GROK

# DO YOU GROK IT?

## USE CASE EXAMPLE

# CASE STUDY

Large Enterprise

01

## THE PROBLEM

Correlation done by static rules

Manual ticketing took too long and increased OPEX and MTTR

Filtered 90% of monitoring signal and were reactive to failures

02

## THE SOLUTION

Integrated with 5 existing monitoring systems

Integrated with SNOW Ticketing

AI Deployed: Clustering, and Classification/Prediction

03

## CUSTOMER TECHNOLOGY

IT / Enterprise Systems (Storage, DB, Cloud)

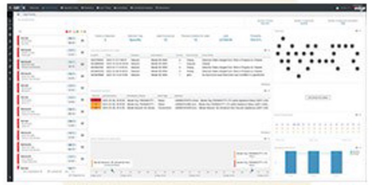
Network LAN/WAN

Security

Applications Health/Monitoring

# HIGH-LEVEL GROK ARCHITECTURE

## ITSM

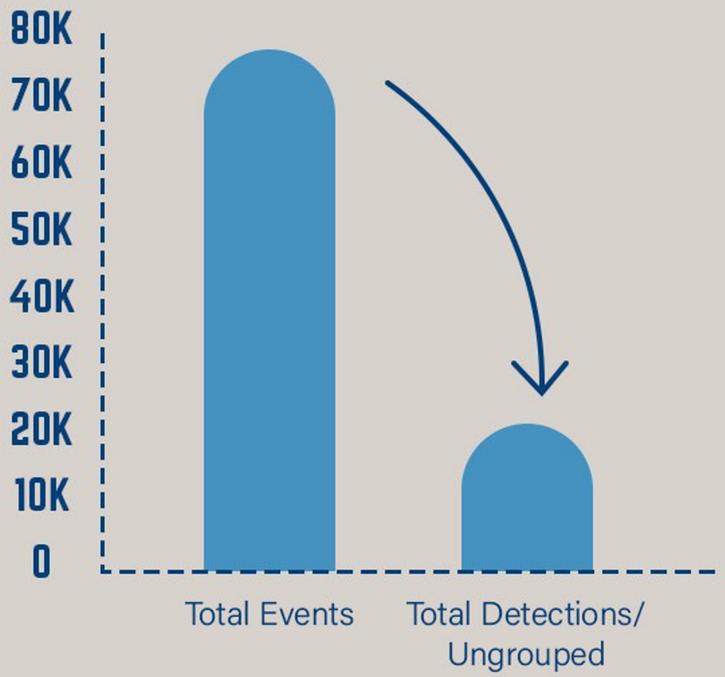


## GROK AIOPS

- LOGICMONITOR
- DYNATRACE
- THOUSAND EYES
- SOLARWINDS
- PINGDOM
- SERVERS
- ROUTERS
- DATABASES
- APPLICATIONS
- STORAGE
- OTHERS

# GROK EVENT COMPRESSION

## 85% EVENT REDUCTION/COMPRESSION




## OPS CENTER BENEFIT ANALYSIS

| | |
|---|---|
| Total Events | 74,694 |
| Total Grok Detections | 8,144 |
| Ungrouped Events | 7,502 |
| Total After Grok (Clustering) | 15,646 |
| Total Unique Labels | 2,031 |
| Ungrouped Events | 7,502 |
| Total After Classification | 9,533 |

# GROK INCIDENT AUTOMATION

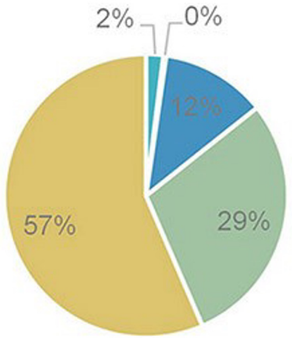
## 89% OF HIGH SEVERITY EVENTS CAN BE AUTOMATED

## OPS CENTER BENEFIT ANALYSIS

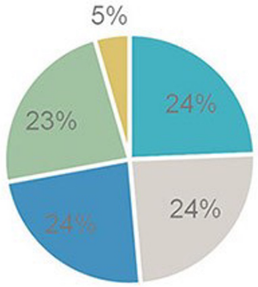
| | | |
|---|---|---|
| Total Events High | | 8981 |
| # of Detections | | 942 |
| Ungrouped Events | | 474 |
| Total After Grok | 84% | 1416 |
| Unique Grok Labels | | 493 |
| Ungrouped Events | | 474 |
| Total with Grok Labels | 89% | 967 |

# GROK ANALYTICS AND ROI

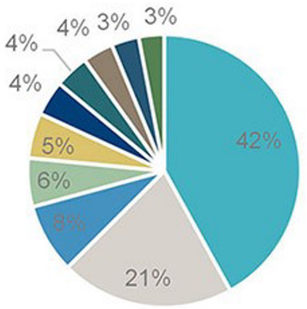
### EVENT BREAKDOWN BY SEVERITY




### TOP 5 DEVICES:EVENTS W/ HIGH SEV. ARE 53% OF TOTAL EVENTS



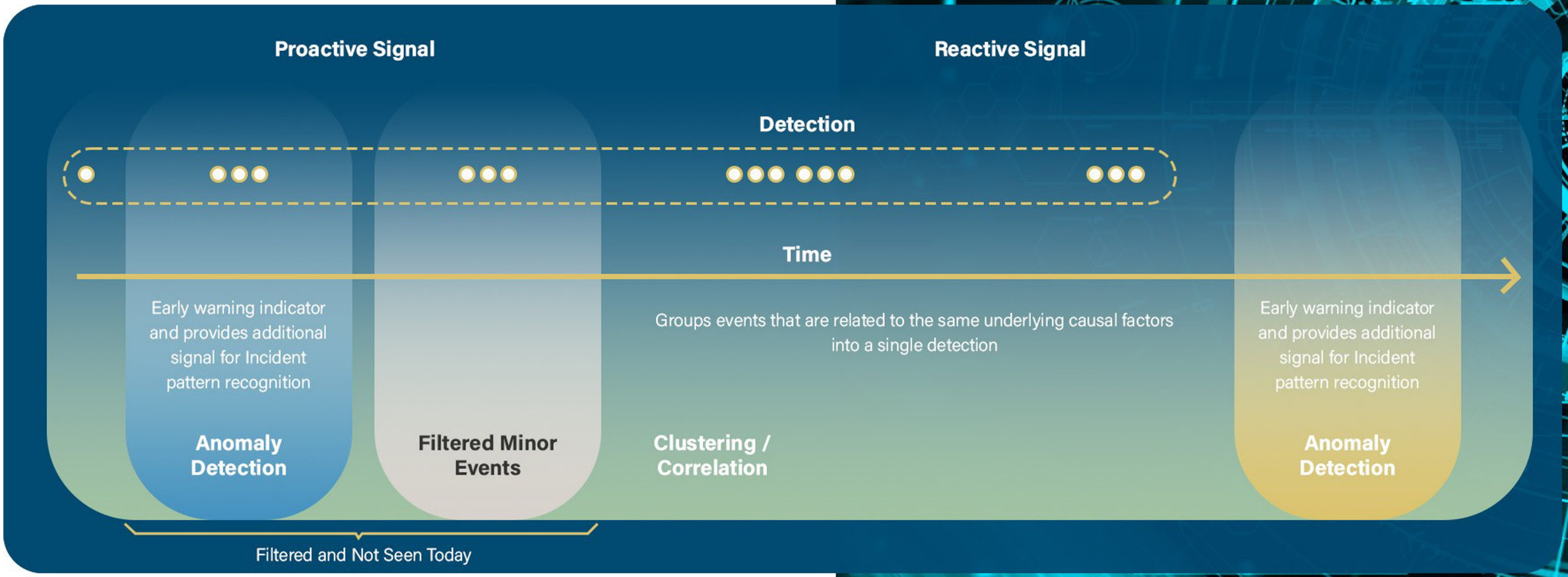

### TOP 10 PROBLEM TYPES



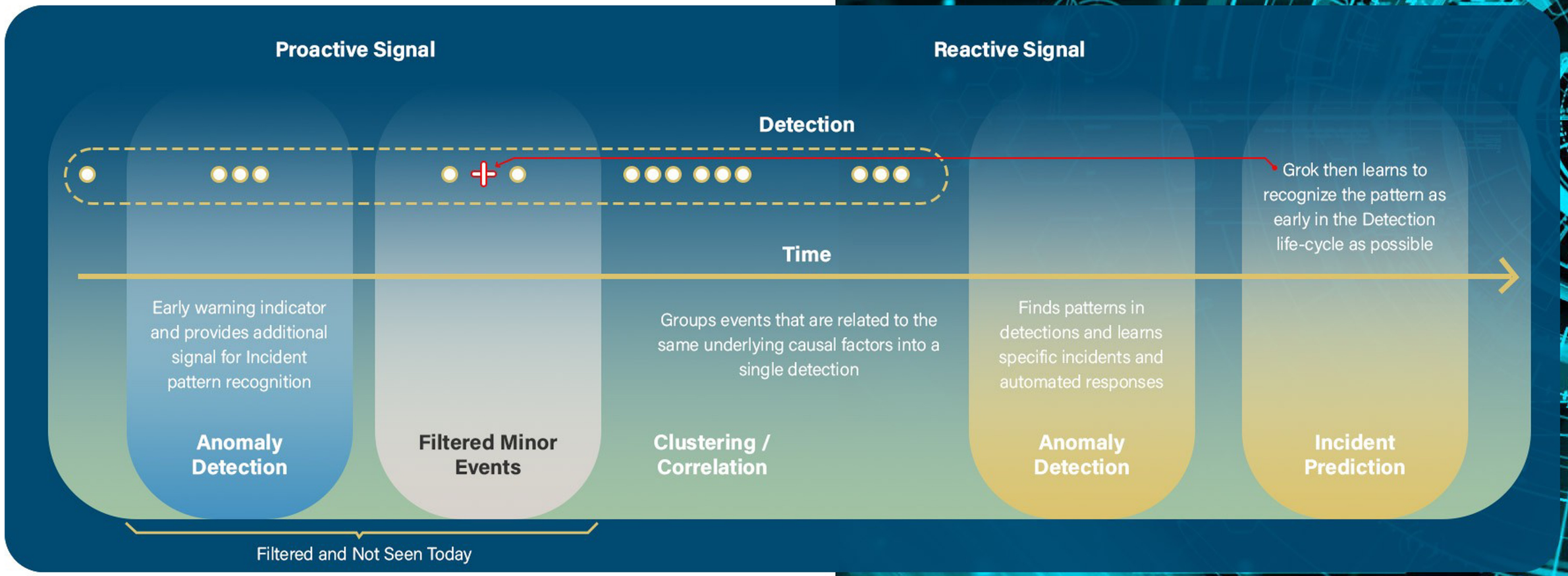

## SAVINGS ANALYSIS (1 DAY)

| | Current | Post Grok | Reduction | Time/Task | Hours Saved |
|---|---|---|---|---|---|
| Total Events | 10,714 | 1,392 | 9,322 | 1 | 56,708 |
| Tickets Manual | 743 | 148 | 594 | 10 | 36,159 |
| Total Hours Per Year Saved | | | | | 92,867 |
| Yearly Cost Avoidance | | | | | $3,250,000 |
| Burdened FTE | $35 | | | | |
| Grok Compression | 85% | | | | |

# USE CASE: How Grok Correlated and Predicted



# USE CASE: How Grok Correlated and Predicted



# DO YOU GROK IT?

## EXAMPLE # 2

# GROK ENTERPRISE CUSTOMER EXAMPLE

## NOC EVENT PROCESSING ANALYSIS (BEFORE AND AFTER GROK)

**Current Operations**

| | Detections | Auto-Ticket/Inci- | Events | Total Work Items |
|---|---|---|---|---|
| Auto-Ticketed | 0 | 0 | 0 | 0 |
| Manual Work | 0 | 0 | 28634 | 28634 |

**After Grok Operations**

| | Detections | Auto-Ticket/Inci- | Events | Total Work Items |
|---|---|---|---|---|
| Auto-Ticketed | | 550.00 | 6025 | |
| Manual Work | 1523 | 0 | 2374 | 3897 |

**WORK ITEM REDUCTION 86%**

# DO YOU GROK IT?

## EXAMPLE # 3

# GROK ENTERPRISE CUSTOMER EXAMPLE

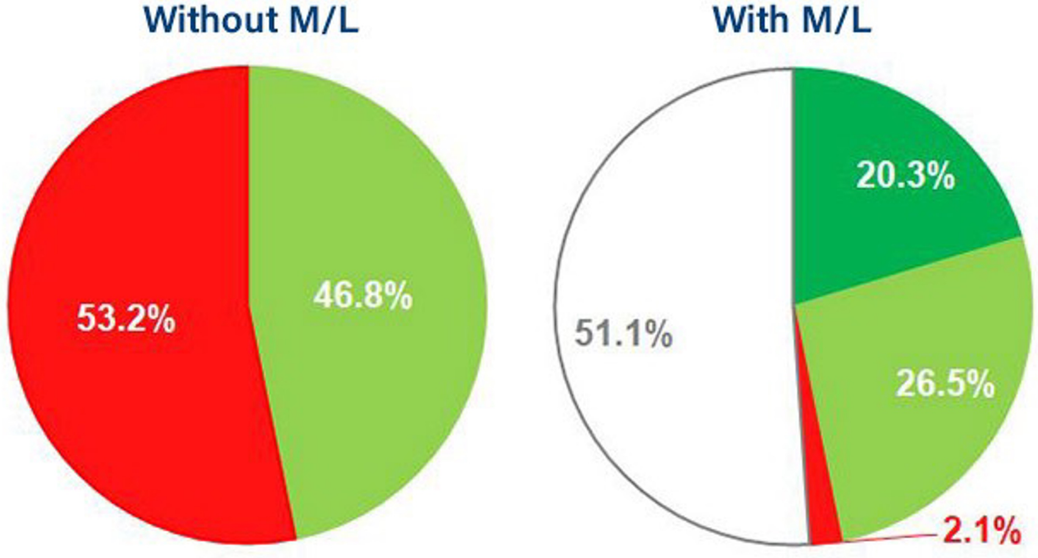
ONE MILLION INCIDENTS REDUCED OVER 2 YEARS!!

# DO YOU GROK IT?

## EXAMPLE # 4

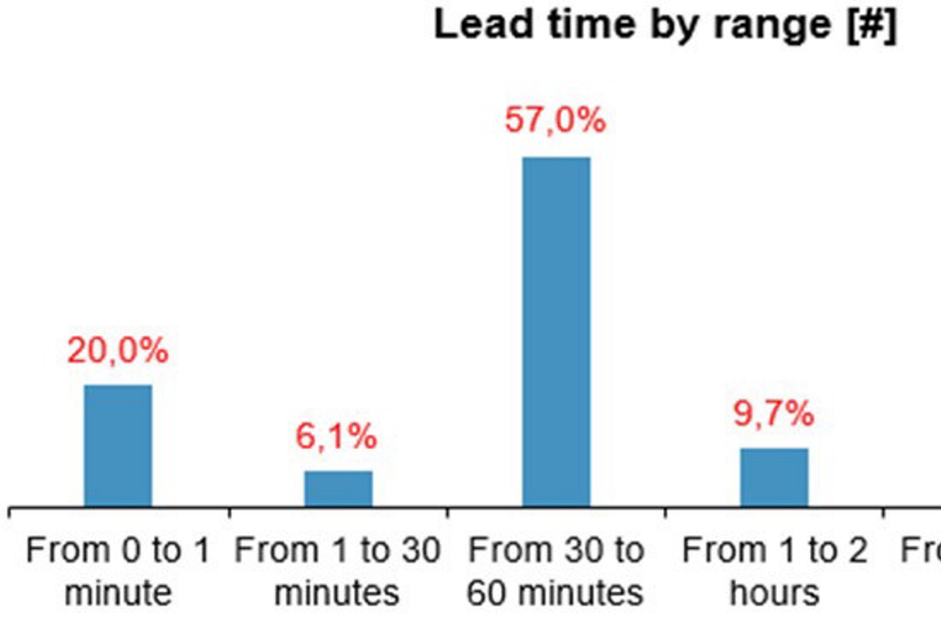
# CUSTOMER EXAMPLE

## BUSINESS IMPACT




- Work that was proactive to the customer's problem
- Work that was reactive to the customer's problem
- Work that didn't "need to be done/ prioritized" but was

## INCIDENT PREDICTION LEA

**Average advanced notification: 33 m**

Lead time = When the INC happens – When