DTEX
WORKFORCE CYBER INTELLIGENCE & SECURITY

splunk>
turn data into doing™

SOLUTION BRIEF

Accelerate Security Operations with Contextual Human Intelligence & Endpoint Telemetry

NEXT-GEN HUMAN ACTIVITY VISIBILITY, DETECTION AND FORENSICS

Prevent Data Loss
with behavioral intent intelligence.

Detect Insider Threats
with dynamic risk scoring.

Enrich SOC Operations
with human telemetry.

Accelerate Incident Response
with real-time forensics.

Splunk and DTEX Systems have partnered to offer a first-of-its-kind Workforce Cyber Intelligence & Security solution that delivers the contextual human activity intelligence and endpoint telemetry ignored by NGAV, UEBA and DLP tools.

Together, Splunk and DTEX are accelerating security response times and root cause analysis, driving faster event resolution with advanced analytics and reporting, and decreasing manual security and IT operations with DMAP+ telemetry that provides the full context regarding the data, machines, applications and people involved in an event via a single, noise-free endpoint data signal.

Applications, data and machines don't move, change or update themselves; they follow the instructions of their human operators. The DTEX Workforce Cyber Intelligence & Security platform is the first and only solution built to ***capture, analyze and stream in real-time the metadata*** that genuinely expresses human intent.

DTEX InTERCEPT™ brings a previously unavailable data source to existing cyber security architectures that multiplies the value of NGAV while allowing for the consolidation of UEBA, Endpoint DLP and Digital Forensics tools with a lightweight, cloud-native platform that scales to hundreds of thousands of endpoints and servers in hours with zero impact on user productivity and endpoint performance.

DTEX InTERCEPT's next-generation DMAP+ forwarders and cloud analytics engine delivers a single, noise-free data source that proactively identifies insider threats, predicts data loss events, protects remote workers, flags possible credential compromise and monitors file servers and packaged applications for abnormal behavior and requests.

BENEFITS

- 90% Fewer False Positives
- 30% Improvement in SOC Tools ROI
- 200% Increase in Automated Interventions
- 80% Reduction in Manual SOC Operations

USE CASES

- Insider Risk Management
- Credential Usage Monitoring
- People-Centric DLP
- Remote Workforce Security
- User Behavior Analytics
- Phishing & Social Engineering Attack Awareness

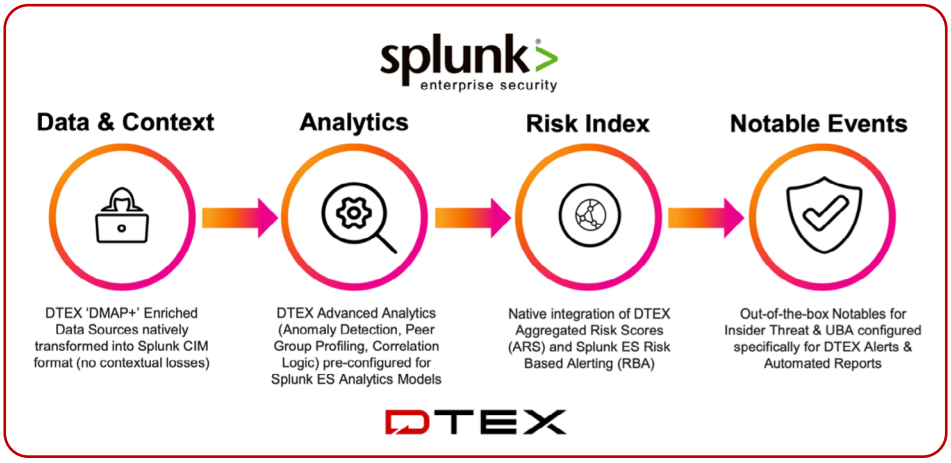
FEATURES

- Lightweight Forwarder with Near Zero Impact to the Endpoint
- Cloud Analytics Engine
- Data Usage Monitoring & Enforcement
- Dynamic Activity Risk Scoring
- Digital Forensics and Audit Intelligence
- On & Off Network Monitoring

Splunk takes DTEX InTERCEPT's 'Indicators of Intent' and uses them to provide the customer with a better, more contextually rich understanding of how user activity is influencing what's happening in their environment and if those behaviors are creating risks to data, users and operational processes.

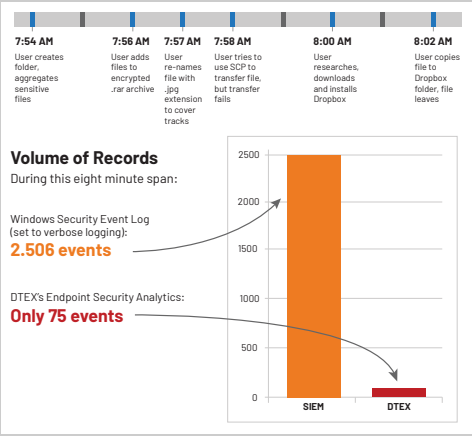
How Organizations Are Utilizing DTEX InTERCEPT with Splunk ES & Phantom

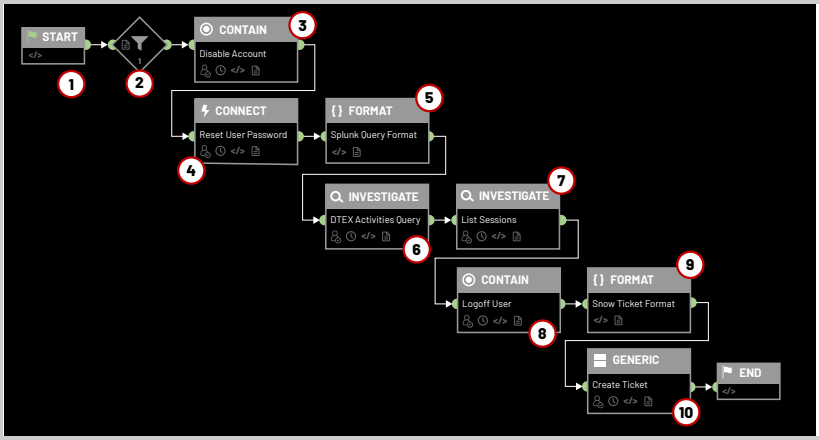
- Advanced integration with DTEX InTERCEPT DMAP+ data source, including transformation into Splunk CIM format (no contextual losses) to provide actionable, human-behavioral intent data within Splunk ES
- Real-time, detailed analytics and reporting for DTEX InTERCEPT to accelerate response times and root cause analysis by upwards of 30%
- Faster, more automated 'notable event' investigation and remediation that can reduce manual operations by 80%



Unlike legacy solutions, DTEX InTERCEPT provides a simple and clear view of human activity. The graphic below on the left illustrates a short sequence of user activities representing high-risk behavior that creates several thousand windows events that can be very di cult to review and interpret. By contrast, DTEX Workforce Cyber Intelligence & Security data is filtered at the source, and the context provided reduces the number of truly notable events from 2500 Windows Security Event Logs to less than 100.

In a similar construct with Splunk Phantom, DTEX InTERCEPT's risk-score stacking and streaming behavioral analysis delivers a noise-free signal that expresses user activity to accurately inform automated response processes. The graphic below on the right is an example of a response orchestration utilizing DTEX InTERCEPT's human intelligence telemetry.





1. Playbook kickoff.
2. User risk score > X? If so, continue, if not, stop.
3. Disable user AD account.
4. Reser user AD password.
5. Format Splunk query for DTEX activity 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.

splunk> turn data into doing

SUPPORTED PLATFORMS

Microsoft Linux macOS® CITRIX®

REQUEST A DEMO

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

ABOUT DTEX SYSTEMS

DTEX Systems is the world leader in Workforce Cyber Intelligence and committed to helping enterprises run safer and smarter. Only DTEX dynamically correlates data, application, machine, and human telemetry to stream context-rich user behavior and asset utilization analytics that deliver a first-of-its-kind human-centric approach to enterprise operational intelligence. Hundreds of the world's largest enterprises, governments and forward-thinking organizations leverage DTEX to prevent insider threats, stop data loss, maximize software investments and deployments, optimize workforce productivity, and protect remote workers. DTEX has offices in San Jose, California, and Adelaide, South Australia, and is backed by Northgate Capital, Norwest Venture Partners, Wing Ventures, and Four Rivers Group. To learn more, visit: www.dtexsystems.com.