platform.

Feed the SOC

Deliver mainframe signals into SIEM and SOC workflows for unified detection and response.

Mapping Observability to NIST Controls

Where mainframe telemetry strengthens the controls auditors and regulators expect.

- **Observability as a cybersecurity control enabler**
- **Continuous validation across risk, access and recovery**

Observability as a Control Enabler

RA

Risk Management

Continuous signal quantifies exposure so risk decisions reflect current reality, not annual snapshots.

AM

Asset Management

Live inventory of systems, jobs and data flows keeps the mainframe estate fully accounted for.

AC

Access Control

RACF and identity telemetry verify least-privilege is enforced and privileged use is watched.

AU

Audit & Accountability

Immutable event trails give auditors provable evidence of who did what, and when.

IR

Incident Response

Correlated forensics shorten investigation and containment when an incident is declared.

CP

Recovery & Continuity

Integrity and workload telemetry confirm systems are restored to a known-good, trusted state.

THREATS & MONITORING LIMITATIONS

Why adversaries succeed against the mainframe, and where legacy monitoring falls short.

The Modern Threat Landscape

SHARE
EDUCATE • NETWORK • INFLUENCE

Advanced Persistent Threats

Well-resourced adversaries move laterally and dwell for months, targeting the systems of record where crown-jewel data lives.

Insider & Privilege Abuse

Legitimate credentials, misused by insiders or attackers, bypass perimeter defenses and blend in with normal activity.

Hybrid Complexity

Cloud, distributed and mainframe estates blur boundaries and multiply the paths an attacker can take.

Credential & Supply-Chain Theft

Stolen keys, tokens and trusted third-party access give attackers a legitimate-looking route inward.

Challenges with Traditional Monitoring

SHARE
EDUCATE • NETWORK • INFLUENCE

Reactive by Design

Threshold alerts fire after impact — they tell you something broke, but rarely why or how.

Siloed Tooling

Mainframe monitors and enterprise SIEM seldom share a view, so related signals stay fragmented.

Limited Context

Metrics without traces or identity cannot explain intent or reconstruct a full sequence of events.

Known-Failure Bias

Monitoring watches for expected failures and misses the novel, unknown-unknown attack.

OBSERVABILITY IN ACTION

- From concept to a working detection pipeline on the mainframe.

Defining Observability for Security

SHARE
EDUCATE • NETWORK • INFLUENCE

Metrics

Numeric time-series such as CPU, throughput and error rates that quantify system state and expose trend shifts.

Logs

Timestamped records of discrete events: RACF decisions, job activity, SYSLOG and application messages.

Traces

End-to-end request paths showing how a transaction moved across systems and exactly where it deviated.

Events

Security-significant signals — logons, privilege changes, configuration edits — normalized for correlation.

Monitoring Versus Observability

SHARE
EDUCATE • NETWORK • INFLUENCE

Monitoring: Known Failures

Watches predefined metrics and thresholds — it tells you when a known thing breaks.

Observability: Unknown Risks

Explores open-ended questions about behavior and surfaces threats no one thought to predefine.

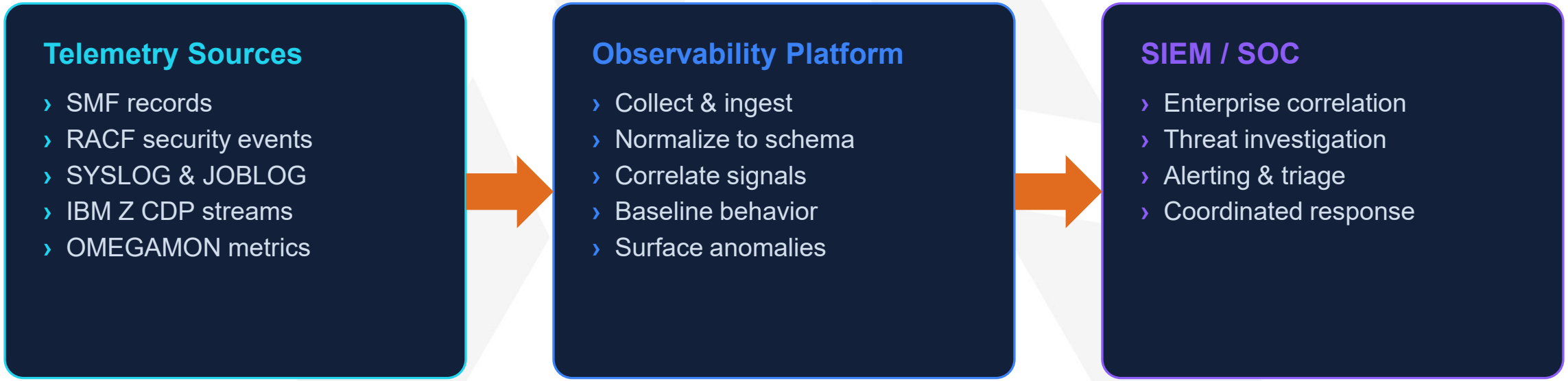
Dashboards & Alerts

Answers “is it up?” with red/green signals and fixed, static thresholds.

Investigation & Context

Answers “what happened, and why?” by correlating metrics, logs, traces and events.

Mainframe Observability Architecture



Native mainframe telemetry flows left to right — collected and normalized in the observability platform, then correlated in the SIEM/SOC for detection and response.

Use Case: Privilege Escalation Detection

SHARE
EDUCATE • NETWORK • INFLUENCE

Baseline Normal

Establish who normally holds privileged access and how they typically use it.

Spot the Anomaly

Flag a user or job suddenly acquiring elevated RACF authority outside their pattern.

Correlate Signals

Tie the privilege change to logon source, time of day and concurrent activity.

Alert & Contain

Raise a high-fidelity SOC alert and revoke or quarantine before misuse spreads.

Use Case: Suspicious Workload Activity

SHARE
EDUCATE • NETWORK • INFLUENCE

Behavioral Baseline

Learn normal CPU, transaction and job profiles for each mainframe workload.

Detect the Shift

Catch an unexpected batch job, off-hours spike or unfamiliar transaction mix.

Add Context

Correlate the shift with identity, dataset access and network signals.

Investigate Fast

Hand the SOC a scoped, evidence-rich lead instead of a raw threshold alarm.

SIEM and SOC Integration

Unified Visibility

Mainframe events sit beside cloud and distributed logs in a single pane of glass.

Cross-Domain Correlation

Link a z/OS privilege change to a suspicious endpoint, identity or network event.

Faster Investigations

Analysts pivot across the full estate without switching tools, teams or context.

Consistent Response

One playbook and workflow covers the mainframe just like any other platform.

Operational and Security Benefits

SHARE
EDUCATE • NETWORK • INFLUENCE

Reduced MTTI

Rich context shortens **mean time to identify** an incident from hours to minutes.

Stronger Risk Posture

Continuous validation closes the blind spots attackers rely on to stay hidden.

Lower Operational Cost

Fewer false alarms and less swivel-chair work across previously siloed tools.

Audit-Ready Evidence

Immutable trails make compliance reporting a by-product, not a quarterly project.

Compliance, Recovery & Key Takeaways

SHARE
EDUCATE • NETWORK • INFLUENCE

Continuous Compliance

Always-on evidence for PCI DSS, SOX, GDPR and DORA — auditability as a by-product, not a project.

Resilient Recovery

Integrity and workload telemetry confirm a clean, trusted restoration after any incident.

Observability = Control

Visibility is the mechanism that makes every NIST CSF function measurable and real.

Defend the Core

Treat the mainframe as a first-class citizen of enterprise security, not an exception.

IBM AND ROCKET SOFTWARE TECHNOLOGY ENABLEMENT

- How IBM Z Common Data Provider and OMEGAMON Data Provider turn native telemetry into detection.

IBM Z Common Data Provider

Streams the Right Data

Forwards RACF, SMF, SYSLOG, JOBLOG and application logs in near real time.

Open Formats

Delivers to Splunk, Elastic, Kafka and other platforms in standard, ready-to-parse schemas.

Low Overhead

Efficient collection that scales across the estate without burdening z/OS.

Security-Ready Feed

Supplies the raw signal SIEM and analytics need to finally see the mainframe.

Detecting Threats with IBM Z Common Data Provider

Privilege Abuse

RACF events reveal unexpected authority changes and repeated failed access attempts.

Insider Threats

Unusual dataset access and command patterns stand out against a learned baseline.

Data Exfiltration

Large or off-hours reads of sensitive datasets and transfers surface as anomalies.

Behavioral Analytics

Mainframe events feed UEBA (User and Entity Behavior Analytics) to score user and entity risk across the estate.

OMEGAMON Data Provider and Security Detection

Operational Telemetry

Streams high-frequency performance metrics from z/OS, CICS, Db2 and IMS.

Security Context

Operational anomalies are frequently the first observable sign of a security event.

Continuous Signal

Metrics arrive between log events, giving earlier warning than logs alone.

SIEM Enrichment

Adds the 'how the system behaved' layer to event-based detection.

Operational Anomalies as Security Indicators

CPU Spikes

Sudden compute surges can signal crypto-mining, brute-force attempts or runaway malicious jobs.

Workload Shifts

Unexpected transaction mixes or batch patterns may indicate misuse or a compromised process.

After-Hours Activity

Jobs and logons outside normal operating windows warrant immediate scrutiny.

Resource Contention

Abnormal I/O or storage patterns can expose data being staged for exfiltration.

SIEM Integration Value

CDP + OMEGAMON

Security events plus operational metrics provide the complete picture of the mainframe.

Enterprise Correlation

Combine mainframe signal with the rest of the estate inside the SIEM.

Faster Response

Correlated context turns raw alerts into decisive, coordinated action.

Provable Coverage

Show the mainframe is monitored to the same standard as everything else.

Your feedback is important!

SHARE
EDUCATE • NETWORK • INFLUENCE

Submit a session evaluation for each session you attend:

www.share.org/evaluation