# ACCELERATE SECURITY OPERATIONS WITH INDICATORS OF INSIDER RISK

The growing importance of the security operations center (SOC) cannot be overstated. It acts as the central location to identify and mitigate security threats so must have visibility into everything which means the volume of tracked security events can be overwhelming.

DTEX and Splunk have partnered to streamline SOC operations and accelerate security response times and root cause analysis, driving faster event resolution. Together, DTEX and Splunk are more effectively managing risk and security operations through a single pane of glass. DTEX delivers behavioral context and endpoint telemetry ignored by next-gen AV (NGAV), user and entity behavior analytics (UEBA) and data loss prevention (DLP) tools. With high fidelity metadata and ML-based risk scoring, DTEX helps Splunk to decrease manual security and IT operations and provide better event context with a single, noise-free endpoint data signal.

## DTEX InTERCEPT™

The most effective approach to insider risk management (IRM) converges the essential capabilities from data loss prevention (DLP), User Activity Monitoring (UAM), and User and Entity Behavior Analytics (UEBA). The key benefits are the ability to identify risks without impacting privacy or endpoint performance, and most importantly the capability to proactively detect and mitigate insider risk before a data breach occurs.

Through DTEX DMAP+ Technology™, InTERCEPT collects unique elements of enterprise telemetry from data, machines, applications, and people to capture activity history, behavior trends, data utilization with situational context from across the enterprise to identify indicators of intent and correct risky behavior sooner, while eliminating false positives.

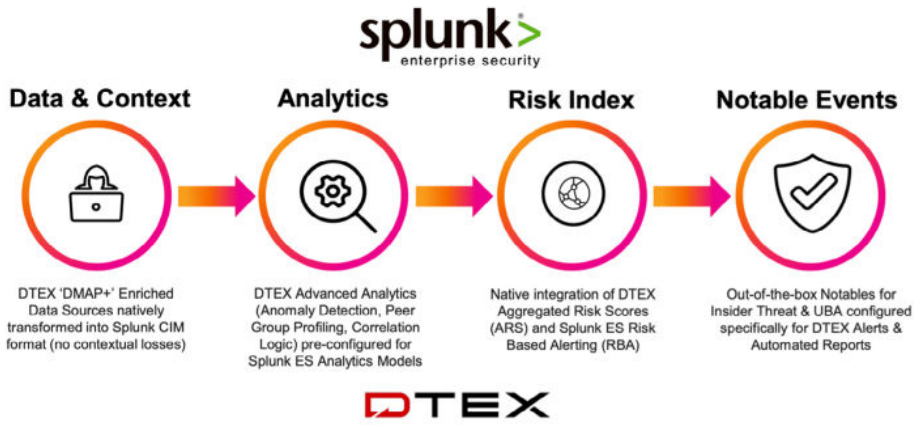
## DTEX and Splunk

Splunk ingests InTERCEPT Indicators of Intent for a better, more contextually rich understanding of user activity to accurately identify risks to data, users and operational processes.

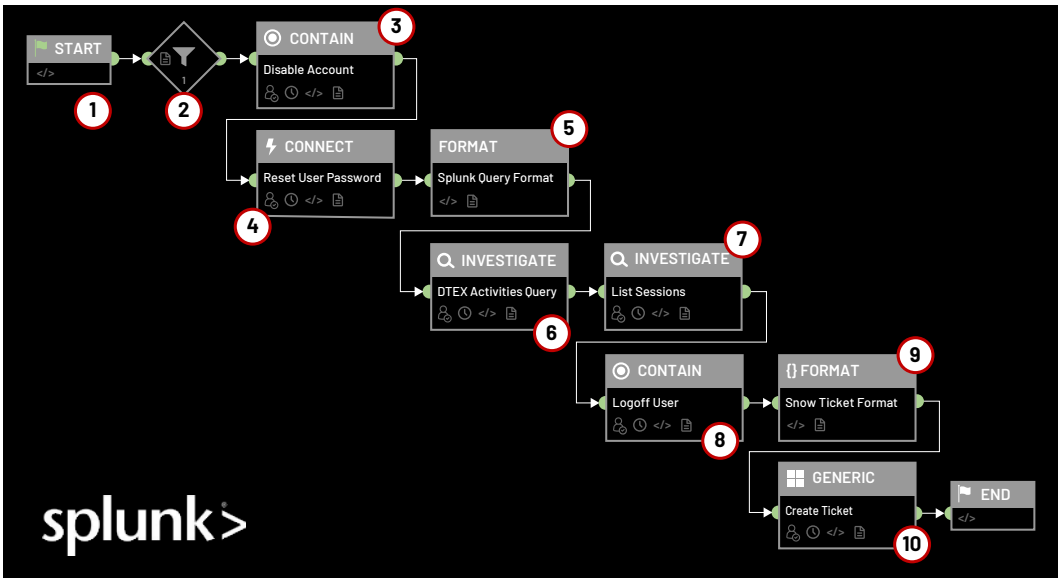
Adding DTEX InTERCEPT to the Splunk workflow provides the following benefits:

- Supports Splunk CIM format with no contextual losses to provide actionable, behavioral intent data within Splunk ES
- Provides detailed analytics and reporting to help accelerate response times and root cause analysis
- Enables faster, more automated 'notable event' investigation and remediation that significantly reduces manual operations

## Integration Data Flow




InTERCEPT risk-scores and streaming behavioral analysis delivers a noise-free signal for user activity to accurately inform automated response processes. Below is an example of a response orchestration utilizing DTEX InTERCEPT telemetry.




1. Playbook kickoff.
2. User risk score > X?
   If so, continue, if not, stop.
3. Disable user AD account.
4. Reset user AD password.
5. Format Splunk query for DTEXactivity search.
6. Gather DTEX activities for user.
7. List user sessions for devices listed in DTEX activities.
8. Log user off of devices.
9. Format ServiceNow ticket.
10. Create ServiceNow ticket with data from prior steps.

DTEX

### REQUEST A DEMO

**Contact us today to schedule a demonstration at demo@dtexsystems.com**

### ABOUT DTEX SYSTEMS

DTEX Systems empowers organizations to prevent data loss and support a trusted workforce by proactively stopping insider risks from becoming insider threats. Its InTERCEPT™ platform consolidates the essential elements of Data Loss Prevention, User Activity Monitoring, and User Behavior Analytics in a single light-weight platform to detect and mitigate insider risks well before data loss occurs. Combining AI/ML with behavioral indicators, DTEX enables proactive insider risk management at scale without sacrificing employee privacy or network performance.

**To learn more about DTEX Systems, visit www.dtexsystems.com.**