Next Generation SOC

DarkMatter – Expo 2020

Eman Al Awadhi
Director | Cyber Security & Resilience – Expo 2020

Eric Eifert
Senior Vice President | MSS – DarkMatter

.conf19

splunk>

Eman Al Awadhi

Vice President | Cyber Security & Resilience – Expo 2020

Eric Eifert

Senior Vice President | MSS – DarkMatter

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Intro

CONTENT

1

EXPO 2020

Mega Event Overview

.conf19

splunk>

Expo 2020: Site Overview

25 Million Visits

50:50 Male vs Female

190+ Countries

70% Adult International Visitors

Expo 2020 sets the UAE stage by bringing together ideas, innovation, and inventions on 20 October 2020 for a period of 6 months. This celebration of human ingenuity offers a glimpse into the future and is anticipated to attract 25 million visits, 70% of which are international visitors from more than 190 countries.

Expo 2020 Security Landscape

New Smart City

Synopsis

- Expo 2020's site will spread across 1083 acres with over 2.15 M square feet of building space.
- It is a new city with the latest technology, building management systems, 5G communication, etc.
- Multiple smart Internet of Things (IoT) solutions are implemented across the campus to ensure a resilient, scalable and secure IoT network is available.

Challenges

- To deliver a smooth and secure anytime, anywhere, and device (ATAWAD) experience for all parties interacting with Expo 2020.
- To facilitate continued connectivity and create the foundation for a smart city.
- Access to telemetry from non-IT monitoring systems and external interconnections.

2

CYBER THREAT LANDSCAPE

.conf19

splunk>

Cyber Threat Landscape

National Infrastructures

	Domains	Sub-Domains
1	Smart **Energy & Environment**	Energy, utilities, agriculture & waste management, etc.
2	Smart **Mobility**	Intel traffic sys, transportation & urban logistics, etc.
3	Smart **Buildings**	Facility management, homes & construction, etc.
4	Smart **Health**	Health info sys, telemedicine & assisted living, etc.
5	Smart **Government**	Digital public administration, defense, governance & e-services, etc.
6	Smart **Education**	Education platforms, digital learning & skills, etc.

Impact to Expo 2020

DATA LEAKAGE
- Public Trust Implications
- International Relations
- Risk impact to Expo's 25 million visit target or vast financial services community

PHYSICAL SECURITY BREAKDOWN
- Risk impact to Expo's 25 million visit target
- Human Safety
- Interruption to Operations

EVENT DISRUPTION & FAILURE TO RECOVER
- Interruption to Operations
- Event Schedule
- Financial, Regulatory and Legal Compliance Implications
- Reputational Damage

FAILURES TO MANDATORY COMPLIANCE
- International Relations
- Public Trust Implications
- Financial, Regulatory and Legal Implications

COMPROMISED SYSTEMS
- Financial, Regulatory and Legal Implications
- Loss of Money, Privacy
- Reputational Damage

GEOPOLITICAL RISK (E.G. Espionage)
- International Relations
- Public Trust Implications
- Interruption To Operations

The main objectives of mega events and large scale systems are reliable and smooth operations, zero downtime, and data integrity; all of which work together to provide both a seamless experience that "wows" visitors and participants as well as a platform for innovation that engages people to create the future.

Mega Event Case Study: Olympic Games

2008

BEIJING – Ticket Scamming | DDoS

First Olympics to report millions of instances of malicious cyber activity. The majority of this activity was low level and did not affect the games.

2010

CANADA – no publicised incidents

2012

LONDON – Ticket Scamming | DOS | DDoS

Suffered an internal DOS attack in addition to more generic DDoS attacks and ticket scamming activities.

2014

SOCHI – Ticket Scamming | Malicious Wi-Fi

Sochi was affected by malicious Wi-Fi, which is reported to have automatically downloaded as attendees connected to the Olympics' networks.

2016

RIO – Ticket Scamming | DDoS | IOC/WADA Data Leak

Hacking and leaking of athletes' medical records, as well as generic DDoS attacks and ticket scamming activities.

2018

PYEONGCHANG – IOC/ WADA Data Leak | Targeted Intrusion Event

Olympics' official website was offline for 12 hours and the network around venue was also down.

Source: https://www.cybereason.com/

3

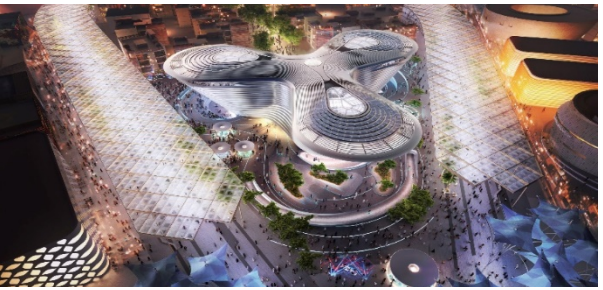
DARKMATTER AT EXPO 2020

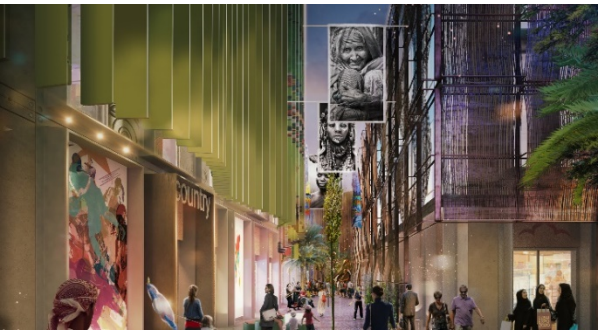
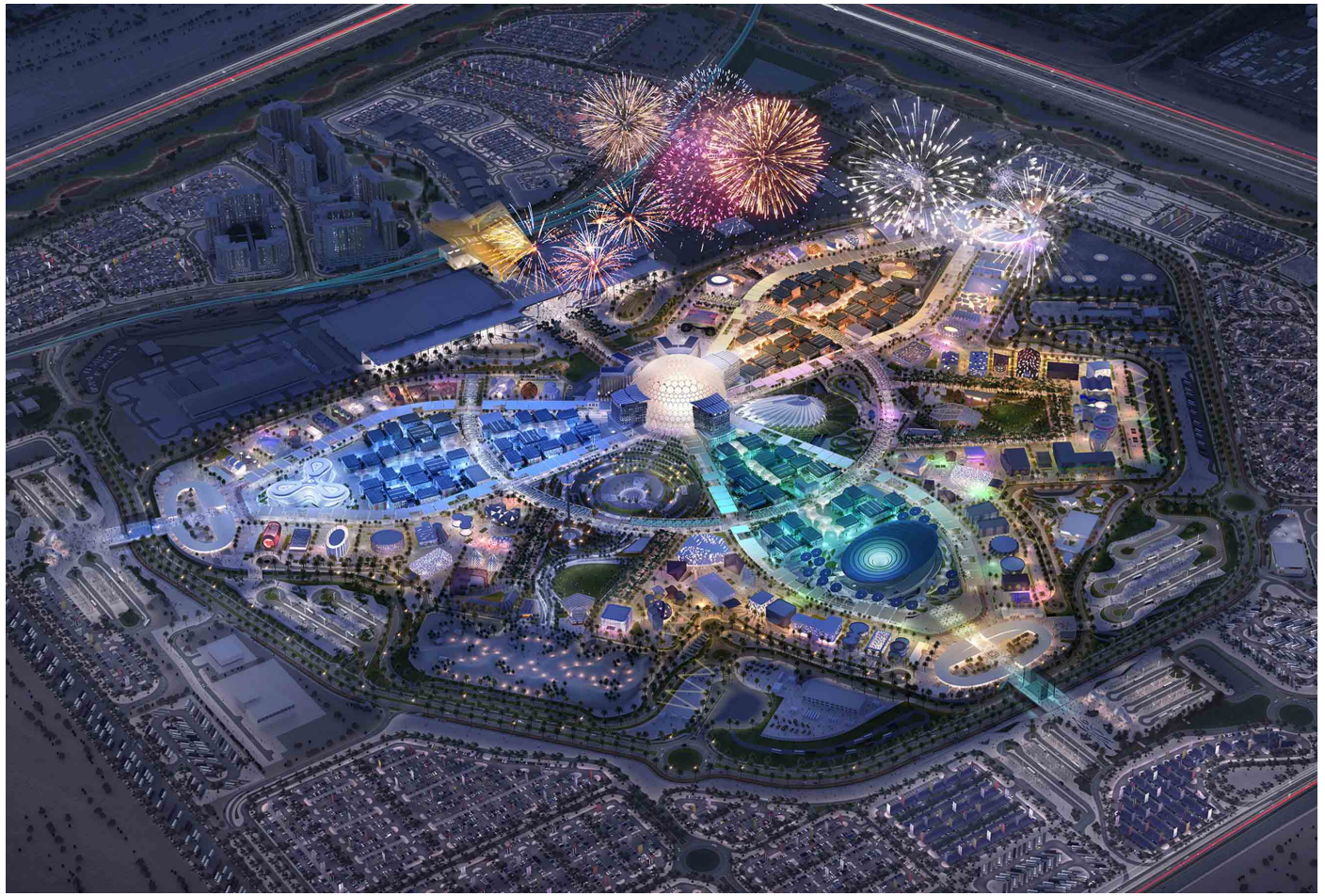
.conf19

splunk>

Role of DarkMatter at Expo 2020

DarkMatter Group will provide Expo 2020 with a holistic cyber security framework delivered through continuous security monitoring, risk assessment, incident response, and digital forensics, to ensure it is one of the safest and most technologically secure World Expos in history




Cyber Security Approach for Expo 2020

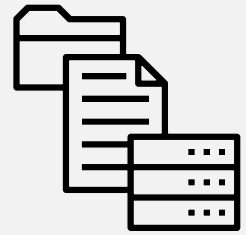
As Expo 2020 Dubai's Official Cyber Security Provider, DarkMatter Group will oversee the cyber security of Expo 2020's entire digital platform, as well as the applications and data it supports, to safeguard the digital experience of millions of visitors and participants

Use Cases

- Security Monitoring
- Internet of Things
- Incident Management
- Log Management

Data Sources

- Internet Service Provider (ISP) Network
- Event Site
- Physical Security Environment
- AWS Environment
- SaaS Environment
- AWS Internet of Things (IoT)



Cyber Security Approach for Expo 2020

To provide Expo 2020 a secure and resilient cybersecurity environment that enhances the visitor and participant experience

Deliver Situational Awareness

- Log Collection
- Log Analysis
- Monitoring of Security Environments
- Event Correlation
- Reporting

Reduce Risk or Downtime

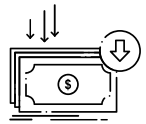
- Log Retention and Archival
- Monitoring of Security Environments
- Event Correlation
- Incident Management
- Reporting

Support Audit and Compliance

- Log Collection
- Log Retention
- Archival Reporting

Prevent and Control Threats

- Log Retention and Archival
- Log Analysis
- Monitoring of Security Environments
- Event Correlation
- Incident Management
- Threat Identification
- Threat Reaction
- Reporting



Diminishing of Administrative Overhead

- Log Retention and Archival
- Log Analysis
- Monitoring of Security Environments
- Event Correlation Reporting

Forensics

- Log Collection
- Reporting

splunk> .conf19

4

NEXT GENERATION SMART SOC

.conf19

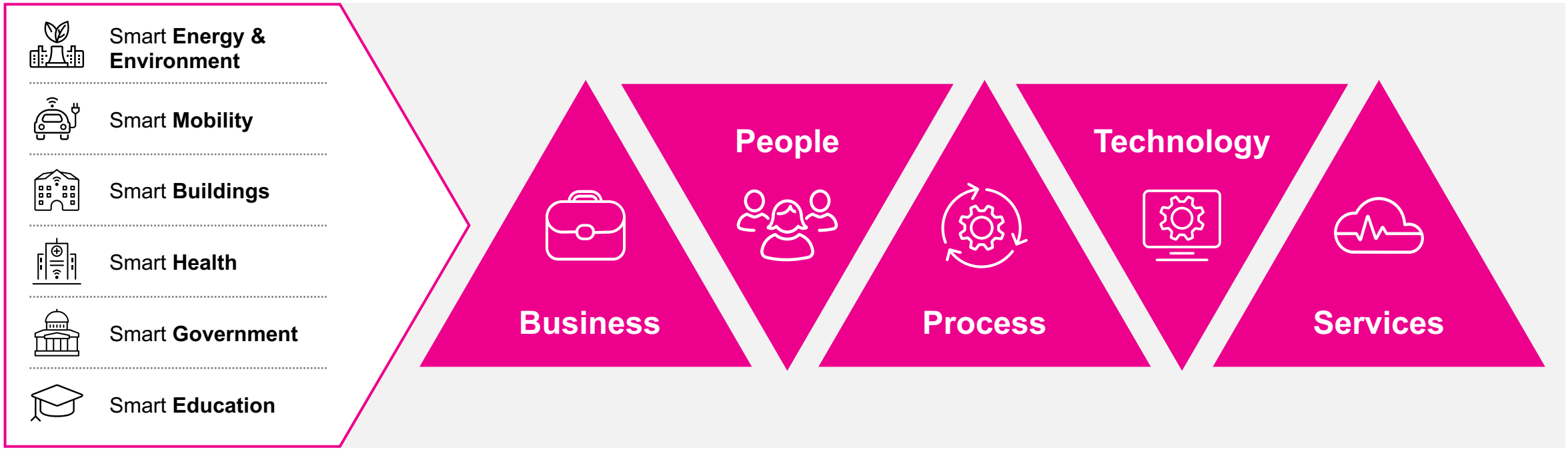
splunk>

Security Operations Center

Next Generation Smart SOC

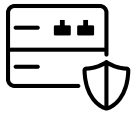
Next Generation Smart SOC should be established using a holistic cyber security approach.

- This provides increased visibility across critical business operations, such as:
- Information Technology
- Operational Technology (Industrial Control Systems/SCADA)
- Internet of Things/Everything



Next Generation Smart SOC Capabilities

To build a Next Gen Smart SOC, a Holistic Approach
that integrates Advanced Capabilities is essential



Security Monitoring

- SIEM platform
- Defined SOP's & playbooks
- Incident management platform
- Defined SLA & OLA

Endpoint Detection and Response

- Increased threat visibility
- Increased visibility & control of assets
- Zero-Day attacks detection

Threat Intelligence

- Advanced threat analytics
- Enterprise vulnerability management
- Enterprise security portal

Big Data Analytics

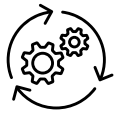
- Ability to ingest and analyze more data sources
- Flexible dashboards & reports
- Threat Hunting

Continuous Monitoring

- Advanced threat protection
- Complete data protection
- Privileged access management
- IT/OT convergence

Automated Response

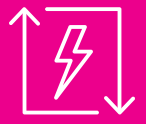
- Advanced incident response
- Security orchestration & automation
- Rapid recovery



Service Optimization

- Integrated solutions
- Use Case Development
- Cross-solution data enrichment

Next Generation Smart SOC Leveraging Splunk

Splunk Enterprise 	Splunk Enterprise product will be used as a big data solution to collect all the logs. Splunk Enterprise Security will be the nerve center of the SOC, giving teams the insight to quickly detect and respond to internal and external attacks, simplify threat management minimizing risk. ES helps teams gain organization-wide visibility and security intelligence for continuous monitoring, incident response, SOC operations, and providing executives a window into business risk.
Data Volumes 	Currently, 500Gb/day but potential increase to 800Gb/1Tb per day.
Deployment 	Deployed in the Expo Datacenter, Telco Datacenter, DR facility, and AWS infrastructure.

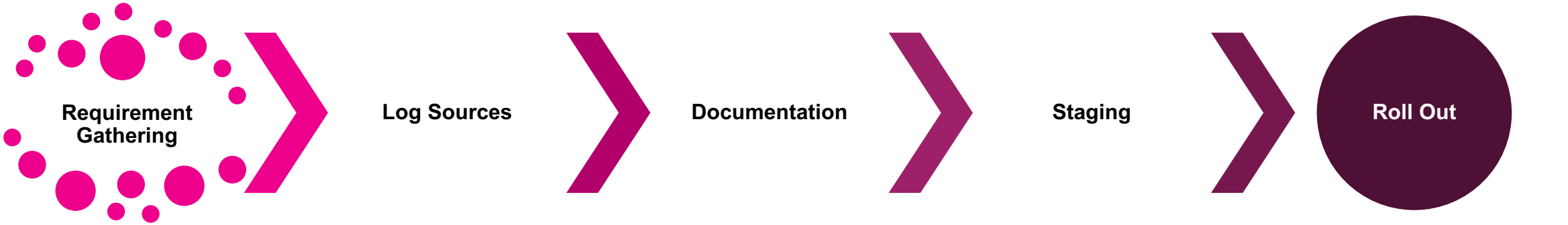
5

USE CASES

.conf19

splunk>

Use Case Development



- Meet with Stake Holders and understand what interests them
- Get your head around the Infrastructure and data flows

- Ensure you have required visibility
- Decide what logs interest you and what is noise

- Define Logic and check for redundancy
- Enrichment/Mapping/ Threat Model alignment
- Define anticipated outcome and recommended course of actions

- Develop and Deploy use case in a staging environment
- Fine-tune here till the FP:TP ratio is around 3:1
- Also watch the load it caused on your SIEM platform
- Have Red Team assessments at this stage to test the use case

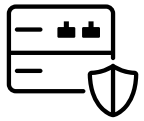
- Once you are confident of the use case, roll it out in production
- Rest is maintenance of the use case for as long as it is relevant

A

USE CASES

SECURITY MONITORING

Expo 2020 Security Use Cases



Security Monitoring

- Mega events risk cyber-attacks and security is a priority.
- Expo 2020 has thousands of IT devices distributed across multiple systems (Private & Public).
- Distributed system events integrated with Splunk Enterprise.
- Advanced use cases are developed and enriched by non/-structured contextual data, from many sources e.g. physical security and IoT.
- Using Splunk, The DarkMatter Group (DMG) will detect threats and respond to security alerts within 15 minutes.

Simple & Consolidated Visualization

- Splunk normalizes large volumes of complex data generated by IoT devices.
- Normalized data provides decision-making information to Security Analysts, allowing them to take action on events of interest.
- DMG will use Splunk to develop consolidated views to detect any abnormalities across the Expo 2020 campus.
- The heat map will provide a graphical representation of the data coming from all IoT and IT devices.

Real Time Analytics

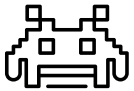
- Data from thousands of IoT devices ingested into Splunk Platform.
- DMG will apply required level filters to configure alerts and notifications to aid detection and response to identified issues.
- Supported by Splunk Adaptive Response; response time reduced to [Target 5 minutes].
- Splunk machine learning capabilities and predictive analysis features allow identification of failures once initiated, avoiding late detection and catastrophic failures.

Security Use Cases

Cyber Security

Advanced Threat Activity Detection

- Creation of correlation rules and use cases.
- Identifying latest known exploit-based attack vendors.



Malware Activity Detection

Malicious activity/programs specifically designed to interrupt, damage, or gain authorized access to a computer system without the knowledge of the owner.

Web Defacement Detection

- Unauthorized hacks on web page/website.
- Mutilating partial/whole structure.
- May include insertion of hazardous content, malicious code, etc.
- Code injections can compromise customer data.
- Defaced web page can inflict severe damage to business reputation and reliability.

Brand Protection Services

- Prevent unauthorized use of brand.
- Prevent activity harmful to brand reputation.

Lateral Movement Detection

Attacker moves from compromised entry point across the network to other systems.

Brute Force Access Detection

A trial and error method used to discover a password by systematically trying every possible combination of letters, numbers, and symbols until the correct combination is found.

Data Exfiltration Detection

- Unauthorized transfer of data from corporate systems, whether those systems are a user's computer or IT servers.
- Unauthorized transfers can be carried out by someone manually or automatically via malicious programs over a network.

splunk> .conf19

C

USE CASES

INTERNET OF THINGS (IoT)

IoT Use Cases

DM SOC collects logs from the Siemens Mindsphere platform hosted in AWS to build below use cases.

Single Platform Visualization of all Deployed Technologies[1]

- All deployed technologies should be made visible and managed through a single platform that aggregates and normalizes the different data sources.
- Provides an aggregate and indicates the compliance status of different businesses.

Real-time Temperature and Humidity Monitoring[2]

- Monitor temperature and humidity across the Expo campus including the indoor area, outdoor areas, and the datacenter.
- Provide a real-time heat map following the color scheme of zones/buildings on Expo's site.

Real-time Pollutant Measurement (O3, SO2, CO, NOx, PM 1, 10, 25)[3]

- Monitor air pollutants harmful to human health through using the smart sensors fixed site wide and in-building that provide specific and high resolution readings of selected areas.

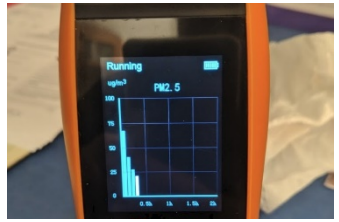
Real-time Energy & Water Monitoring[4]

- Monitor energy and water usage through smart meters to view campus utilization levels.
- Total energy and energy consumed by lighting and HVAC should be measured separately and displayed for the entire campus.
- Monitor quality of water used for drinking and for water bodies. E.g. parameters: pH, turbidity, bacterial count, etc.
- Monitor water leakage in data center false flooring using smart sensors.

Identify Health Impact[5]

- Indicate the health impact of GHG concentration – to humans, environment, in both the short term and long term.

Trends and Patterns[6]



- Provide a historical view of air quality measurement, extending past time of deployment – aggregating existing data sources and readings of air quality into the single platform.

splunk> .conf19

D

USE CASES

INCIDENT AND LOG MANAGEMENT

Incident and Log Management

Incident Management

- DM SOC team will consistently detect, report, and respond to incidents throughout the organization to minimize disruption to Expo 2020.
- Incident priority determined by impact on Expo 2020 business and urgency of required response.
- In case of incident, primary concern is restoring services ASAP to comply with SLAs and expectations based on impact to business.

Log Management

- Integrating, managing, and monitoring Expo 2020's security, system, application and other logs from agreed set of data sources.
- This supports the Expo 2020 Security Monitoring policy and details the procedures involved in managing the life cycle of security logs from information systems owned and managed by Expo 2020.

7

AUTOMATION

.conf19

splunk>

Security Orchestration Automation and Response

SECURITY ORCHESTRATION AND AUTOMATION

Integrate disparate technologies and people, and automate response to accelerate security operations.

SOAR

SECURITY INCIDENT RESPONSE PLATFORMS

Centralize data from multiple sources for effective security operations.

THREAT INTELLIGENCE PLATFORMS

Gather and contextualize threat data, implement alerts, respond to threats, strengthen proactive defense.

Outro

Q&A

Eman Al Awadhi | Speaker

Eric Eifert | Speaker

.conf19

splunk>

Thank You!