Securing Hyperledger Fabric

Monitoring and analyzing
blockchain deployments using Splunk

Christopher Cordi

splunk> turn data into doing™

Chris Cordi

Software Engineer

Splunk Blockchain Team

Why Splunk Blockchain?

Blockchain solutions hold a lot of promise but add new and difficult infrastructure, application and security requirements.

- Hard to gain **end to end visibility** between all components
- Many options to choose for infrastructure including **on-prem, cloud, hybrid, unmanaged, managed and multi-organization**.
- **Diverse set of data sources** both with differing formats and velocities.
- Different blockchain technologies and platforms
- **Interoperability** and collaboration between consortiums
- **Disparate tools** for logging, metrics, tracing, transaction analytics and security.
- **Different tools (if any)** for load testing and development performance vs production monitoring and investigation.

Hyperledger Fabric Overview

Hyperledger Fabric is designed to enable secure collaboration between multiple organizations operating with limited trust.

Despite the security improvements Hyperledger Fabric provides, deployments still require careful configuration and monitoring to ensure that they are operating securely.

We're going to review different types of threats that Hyperledger Fabric operators should consider and discuss how to mitigate them.

Assets to Protect

- Data
  - IP or otherwise sensitive data
- Hardware
- Software/Applications

Threats to Hyperledger Fabric Networks

As a permissioned blockchain, Hyperledger Fabric's network threats can differ from popular permissionless chains.

Some attacks are common to all distributed systems like Denial of Service (DoS) or consensus manipulation.

Other attacks target specific components in a Hyperledger Fabric network, such as the Membership Service Provider (MSP).

Threats: Denial of Service (DoS)

Denial of Service attacks disrupt the network's availability and are a threat to any distributed system.

Many different attacks can result in denial of service, which makes it difficult to proactively prevent.

Mitigation:

- collecting performance metrics, such as transaction throughput and latency, to detect compromised availability early on

Threats: Consensus Manipulation

Attacks on the network consensus include DoS and transaction reordering attacks.

Mitigation:

- Logging threat indicators, such as leadership elections and transaction latencies, can speed up detection.

Threats: MSP Compromise

The Membership Serice Provider (MSP) is able to modify access control to the network and, if malicious, could deny service and perform Sybil attacks.

The MSP may be compromised by a rogue insider or through private key theft, which may only be detectable after exploitation.

Mitigation:

- Follow Key Management and Access Control best practices
- Logging and alerting MSP actions, such as certificate creation and revocation

Threats: Smart Contract Exploitation

Smart contract exploits can compromise business logic and network performance.

In addition to ordinary programming logic bugs, common errors can also stem from inappropriately handling concurrency or nondeterminism.

Mitigation:

- Design smart contracts with security in mind
- Smart contract analysis tools like the Hyperledger Lab Chaincode Analyzer
- External Security Audits
- Monitor performance and usage of the smart contract to detect anomalous behavior.

Key Data Sources

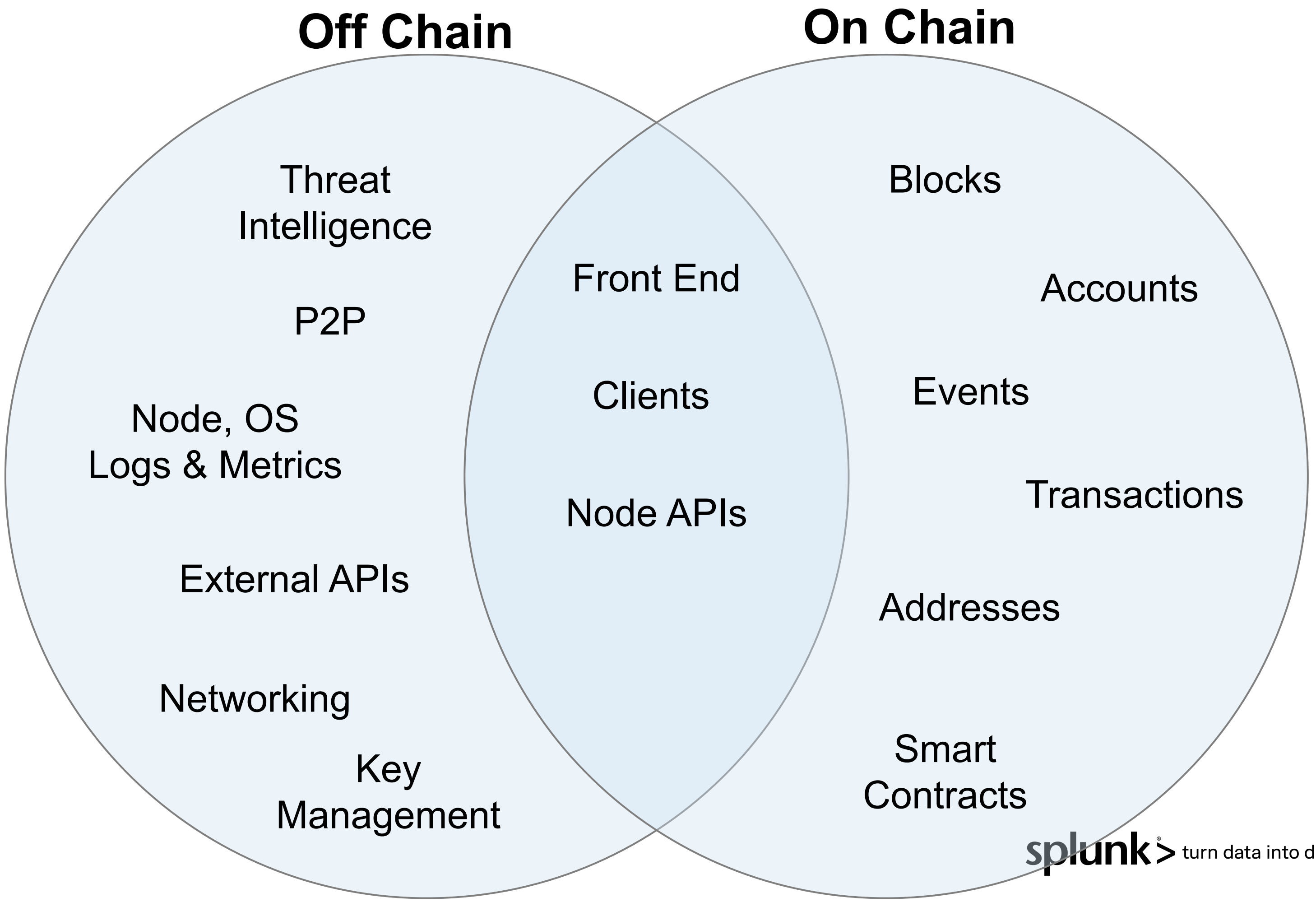
Threat	**Indicators**	**Data Source**
Denial of Service	Tx throughput & latency Block latency # Senders # Open connections	Block headers, Node metrics
Consensus Manipulation	Changes in chain config Leadership Elections	Blocks Node logs
Ledger Manipulation	Orphaned blocks	Block headers
Smart Contract Exploitation	Scanned Vulnerabilities	Vulnerability Scanner

Additional Threats & Data Sources

Effective Monitoring Requires Both On Chain & Off Chain Data

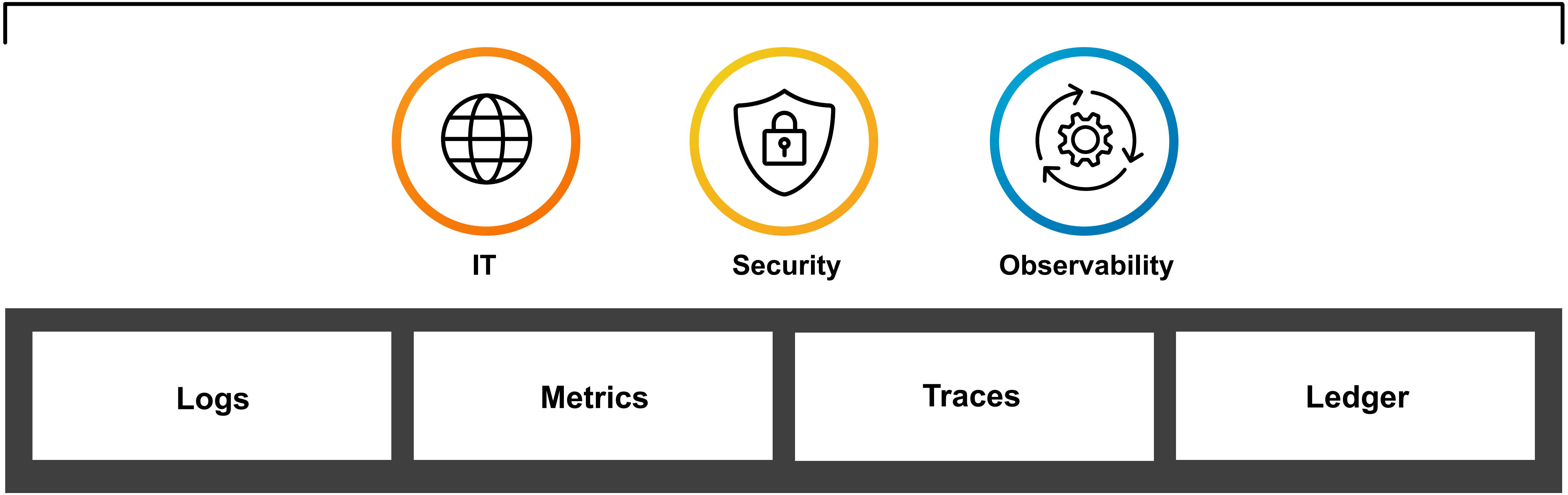
Threats

- Front End / Application Vulnerability
- Key Theft
- Smart Contract Vulnerability
- Denial of Service
- Network Partitioning
- Malicious Consensus Behavior



splunk> turn data into doing™

Data-to-Everything Platform



IT

Security

Observability

Logs

Metrics

Traces

Ledger

Splunk App for Hyperledger Fabric

Gain full observability around Hyperledger Fabric environments

INFRASTRUCTURE HEALTH & MONITORING | ANALYZE LEDGER DATA | ACT ON CHAINCODE EVENTS

Gain observability into the Consortium

Unify monitoring, troubleshooting, investigation, and take action on Hyperledger Fabric components across organizations and multi-cloud environments.

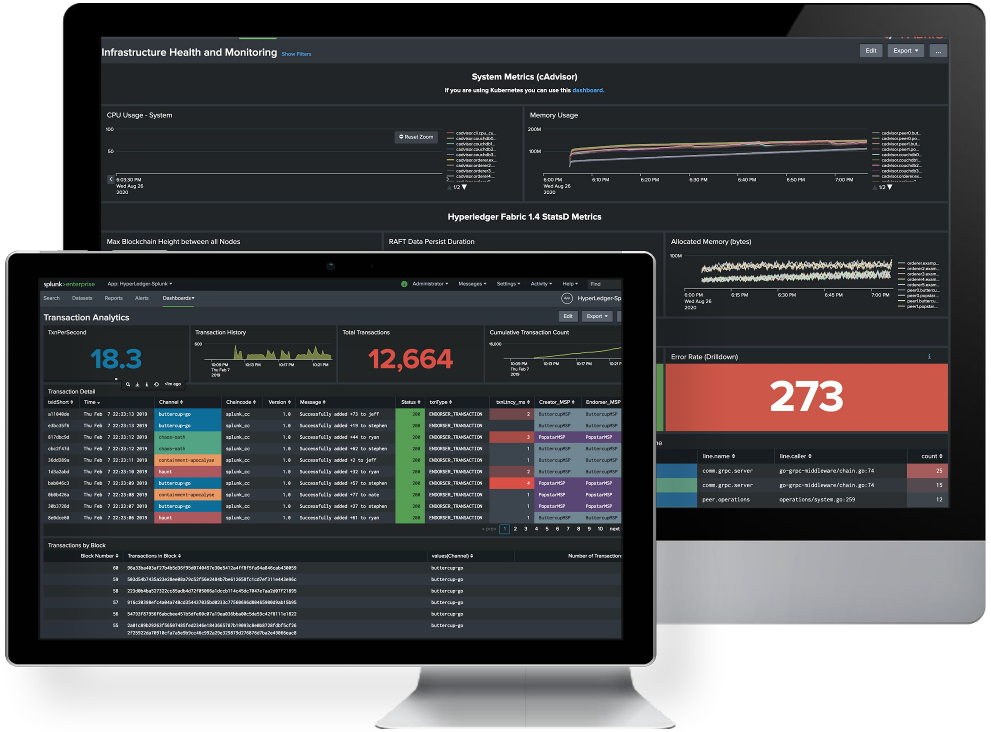
Reduce MTTR by combining logs, metrics and traces

Remove data silos and the need for multiple tools when troubleshooting and optimizing the network.

Get to production faster and securely

Understand the performance of your development and monitor configuration changes.

https://splunkbase.splunk.com/app/4605



Infrastructure Health and Monitoring Show Filters

System Metrics (cAdvisor)

If you are using Kubernetes you can use this dashboard.

Hyperledger Fabric 1.4 StatsD Metrics

Max Blockchain Height between all Nodes

RAFT Data Persist Duration

Error Rate (Drilldown)

273

line.name	line.caller	count
comm.grpc.server	go-grpc-middleware/chain.go:74	25
comm.grpc.server	go-grpc-middleware/chain.go:74	15
peer.operations	operations/system.go:259	12

Transaction Analytics

TxnPerSecond

18.3

Total Transactions

12,664

Transaction Detail

txidShort	Time	Channel	Chaincode	Version	Message	Status	txnType	txnLtncy_ms	Creator_MSP	Endorser_MSP
a11040de	Thu Feb 7 22:23:13 2019	buttercup-go	splunk_cc	1.0	Successfully added +73 to jeff	200	ENDORSER_TRANSACTION	2	ButtercupMSP	ButtercupMSP
e3bc35f6	Thu Feb 7 22:23:13 2019	buttercup-go	splunk_cc	1.0	Successfully added +19 to stephen	200	ENDORSER_TRANSACTION		ButtercupMSP	ButtercupMSP
817dbc9d	Thu Feb 7 22:23:12 2019	chaos-oath	splunk_cc	1.0	Successfully added +44 to ryan	200	ENDORSER_TRANSACTION	3	PopstarMSP	PopstarMSP
cbc2f47d	Thu Feb 7 22:23:12 2019	chaos-oath	splunk_cc	1.0	Successfully added +62 to stephen	200	ENDORSER_TRANSACTION	1	ButtercupMSP	ButtercupMSP
36dd289a	Thu Feb 7 22:23:11 2019	containment-apocalyse	splunk_cc	1.0	Successfully added +2 to jeff	200	ENDORSER_TRANSACTION	1	ButtercupMSP	ButtercupMSP
1d3a2abd	Thu Feb 7 22:23:10 2019	haunt	splunk_cc	1.0	Successfully added +32 to ryan	200	ENDORSER_TRANSACTION	2	ButtercupMSP	ButtercupMSP
bab046c3	Thu Feb 7 22:23:09 2019	buttercup-go	splunk_cc	1.0	Successfully added +57 to stephen	200	ENDORSER_TRANSACTION	4	PopstarMSP	PopstarMSP
0b0b426a	Thu Feb 7 22:23:08 2019	containment-apocalyse	splunk_cc	1.0	Successfully added +77 to nate	200	ENDORSER_TRANSACTION	1	PopstarMSP	PopstarMSP
30b3728d	Thu Feb 7 22:23:07 2019	buttercup-go	splunk_cc	1.0	Successfully added +27 to stephen	200	ENDORSER_TRANSACTION	1	PopstarMSP	PopstarMSP
8e0dce60	Thu Feb 7 22:23:06 2019	haunt	splunk_cc	1.0	Successfully added +61 to ryan	200	ENDORSER_TRANSACTION	1	ButtercupMSP	ButtercupMSP

Transactions by Block

Block Number	Transactions in Block	values(Channel)	Number of Transaction
60	96a33ba403af27b4b5d36f95d0740457e30e5412a4ff8f5fa94a846cab430059	buttercup-go	
59	503d54b7435a23e28ee08a79c52f56e2484b7be612658fc1cd7ef311e443e96c	buttercup-go	
58	223d0b4ba527322cc85adb4d72f05066a1dccb114c45dc7047e7aa2d07f21895	buttercup-go	
57	916c20398efc4a04a748cd354437035bd0233c77560696d80465900d9ab15b95	buttercup-go	
56	54793f87956f6abcbee451b5dfe60c07a19ea036bba00c5de59c42f8111e1822	buttercup-go	
55	2a01c89b29263f56507485fed2346e1843665787b19093c8e0b8728fdbf5cf26 2f25922da70910cfa7a5e9b9cc46c992a29e329879d276876d7ba2e49066eac8	buttercup-go	

splunk> turn data into doing

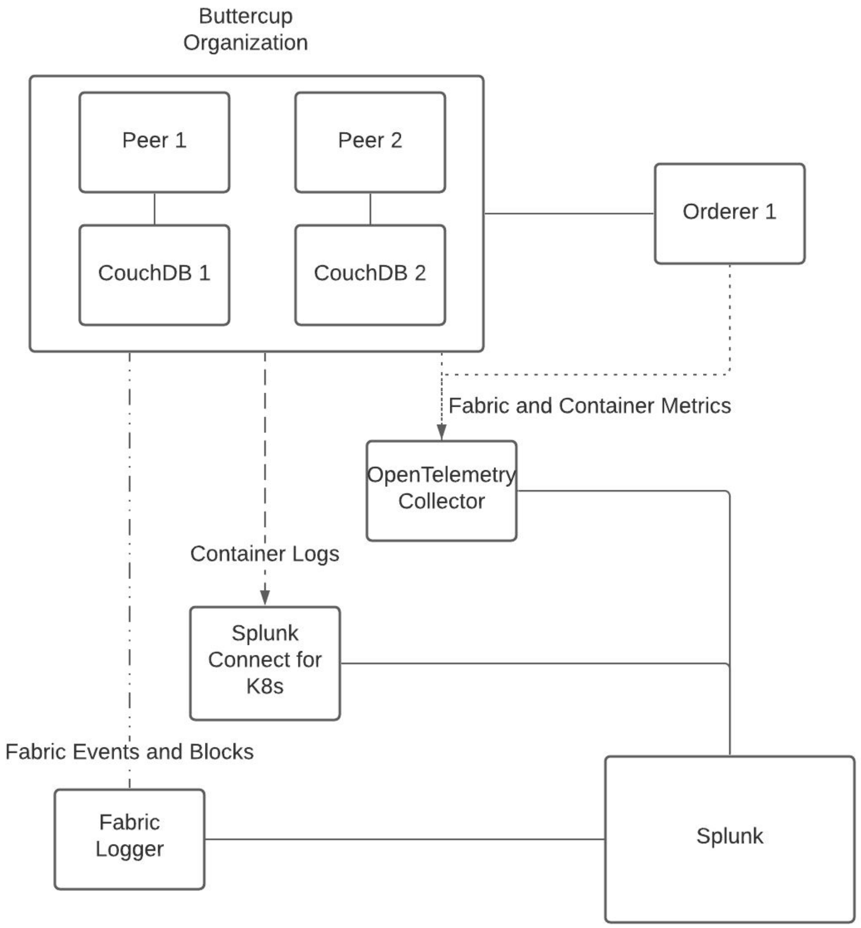
Getting Started with Splunk App for Fabric

We can easily analyze Hyperledger Fabric’s ledger, log, and metric data with the following tools.

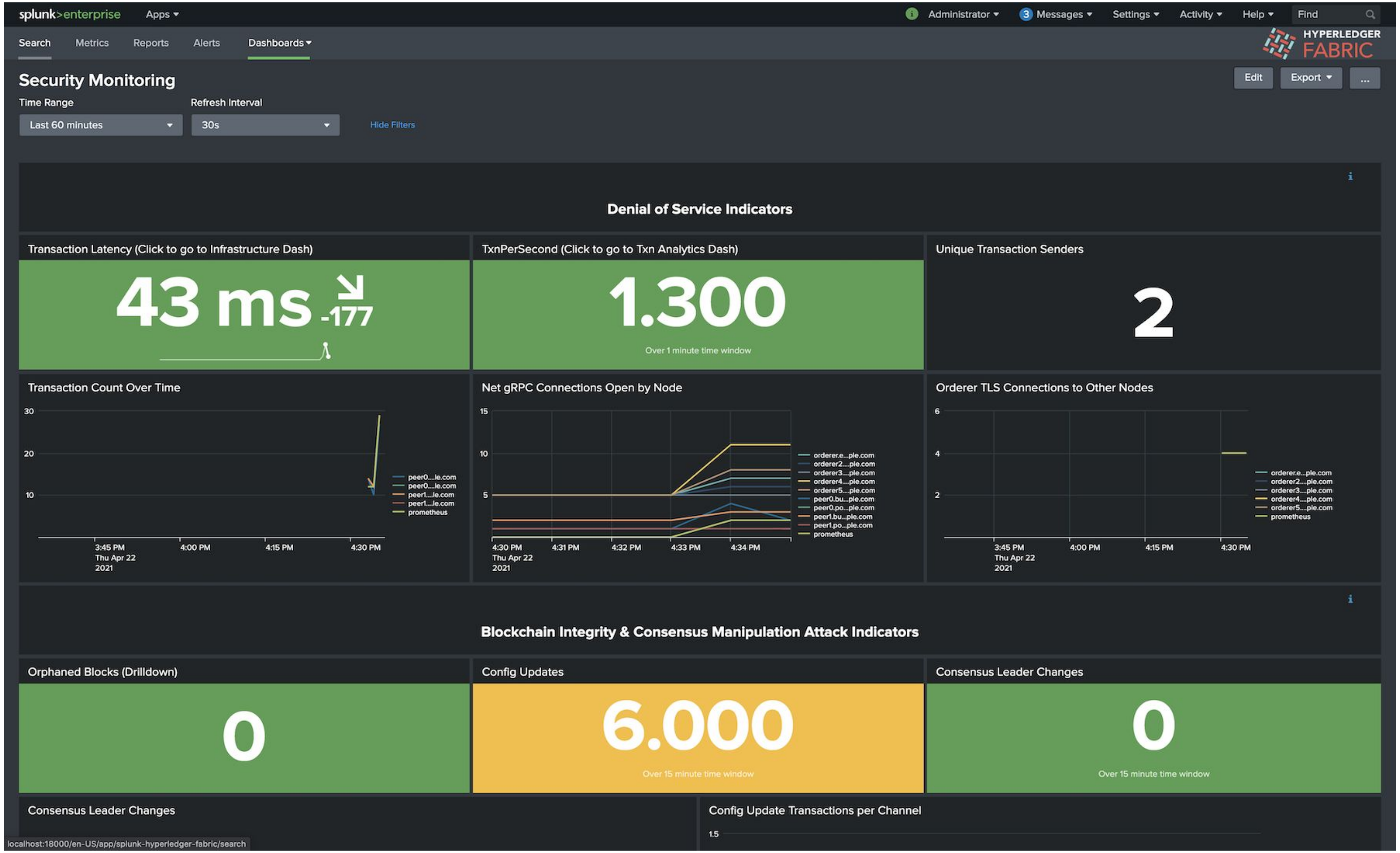
- Splunk Connect for Hyperledger Fabric grabs ledger and metric data from a Hyperledger Fabric deployment.
- The Splunk Docker logging driver or Splunk Connect for Kubernetes can be used to send container logs to Splunk.
- Finally, Splunk App for Hyperledger Fabric visualizes this data in Splunk.

See https://github.com/splunk/fabric-logger for an example docker-compose incorporating these tools.

Getting Data In



Example Security Dashboard



Security Monitoring

Time Range: Last 60 minutes

Refresh Interval: 30s

Denial of Service Indicators

Transaction Latency (Click to go to Infrastructure Dash)

43 ms -177

TxnPerSecond (Click to go to Txn Analytics Dash)

1.300

Over 1 minute time window

Unique Transaction Senders

2

Transaction Count Over Time

Net gRPC Connections Open by Node

Orderer TLS Connections to Other Nodes

Blockchain Integrity & Consensus Manipulation Attack Indicators

Orphaned Blocks (Drilldown)

0

Config Updates

6.000

Over 15 minute time window

Consensus Leader Changes

0

Over 15 minute time window

Consensus Leader Changes

Config Update Transactions per Channel

splunk> turn data into doing™

Detecting DoS Attacks

What would detect during a DoS attack?

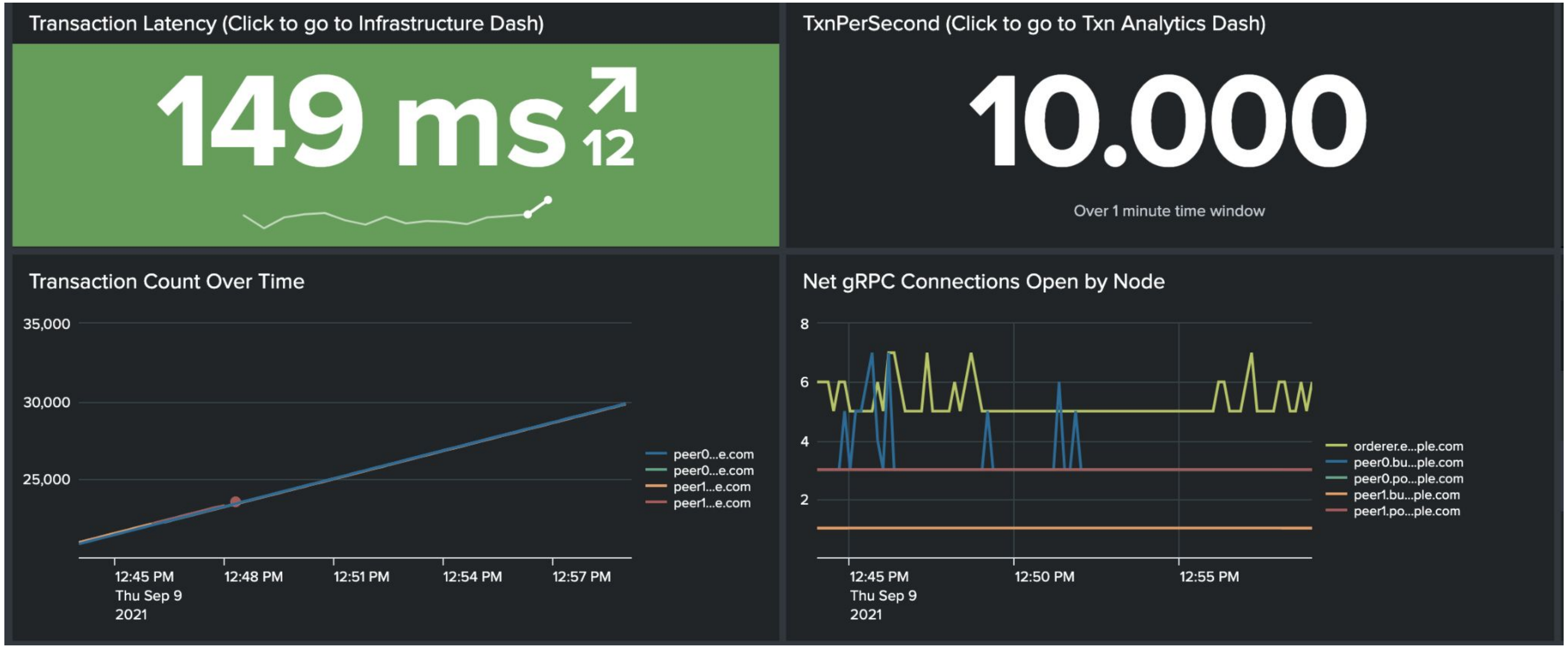
In this scenario, an authorized user has their keys compromised and begins spamming the network with transactions.

We will be paying particular attention to the **transaction latency**, **throughput**, and **number of open connections**.

First, we'll look at the normal case where a single client is sending 10 transactions per second.

Baseline Measurements

Normal case: a single client is sending 10 transactions per second.



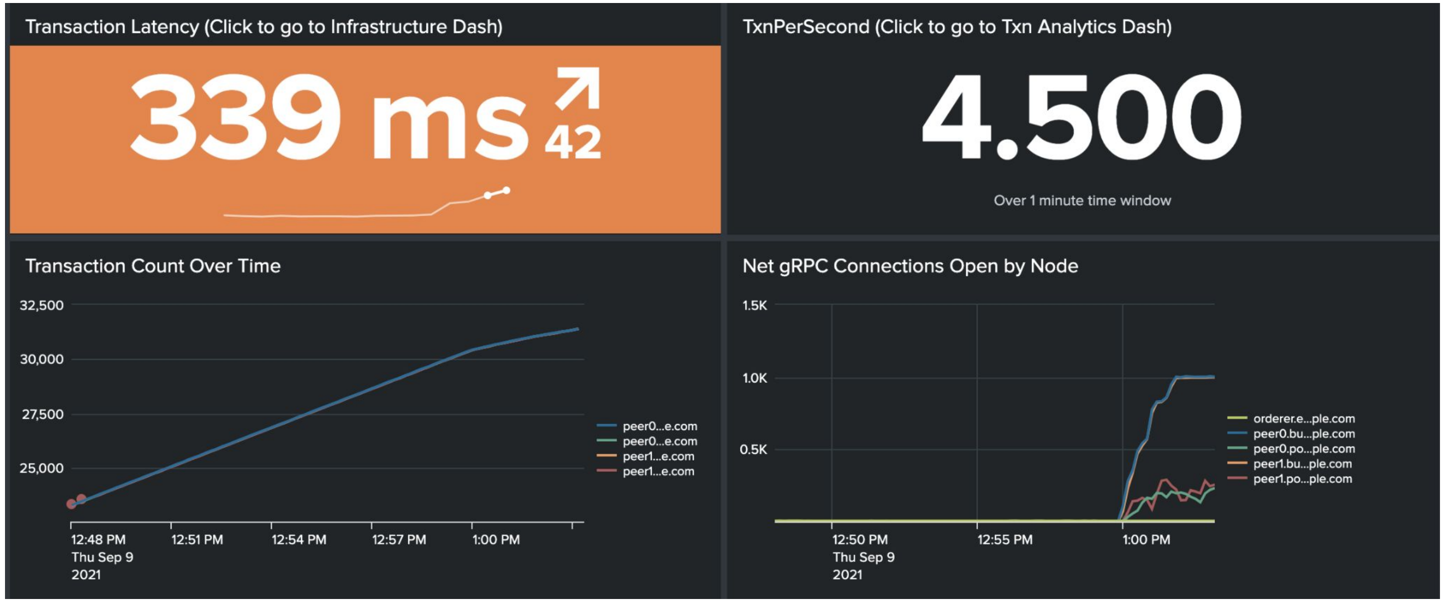
Adversary Scenario

Next, we'll have a single client open up persistent 1000 connections each performing 1 query per minute.

We expect to see:

- ○ transaction latency starts to increase
- ○ transactions per second decreases
- ○ the number of open connections increases.

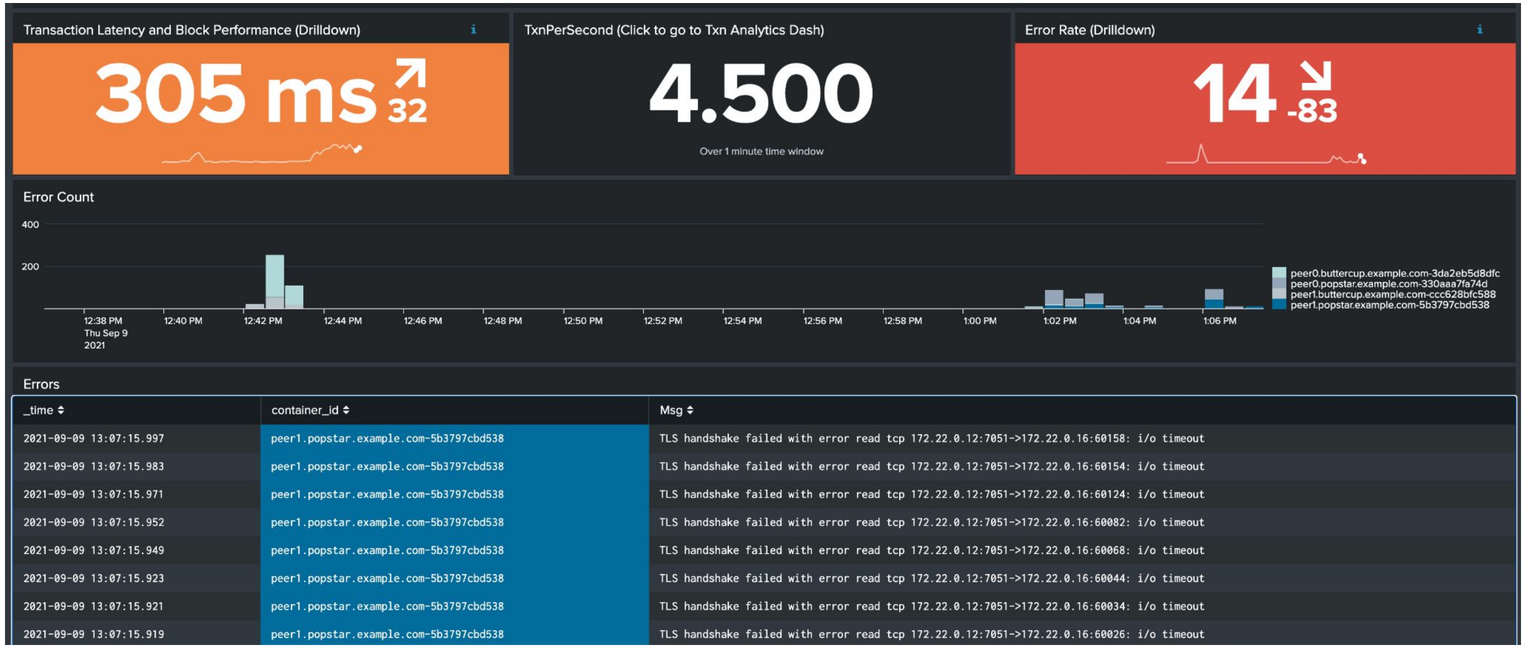
Adversary Scenario Results



At this point, it may be difficult to determine if this is reflective of a high period of load, misconfiguration, or a denial of service attack.

Adversary Scenario Results

Drilling Down on Errors



Transaction Latency and Block Performance (Drilldown)

305 ms ↗ 32

TxnPerSecond (Click to go to Txn Analytics Dash)

4.500

Over 1 minute time window

Error Rate (Drilldown)

14 ↘ -83

Error Count

400
200
12:38 PM
Thu Sep 9
2021
12:40 PM
12:42 PM
12:44 PM
12:46 PM
12:48 PM
12:50 PM
12:52 PM
12:54 PM
12:56 PM
12:58 PM
1:00 PM
1:02 PM
1:04 PM
1:06 PM
peer0.buttercup.example.com-3da2eb5d8dfc
peer0.popstar.example.com-330aaa7fa74d
peer1.buttercup.example.com-ccc628bfc588
peer1.popstar.example.com-5b3797cbd538

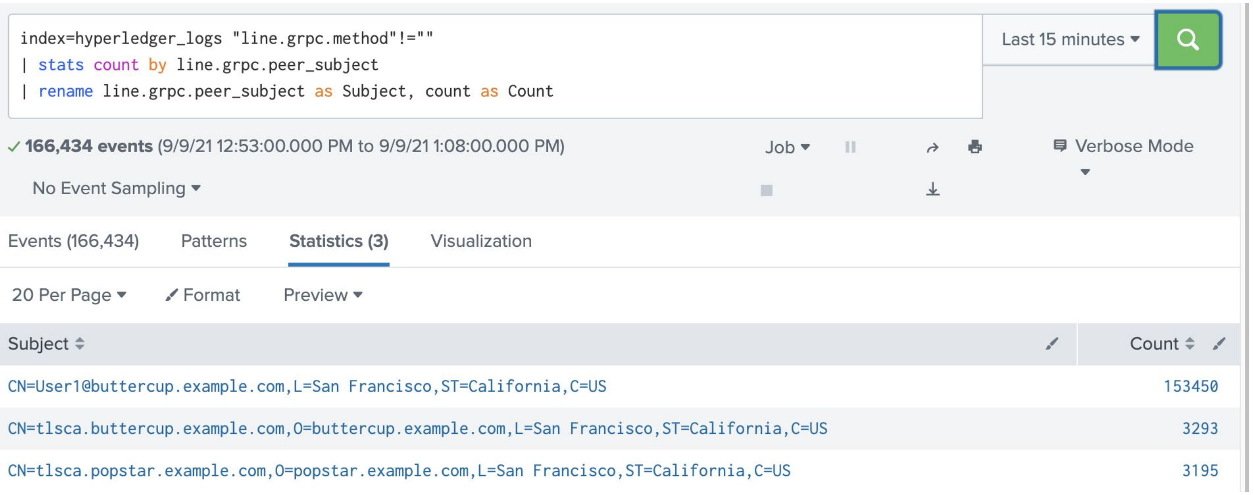
Errors

_time ⬍	container_id ⬍	Msg ⬍
2021-09-09 13:07:15.997	peer1.popstar.example.com-5b3797cbd538	TLS handshake failed with error read tcp 172.22.0.12:7051->172.22.0.16:60158: i/o timeout
2021-09-09 13:07:15.983	peer1.popstar.example.com-5b3797cbd538	TLS handshake failed with error read tcp 172.22.0.12:7051->172.22.0.16:60154: i/o timeout
2021-09-09 13:07:15.971	peer1.popstar.example.com-5b3797cbd538	TLS handshake failed with error read tcp 172.22.0.12:7051->172.22.0.16:60124: i/o timeout
2021-09-09 13:07:15.952	peer1.popstar.example.com-5b3797cbd538	TLS handshake failed with error read tcp 172.22.0.12:7051->172.22.0.16:60082: i/o timeout
2021-09-09 13:07:15.949	peer1.popstar.example.com-5b3797cbd538	TLS handshake failed with error read tcp 172.22.0.12:7051->172.22.0.16:60068: i/o timeout
2021-09-09 13:07:15.923	peer1.popstar.example.com-5b3797cbd538	TLS handshake failed with error read tcp 172.22.0.12:7051->172.22.0.16:60044: i/o timeout
2021-09-09 13:07:15.921	peer1.popstar.example.com-5b3797cbd538	TLS handshake failed with error read tcp 172.22.0.12:7051->172.22.0.16:60034: i/o timeout
2021-09-09 13:07:15.919	peer1.popstar.example.com-5b3797cbd538	TLS handshake failed with error read tcp 172.22.0.12:7051->172.22.0.16:60026: i/o timeout

We can investigate further in the Infrastructure Health and Monitoring Dashboard, where we see connection and I/O timeout errors.

Adversary Scenario Results

Because we noticed a large number of open connections, we should query Splunk to see the distribution of gRPC message subjects and addresses.



```
index=hyperledger_logs "line.grpc.method"!=""
| stats count by line.grpc.peer_subject
| rename line.grpc.peer_subject as Subject, count as Count
```

✓ 166,434 events (9/9/21 12:53:00.000 PM to 9/9/21 1:08:00.000 PM)

Subject	Count
CN=User1@buttercup.example.com,L=San Francisco,ST=California,C=US	153450
CN=tlsca.buttercup.example.com,O=buttercup.example.com,L=San Francisco,ST=California,C=US	3293
CN=tlsca.popstar.example.com,O=popstar.example.com,L=San Francisco,ST=California,C=US	3195

When we perform this search we see a large discrepancy in message count -- indicating that “User1@buttercup.example.com,L=San Francisco,ST=California,C=US” is likely compromised or misconfigured and should be investigated further.

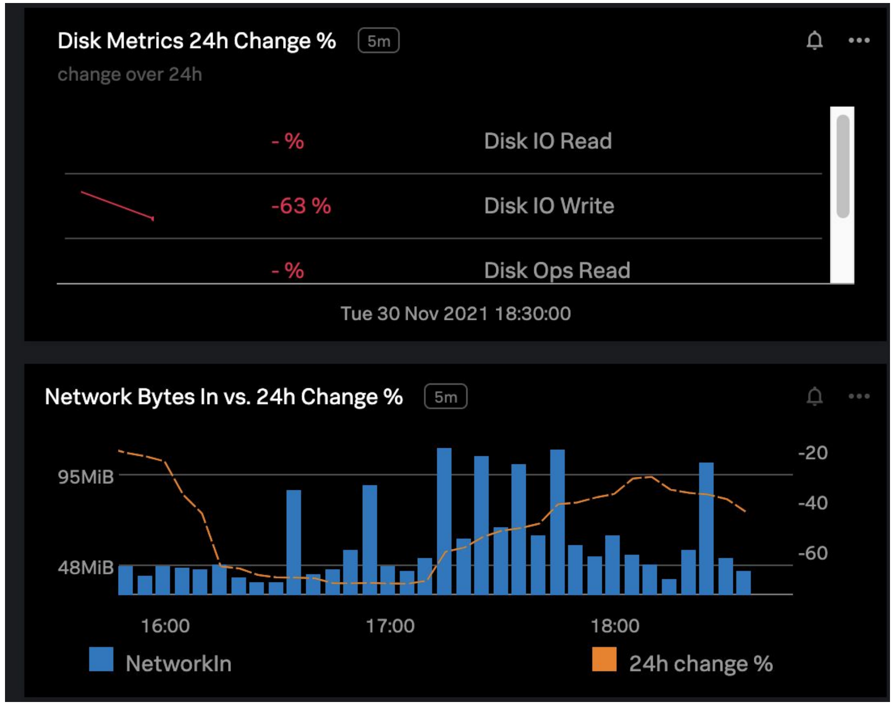
More Integrations

Splunk Application Performance Monitoring (APM)
real-time observability

Splunk On-Call
intelligent outage alerting

Splunk Enterprise Security
enrich and prioritize notables based on risk

Splunk SOAR
automate parts of the incident response process.



Disk Metrics 24h Change % 5m

change over 24h

- %	Disk IO Read
-63 %	Disk IO Write
- %	Disk Ops Read

Tue 30 Nov 2021 18:30:00

Network Bytes In vs. 24h Change % 5m

S&P Case Study

Case Study

Splunk correlates data across all datasets —including Hyperledger Fabric

https://www.hyperledger.org/learn/publications/splunk-sp-case-study

Thank You

splunkdlt.com

splunk> turn data into doing™