VIRGINIA IT AGENCY

AIsaac to Splunk Migration

Streamlining SIEM and Logging at VITA

August 14, 2025

Atos

Agenda

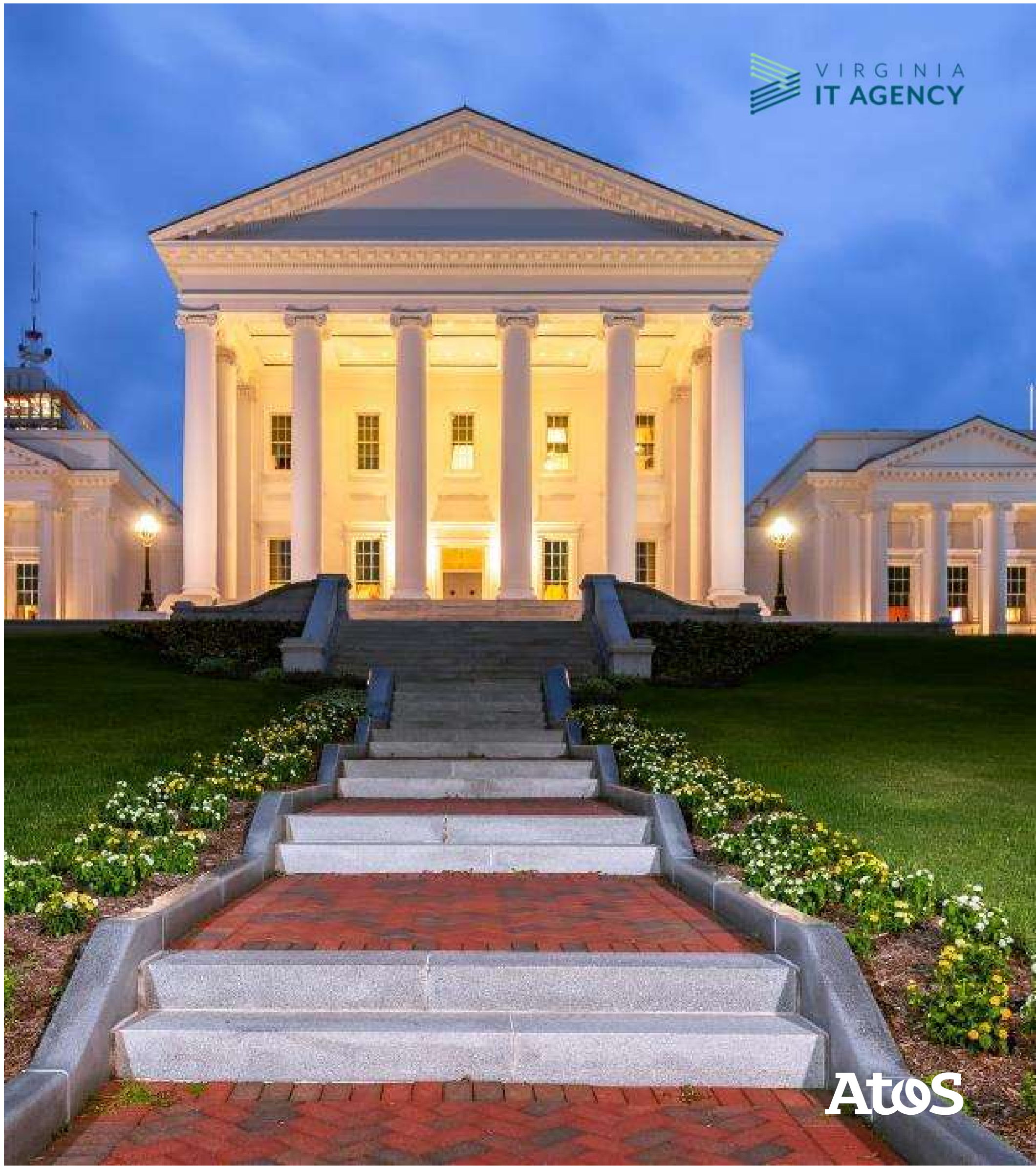
Introductions and Background

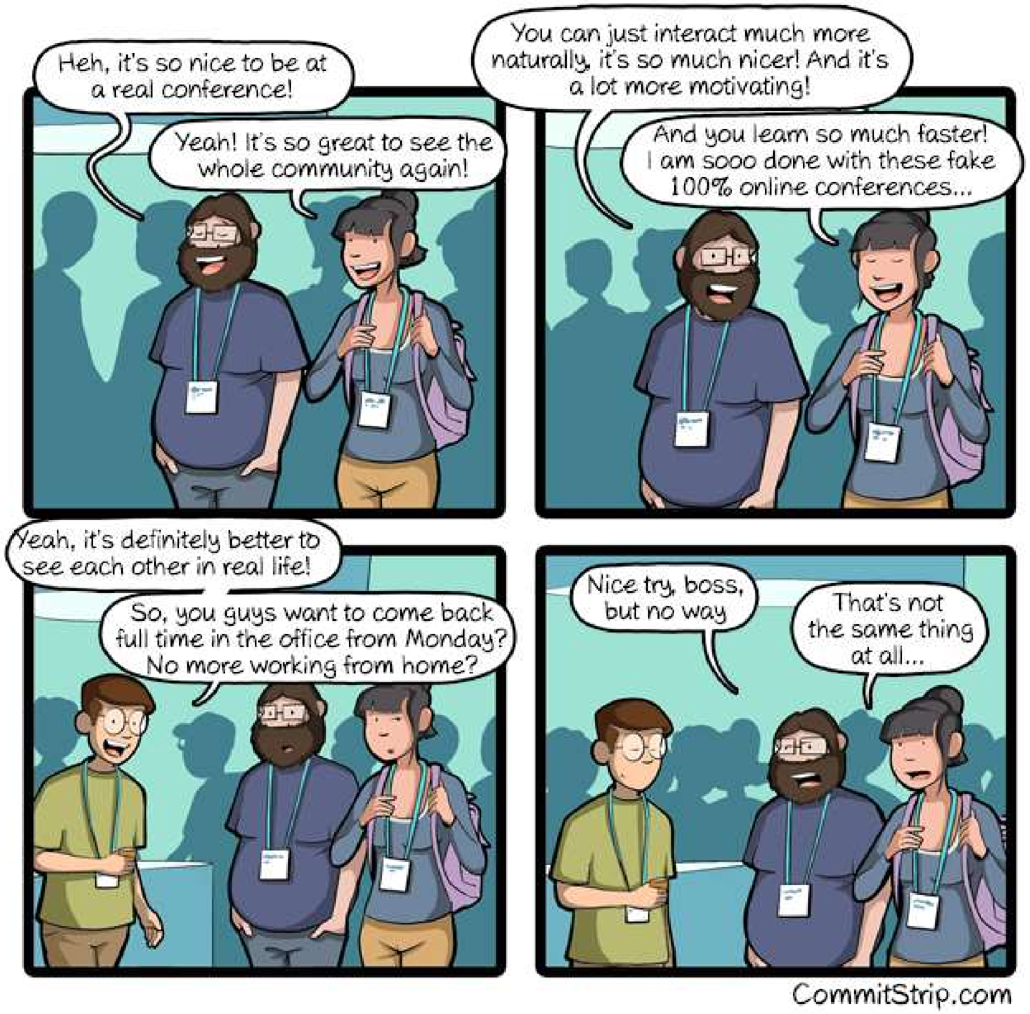
Project Overview

Migration Approach

Desired Outcomes

Introductions and Background




Heh, it's so nice to be at a real conference!
Yeah! It's so great to see the whole community again!
You can just interact much more naturally, it's so much nicer! And it's a lot more motivating!
And you learn so much faster! I am sooo done with these fake 100% online conferences...
Yeah, it's definitely better to see each other in real life!
So, you guys want to come back full time in the office from Monday? No more working from home?
Nice try, boss, but no way
That's not the same thing at all...
CommitStrip.com

Today’s Team

Greg Booth
VITA Security Service Owner

Kevin McLees
Atos Account Executive

Richard White
VITA Director of Security Products and Services

Atos: MSS for VITA and a Leader in Cybersecurity

#1 Managed Security Services Vendor in Europe and # 5 Globally by Gartner

VIRGINIA IT AGENCY

6,500+
security professionals

31 billion
security events processed per day

17
Security Operations Centers

15 million
vulnerability scans test cases

3.2 million
endpoints secured by Atos

300 million
citizens covered by our solutions

30+ million
network equipment and secure mobile phones

AIsaac
Patented AI platform

Evidian
Identity and access management

IDnomic cryptovision
Trusted identities for people and devices

Trustway
Data protection at rest and in motion

Gartner	IDC	ISG	NelsonHall	Everest Group	AVASANT
Top 1	LEADER	LEADER	LEADER	LEADER	LEADER
Managed Security Services **European Vendor** (based on 2023 revenues)	MDR **MEA 2024** **Major Player** MDR **Worldwide 2024** **Major Player** Cybersecurity Consulting **Worldwide 2024** **Major Player** **Worldwide** Cloud Security Services in the AI Era **2024**	IAM, MSS, TSS, SSS and DFIR **France** **Germany** **Switzerland** **UK** **US** **2024**	Cyber Resiliency Services **Global 2024**	Cybersecurity Services PEAK Matrix **Europe 2024** **Major Contender** Cybersecurity Services PEAK Matrix **North America 2024**	Cybersecurity Services **Global 2024**

Atos

End to End Cybersecurity Solutions

Empowering Resilience and innovation

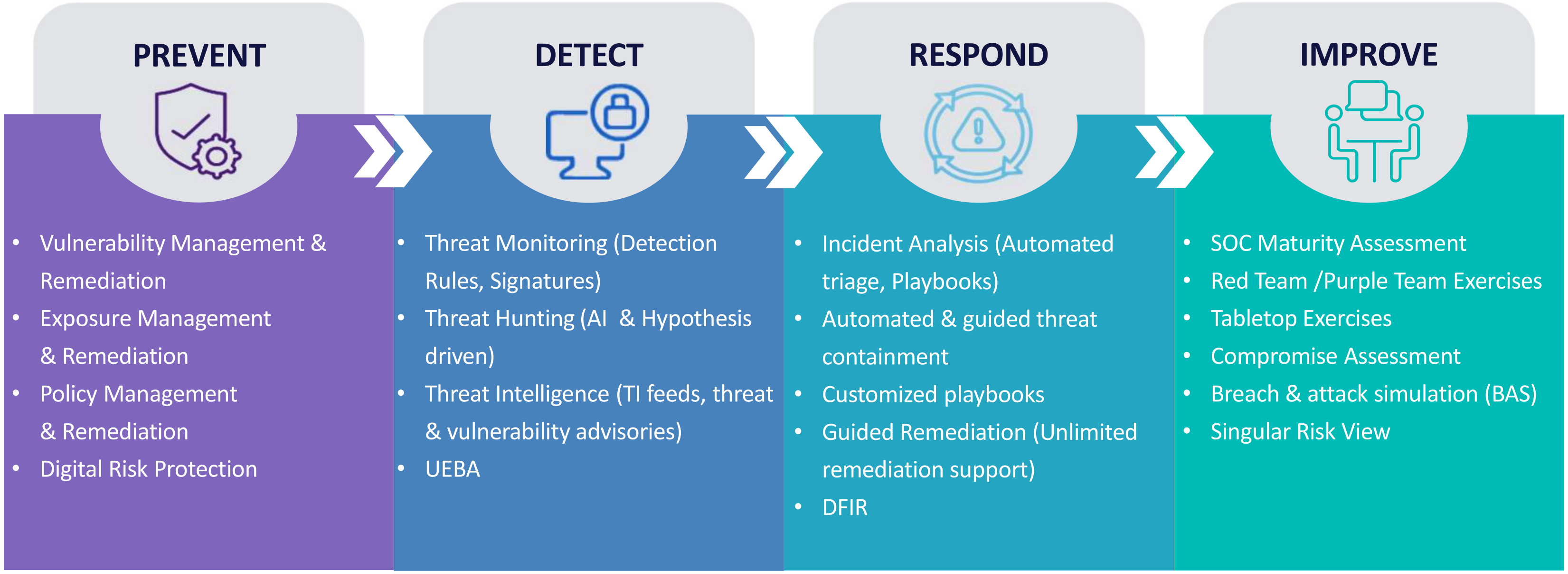
Cybersecurity Services Detailed Offering

Strategic guidance for resilience & compliance	*Cyber Assurance*	*Hybrid Cloud resilience @scale*	*Identity & Access resilience @scale*	*360° OT resilience*	*Proactive Threat Defense & Response*	*Future-proof Security*
1 **Advisory**	2 **Security Testing**	3 **Hybrid Cloud Security**	4 **Identity & Access Management**	5 **OT Security**	6 **TDIR/ MDR**	7 **Disruptive Offers**
Cybersecurity Investments Quantitative Analysis	Vulnerability Management Services	Cloud Service Provider Security *(AWS, Msft, GCP)*	Federated Id. / SSO	OT Advisory (Policy Creation, Vuln. Scan, Archi., Risk Ass.)	MDR powered by AIsaac	Post Quantum Cryptography (MVP)
Security Strategy & Planning	Secured Code Review (SAST)	Multi-Cloud Protection Platforms *(CNAPP, SASE)*	Identity Governance & Administration	OT security testing	MDR by Chronicle	Privacy Enhancing computation Tools
Security Archi. & Design	IoT/IIoT/Embedded Security Assessment	Network & Workplace Security	PAM	IoT Cloud Security Platform	SOC powered by Microsoft SecOps	GenAI Security
Governance, Risk and Compliance	Specialized Testing (includes SAP)	Firewall Services	PKI & CLM	Network Security for OT/ IoT	Managed Endpoint Detection & Response	Digital Sovereignty
Ent. Security Dashboard	Red & Purple Teaming Service	DDoS Mitigation	DevOps Secret Mgt.	5Guard	MDR for OT	
Third Party Risk Assessment	Penetration Testing	Secure Mail Gateway	Secure Cloud Access *(CIEM)*	Network Traffic Analysis	MDR for Healthcare	
Certifications Services *(ISMS-ISO 27001, PIMS-ISO 27701, PCI-PSS Audit)*	Application Security Testing (DAST)	Secure Web Gateway		Network Trusted Identity	MDR for Automotive	
Data Classification	Cloud Security Testing	Intrusion Prevention Service		OT PAM	Cyber Threat Hunting	
Data Protection	OT Security Testing	Data Loss Prevention		OT Endpoint Defense	DFIR Services	
Domain Advisory (Cloud, IAM, Data)	Secure Network Architecture Review	Endpoint Protection-aaS		Railway Security	Crisis management	
	Security Rating Services	Managed Endpoint Encryption Services			Tabletop Exercise Service	
	Compromise Assessment Service	Mobile Threat Defense			Digital Risk Protection Services	
	Social Engineering	Sovereign Cloud/ Cloud Encryption Services			External Attack Surface Management	
					Threat Intelligence	
					Compromise Assessment	
					Cyber Recovery	

Included in VITA MSS

Atos Next Gen SOC/MDR Service

From Threats to Resilience—Security Without Silos



PREVENT

- Vulnerability Management & Remediation
- Exposure Management & Remediation
- Policy Management & Remediation
- Digital Risk Protection

DETECT

- Threat Monitoring (Detection Rules, Signatures)
- Threat Hunting (AI & Hypothesis driven)
- Threat Intelligence (TI feeds, threat & vulnerability advisories)
- UEBA

RESPOND

- Incident Analysis (Automated triage, Playbooks)
- Automated & guided threat containment
- Customized playbooks
- Guided Remediation (Unlimited remediation support)
- DFIR

IMPROVE

- SOC Maturity Assessment
- Red Team /Purple Team Exercises
- Tabletop Exercises
- Compromise Assessment
- Breach & attack simulation (BAS)
- Singular Risk View

20+ years of Adaptive and Autonomous SOC experience

Platform-Agnostic & Modular MDR Solution

6500+ Security experts

17 SOCs

AIsaac Microsoft Sentinel Google SecOps splunk>enterprise CROWDSTRIKE & others

Atos

VIRGINIA IT AGENCY

Platform-Agnostic & Modular MDR Solution Models

	Detect	Respond	Client Portal
Model 1: MDR with AIsaac	■	■	■
Model 2: MDR with 3rd party technology and AIsaac as client portal	□ e.g., Microsoft Sentinel, Google SecOps	□	■
Model 3: MDR with 3rd party technology and AIsaac as automation layer and client portal	□ e.g., Splunk ES, IBM QRadar	■	■
Model 4: MDR fully delivered through 3rd party technology	□ e.g., CrowdStrike, Cortex XDR, Defender XDR, **Splunk**	□	□

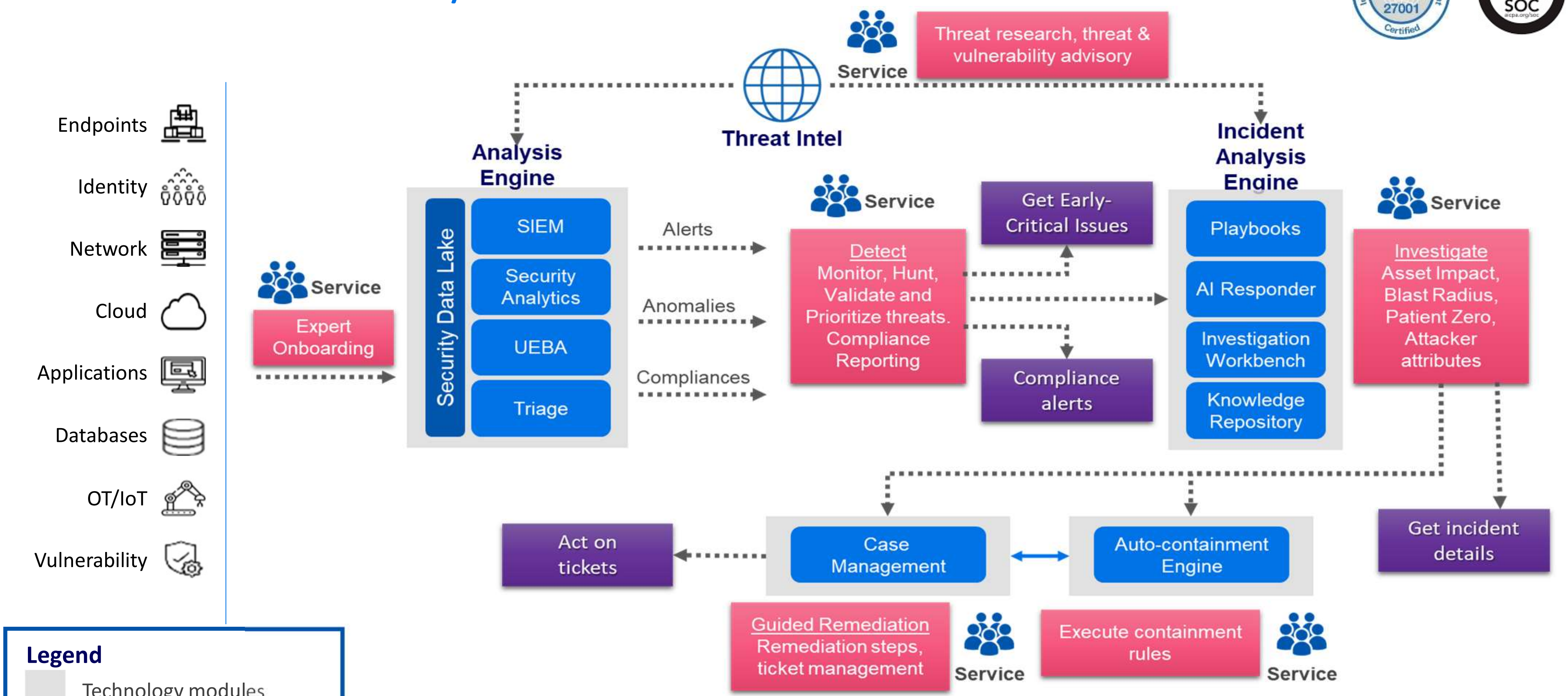
■ AIsaac □ 3rd Party Technology

"Our MDR adapts to customer needs—fully deploy our platform, enhance existing SIEM, XDR, EDR, and SOAR, or deliver end-to-end security leveraging investments in existing platforms"

Atos

How we deliver MDR/Next Gen SOC

SOC 2 TYPE II CERTIFIED



Legend

- ⬜ Technology modules
- 🟥 Service
- 🟪 Customer outcomes

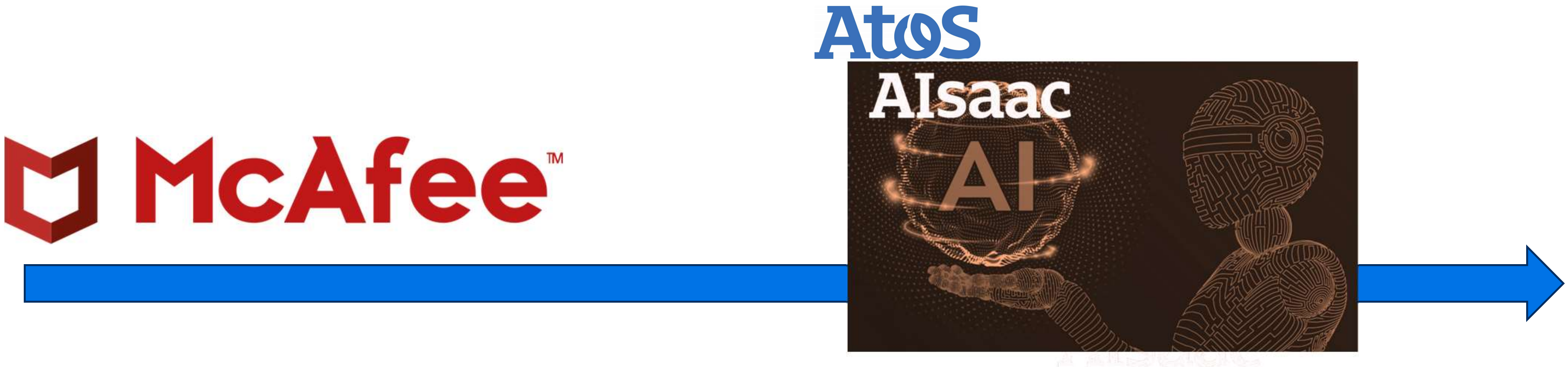
Singular Risk visualizations and customizations (Dashboards, Reporting)

Global and local governance models

Continuous improvement with expert teams: content engineering, content enrichment, model creation, playbooks, research, forensics, threat hunting…

Background

Evolution of the SIEM at VITA



2018 – Atos starts as VITA’s Managed Security Services Provider

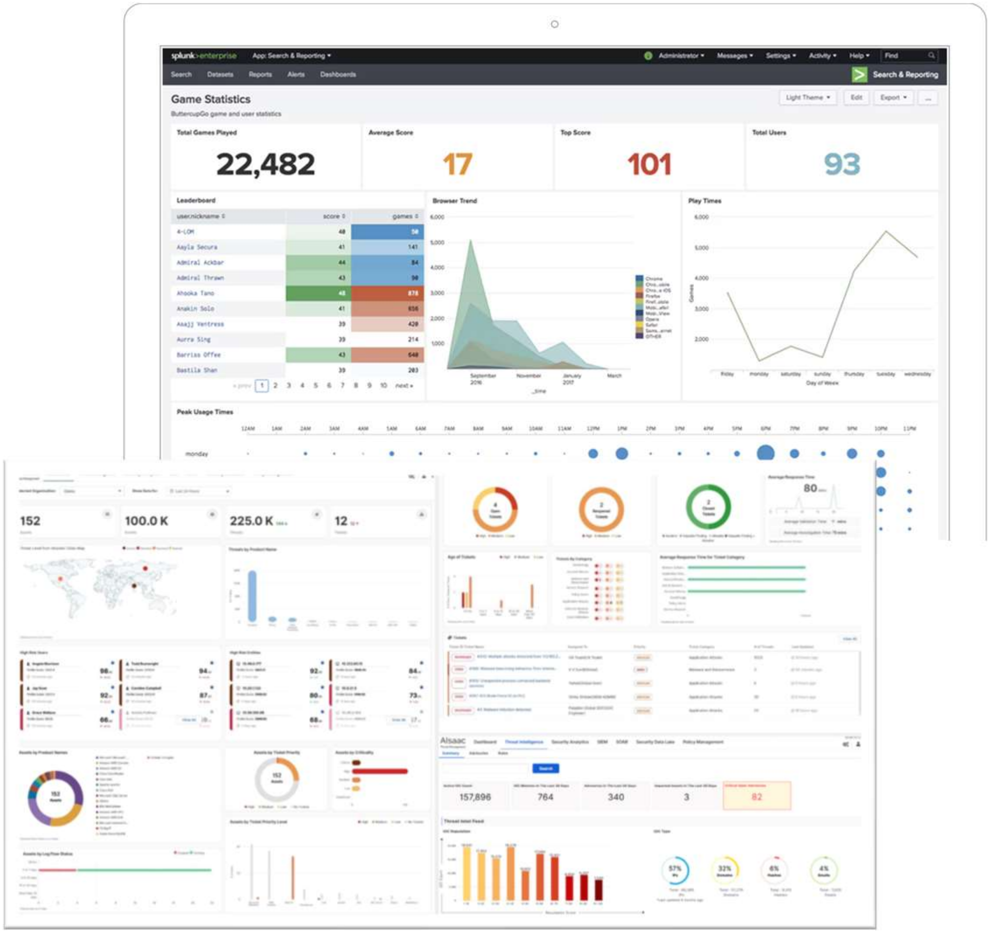
2022 – Atos converted VITA’s SIEM to AIsaac and our Managed Detection and Response Service

2020 – Atos acquisition of Paladion and it’s state-of-the-art AIsaac artificial intelligence (AI) platform for cyber analytics and hybrid SecOps

Splunk Added Late 2023 for Logging

Splunk and AIsaac working independently

- Application logs are directed to Splunk for centralized log management.
- Splunk enables application monitoring and troubleshooting capabilities.
- Security events are forwarded to AIsaac for advanced detection and response.
- AIsaac focuses on real-time threat detection and incident response.



Game Statistics

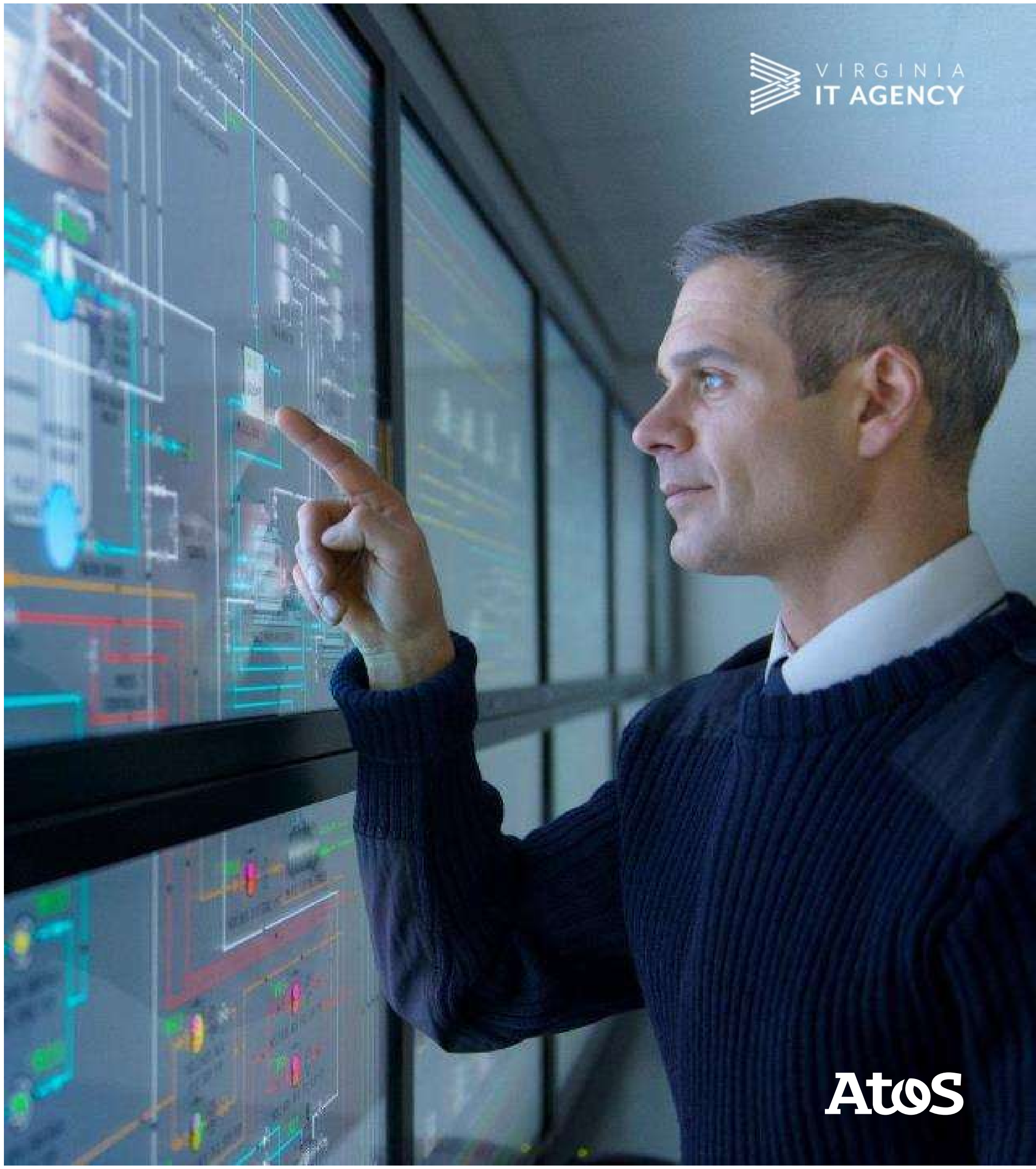
ButtercupGo game and user statistics

Total Games Played	Average Score	Top Score	Total Users
22,482	17	101	93

Leaderboard

user.nickname	score	games
4-LOM	48	58
Aayla Secura	41	141
Admiral Ackbar	44	84
Admiral Thrawn	43	98
Ahsoka Tano	48	878
Anakin Solo	41	656
Asajj Ventress	39	429
Aurra Sing	39	214
Barriss Offee	43	648
Bastila Shan	39	283

Project Overview



Project Goal

The objective of this project is to migrate all Atos AIssac data feeds and SOC support

to VITA's Splunk, ensuring a smooth transition from one system to another.

Migrating AIsaac to Splunk

Centralized Logging

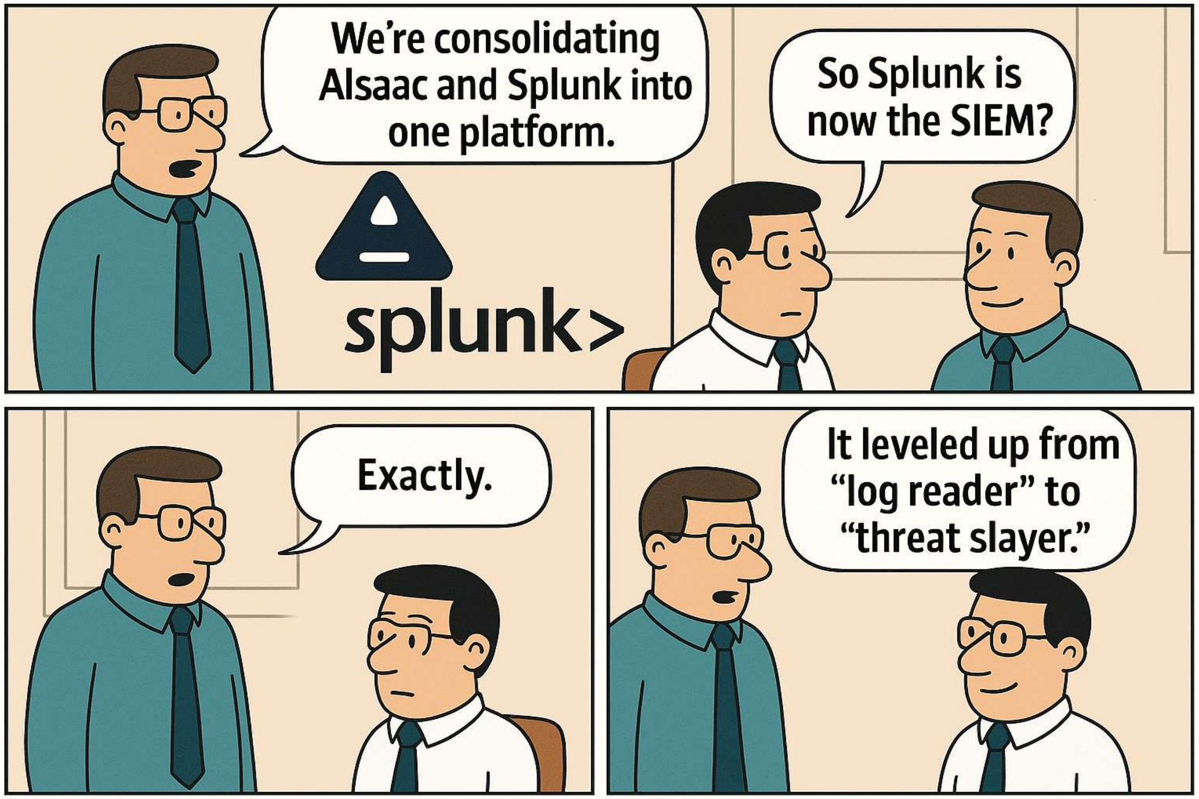
Splunk currently provides centralized logging. The addition of security information unifies data collection and simplifies monitoring and analysis.

Enhanced SIEM Capabilities

Splunk's advanced features with the additional log information improve threat detection, compliance, and overall security operations.

Scalable Infrastructure

The migration creates a robust, scalable infrastructure for both security and logging requirements.


We're consolidating AIsaac and Splunk into one platform.
splunk>
So Splunk is now the SIEM?
Exactly.
It leveled up from "log reader" to "threat slayer."

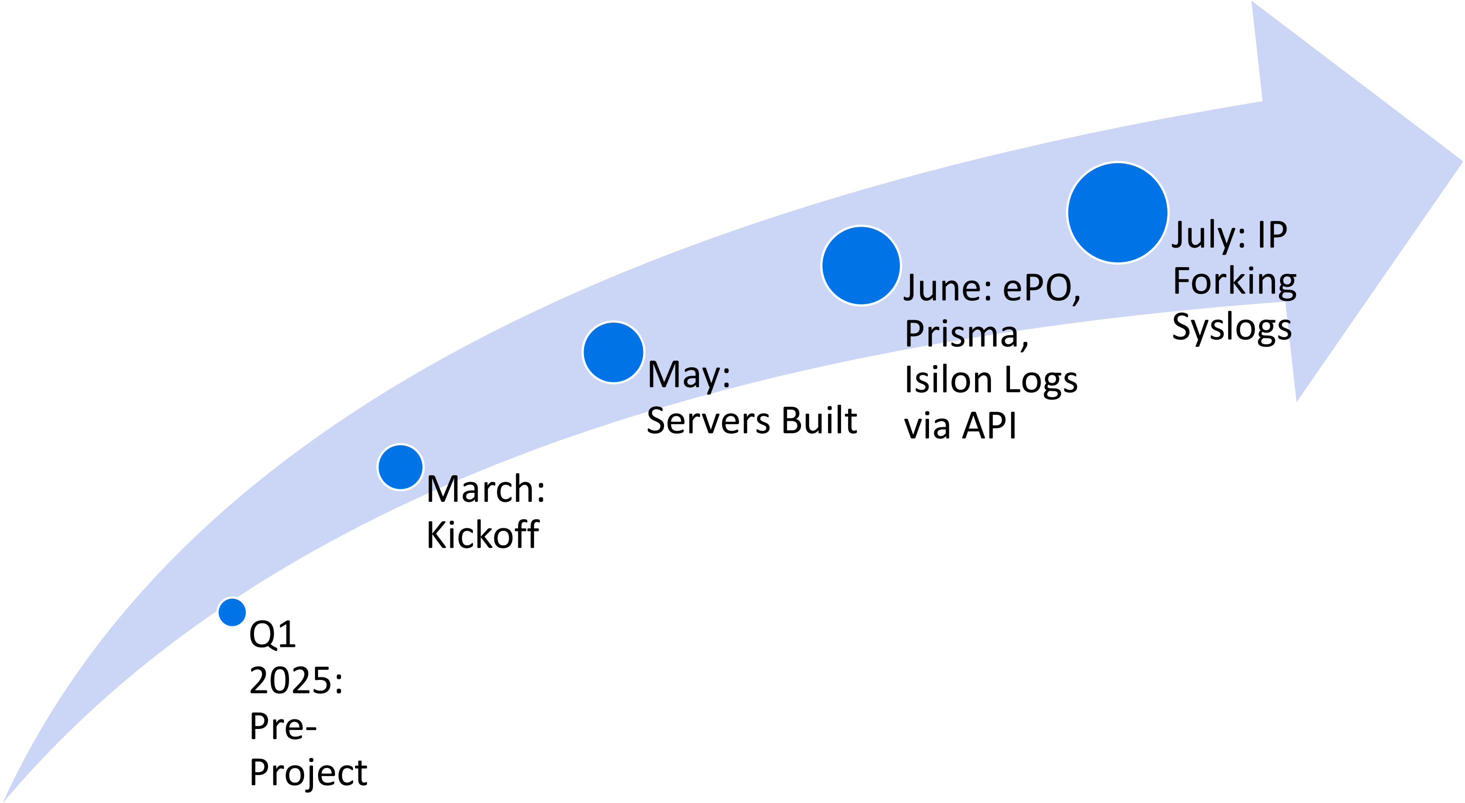
Expertise and Experience

Atos with NuHarbor – supporting the Commonwealth Splunk consolidation

- Global reach, U.S. focus
- 6+ years supporting VITA & Executive Branch agencies
- Extensive experience supporting multiple commercial, state, & local clients

Project Progress

Activities completed to data



Q1 2025: Pre-Project

March: Kickoff

May: Servers Built

June: ePO, Prisma, Isilon Logs via API

July: IP Forking Syslogs

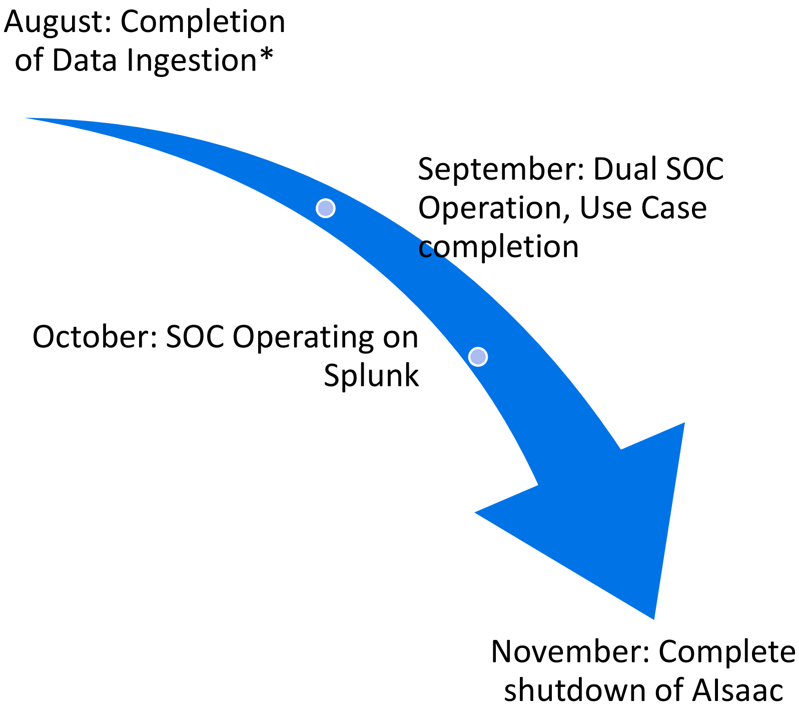
Current Status

As of 8/11/2025

- Overall progress: 73% complete
- Syslog/IP forking: Complete; dual-forwarding achieved.
- Server agent deployment: 73% complete (excepting Agency Splunk coverage)
- Recent technical issues:
  - - Duplicate firewall events causing inflated ingest.
  - - Ingestion latency; indexer expansion

Remaining High Level Plan

The last 20%...



August: Completion of Data Ingestion*

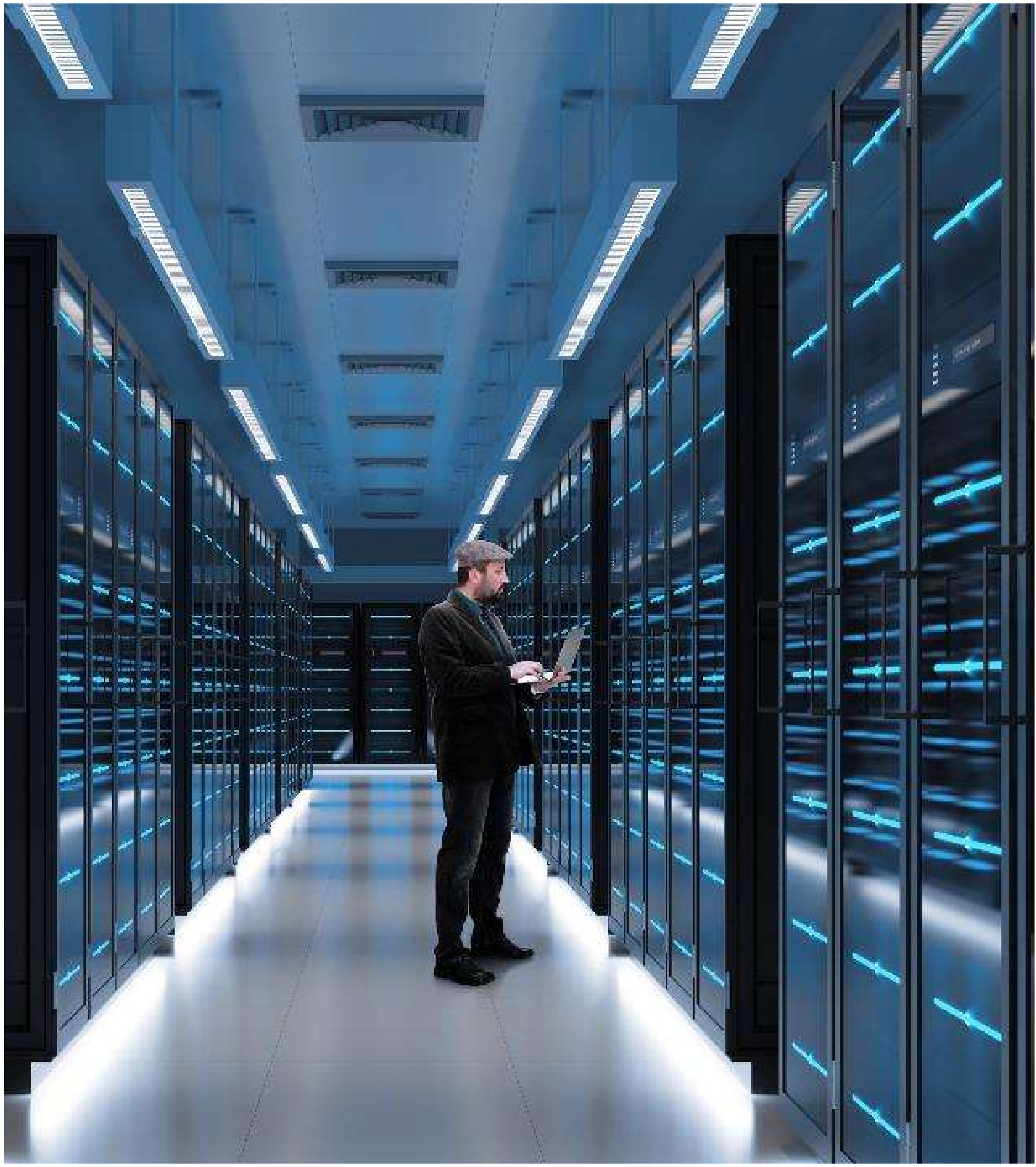
September: Dual SOC Operation, Use Case completion

October: SOC Operating on Splunk

November: Complete shutdown of AIsaac

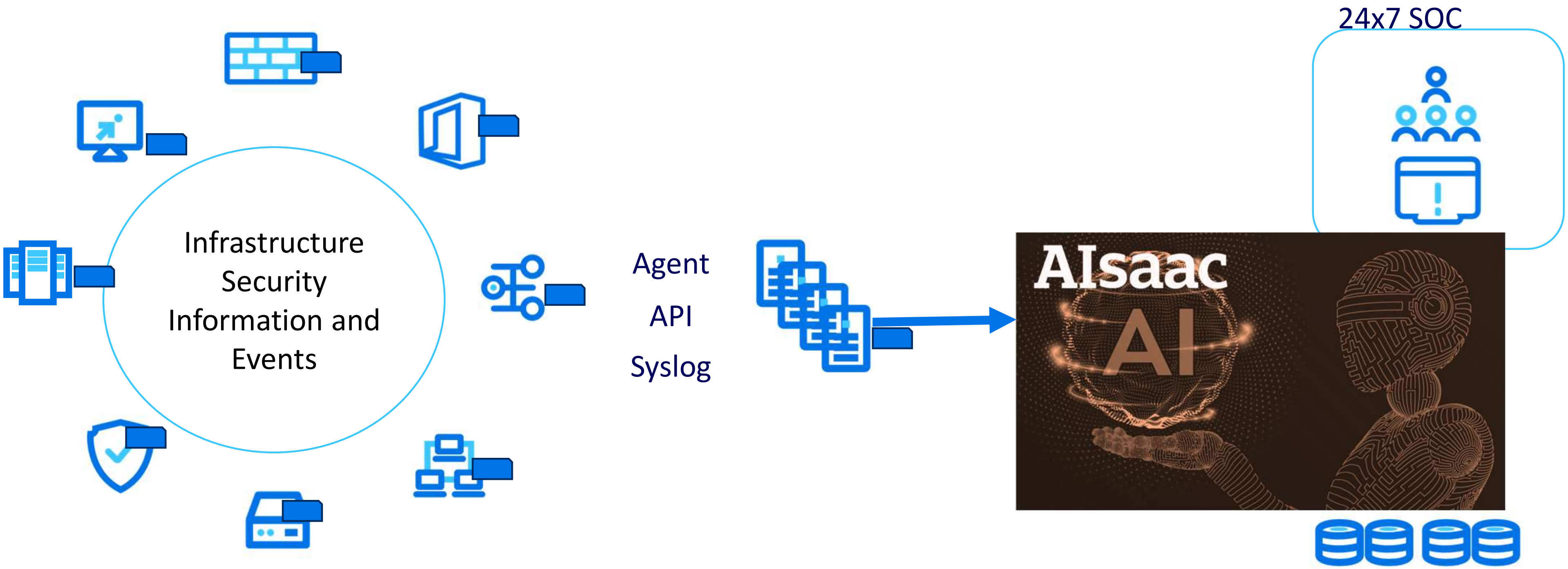
*Except Agency Splunk coverage TBD

Migration Approach



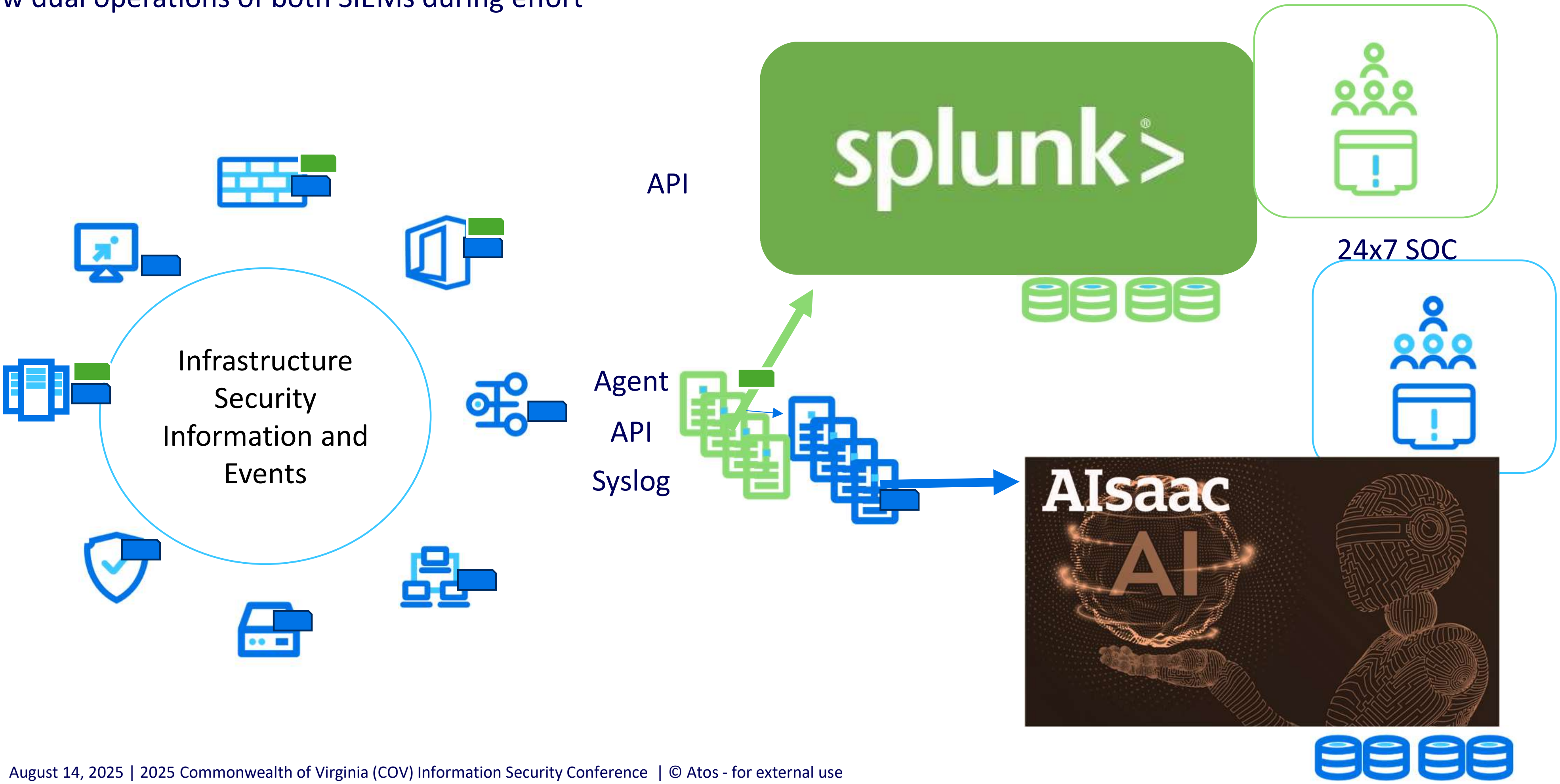
AIsaac Architecture

Security Information and Event forwarding and storage



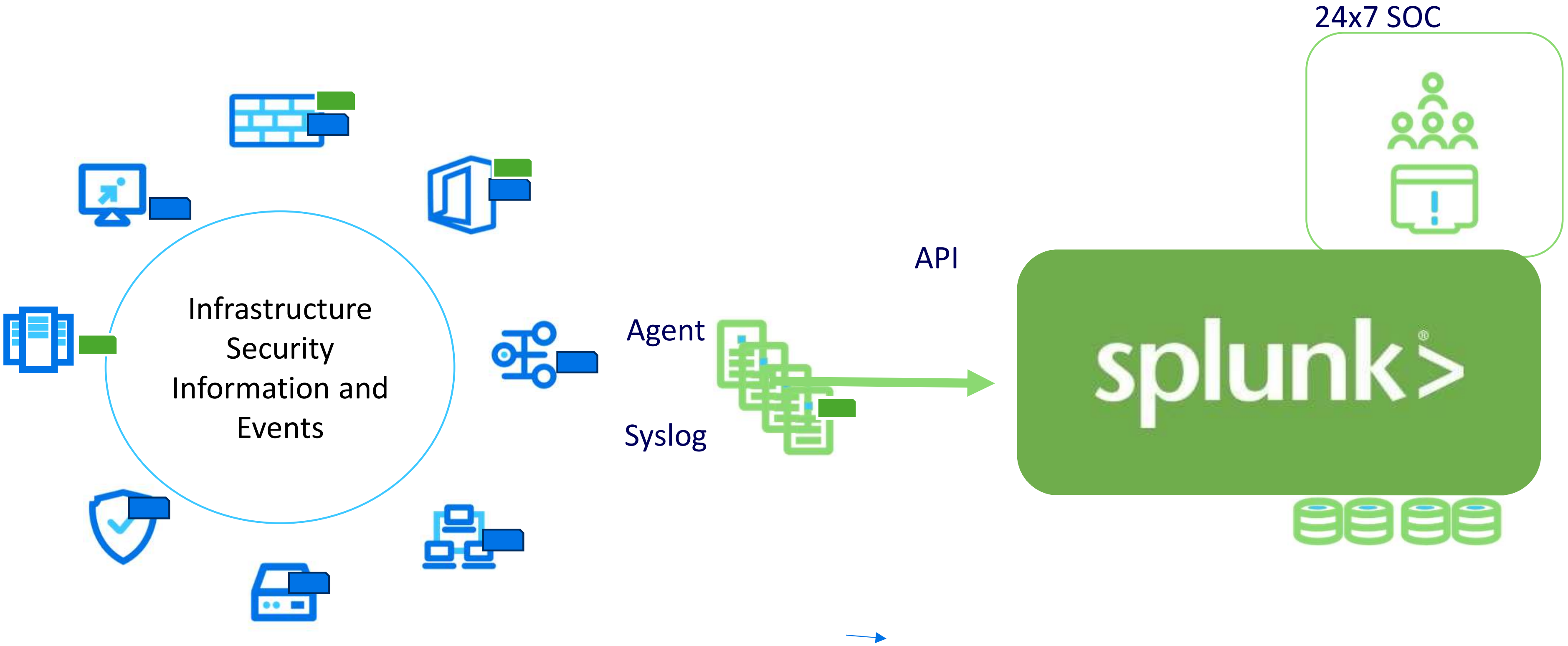
AIsaac and Splunk Architecture

Allow dual operations of both SIEMs during effort

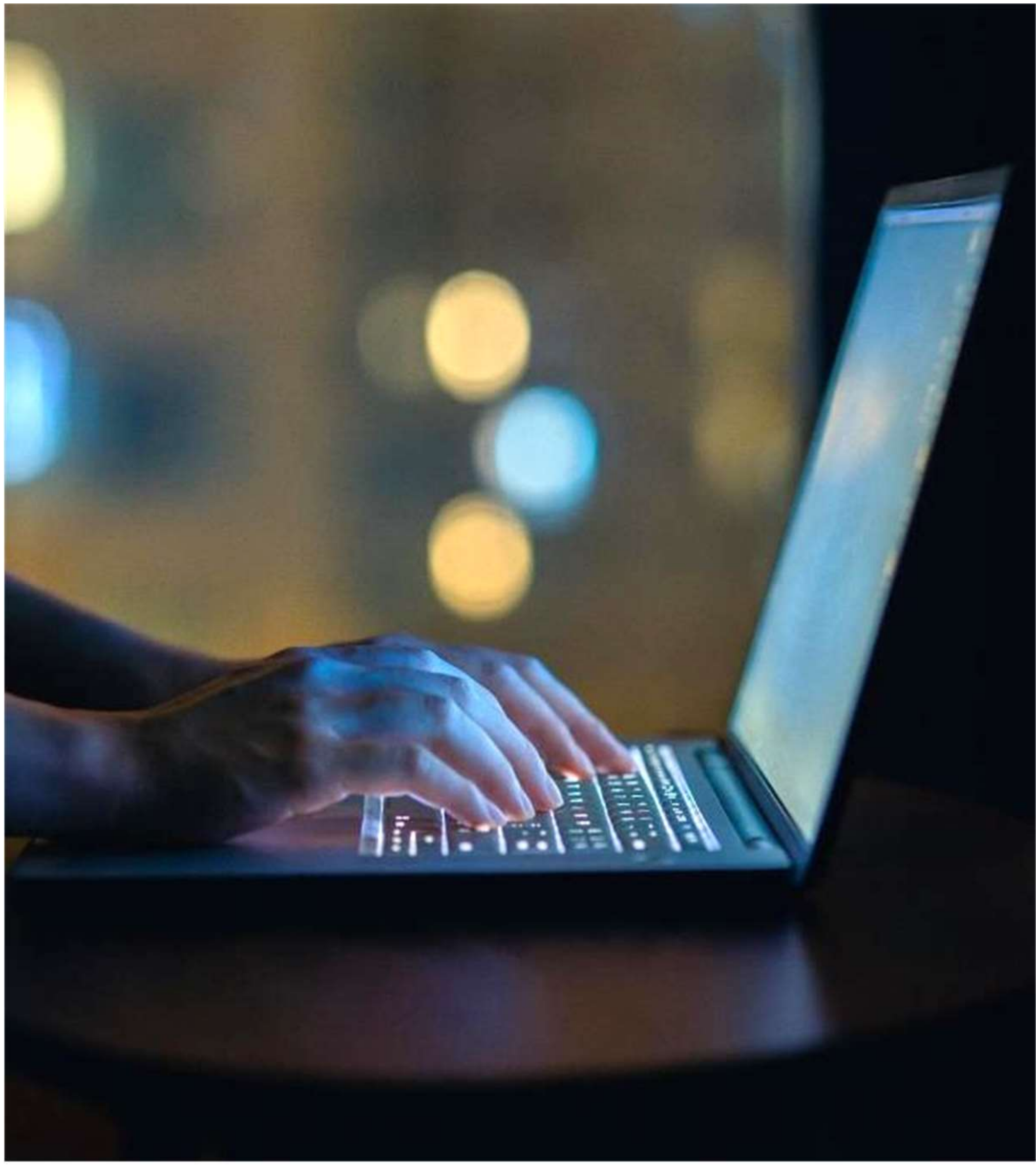


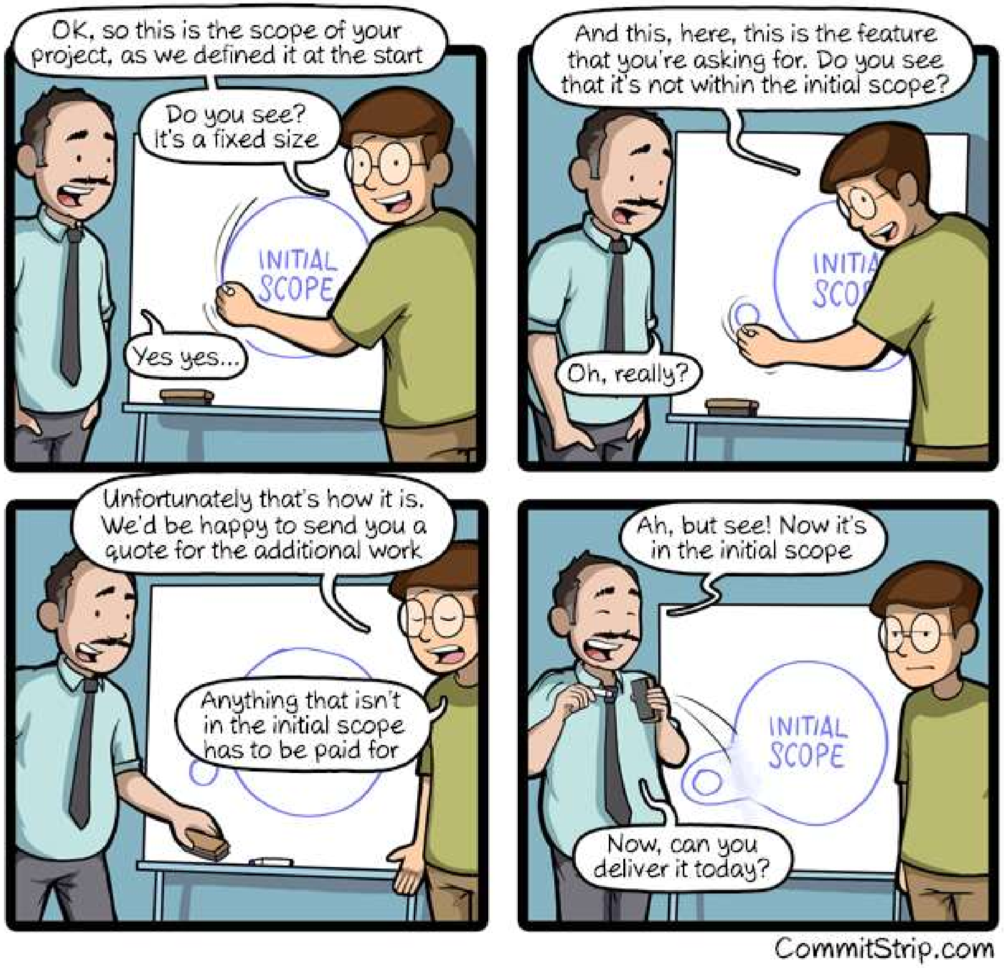
Splunk Architecture

Security Information and Event forwarding and Storage to Splunk only



Desired Outcomes

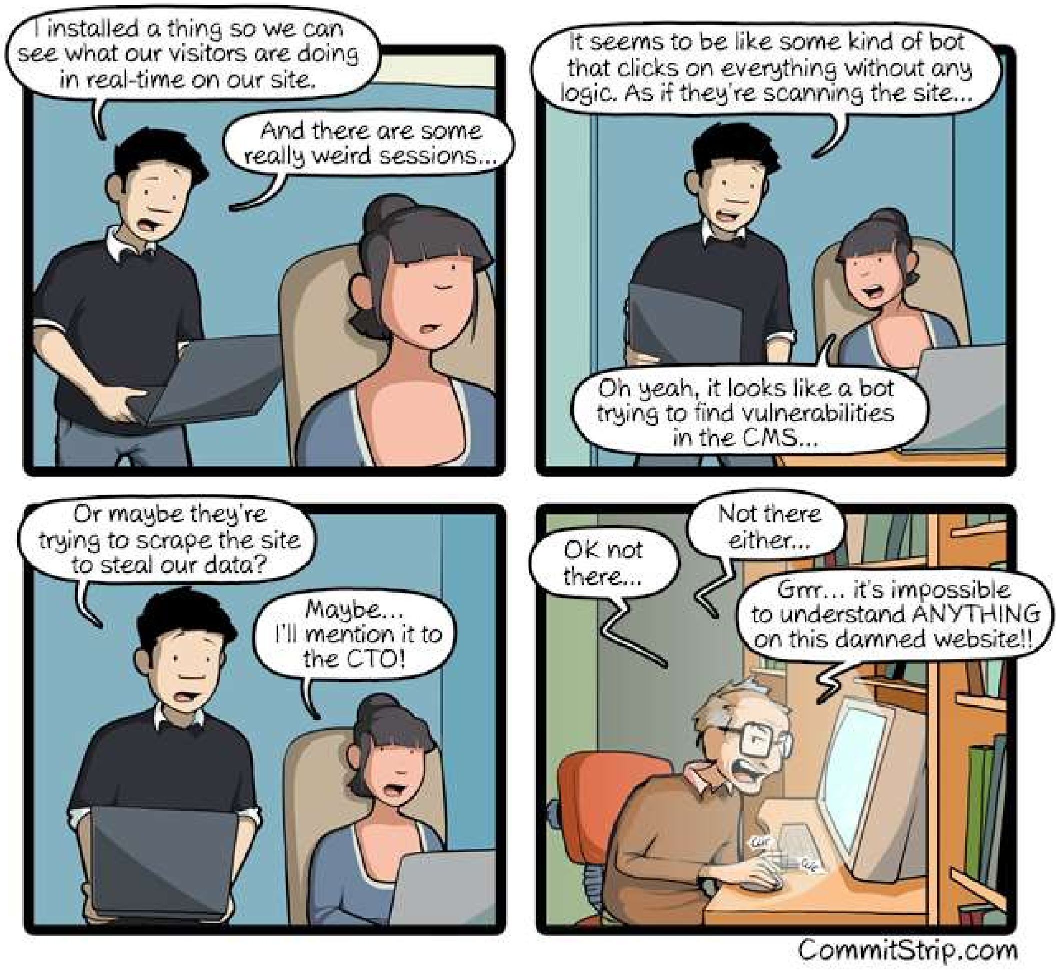



OK, so this is the scope of your project, as we defined it at the start
Do you see? It's a fixed size
INITIAL SCOPE
Yes yes...
And this, here, this is the feature that you're asking for. Do you see that it's not within the initial scope?
Oh, really?
Unfortunately that's how it is. We'd be happy to send you a quote for the additional work
Anything that isn't in the initial scope has to be paid for
Ah, but see! Now it's in the initial scope
INITIAL SCOPE
Now, can you deliver it today?
CommitStrip.com

Completion Criteria

How we know we are finished

- Suppliers have completed all related activities and tasks associated with Suppliers’ proposed scope of work or Customer has notified that the proposed Project can be closed out.
- Deployment of UBA and SOAR Configuration of ES, UBA, and SOAR Integration of data sources using Splunk Universal Forwarder (UF) or other methods. Data normalization and enrichment. Development of search queries for specific use cases (e.g., anomaly detection, threat hunting). Creation of dashboards and reports for visualization and reporting. Configuration of alerts based on predefined criteria. Integration with incident response tools (e.g., ticketing systems, SOAR platforms). Development of automated response actions for common threats. Should be modeled after MITRE ATT&CK Adherence to relevant compliance frameworks (e.g., PCI DSS, HIPAA, GDPR). Generation of compliance reports as required. The documentation of SMM manuals, administrative guides, and knowledge base articles.
- VITA Splunk is receiving / accepting format from Vanguard.
- Events from all devices reporting to AIssac are also received in Splunk.
- Feed to AIssac is closed.
- Testing completed to verify VITA Splunk is receiving/accepting format and feed to AIssac is closed.
- Existing sources are configured to forward logs to VITA Splunk, search queries, dashboards, and reports for real-time monitoring, threat hunting, and incident investigation are developed and deployed. Other alerts, playbooks, and integration with incident response tools for automated actions are completed.


I installed a thing so we can see what our visitors are doing in real-time on our site.
And there are some really weird sessions...
It seems to be like some kind of bot that clicks on everything without any logic. As if they're scanning the site...
Oh yeah, it looks like a bot trying to find vulnerabilities in the CMS...
Or maybe they're trying to scrape the site to steal our data?
Maybe... I'll mention it to the CTO!
OK not there...
Not there either...
Grrr... it's impossible to understand ANYTHING on this damned website!!
CommitStrip.com

Security Monitoring Service Details

VIRGINIA IT AGENCY

Health Check

- Assessment of desired security outcomes, gaps, & optimal data ingestion strategy
- Actionable recommendations within Splunk

Consistent Tuning

- Security reviews for improvement of alerts, workbooks, & playbooks
- A cycle that ensures security alerts & incidents become continually more efficiently manageable

Daily Environment Reviews

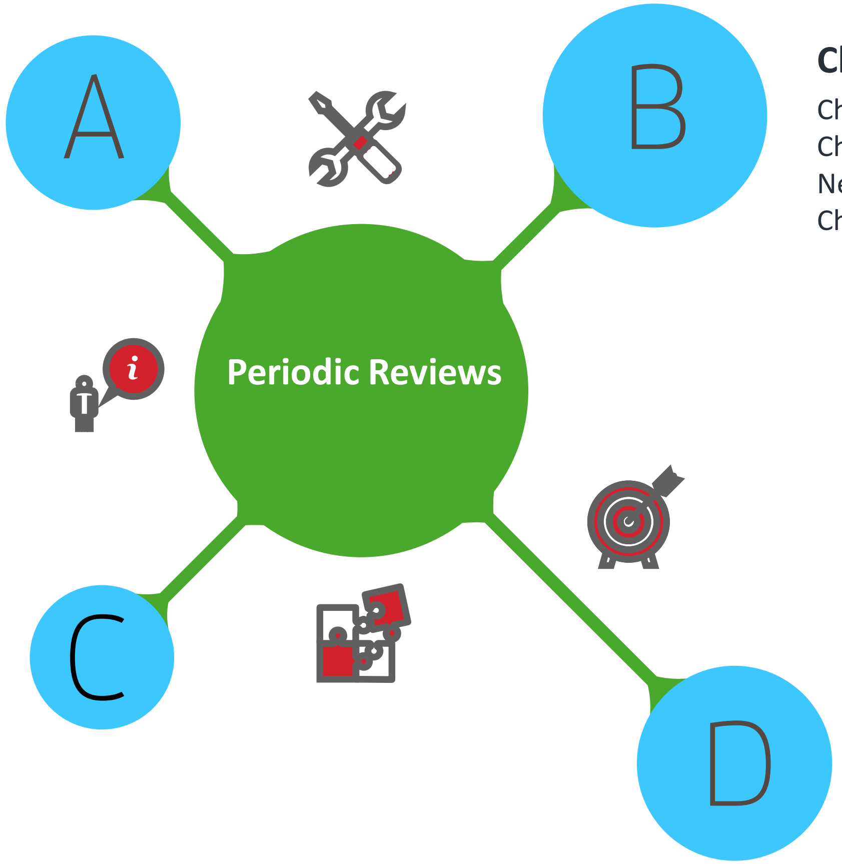
- Daily expert review of the Splunk environment, including anomalies
- Filtering of false positives, identification of possible threats, & escalations of valid incidents

Rapid Investigation & Remediation Strategies

- Contextual expert analysis of threats for proactive protection & effective remediation support
- Management of threats/vulnerabilities that go beyond alerts not prioritized by Splunk

Continual Improvement – Security Monitoring

Runbook / Use case maintenance



Threat Intelligence Inputs

Threat & Vulnerability Advisories
Breaches & Hacks
IOC Feeds

Change in Business Environment

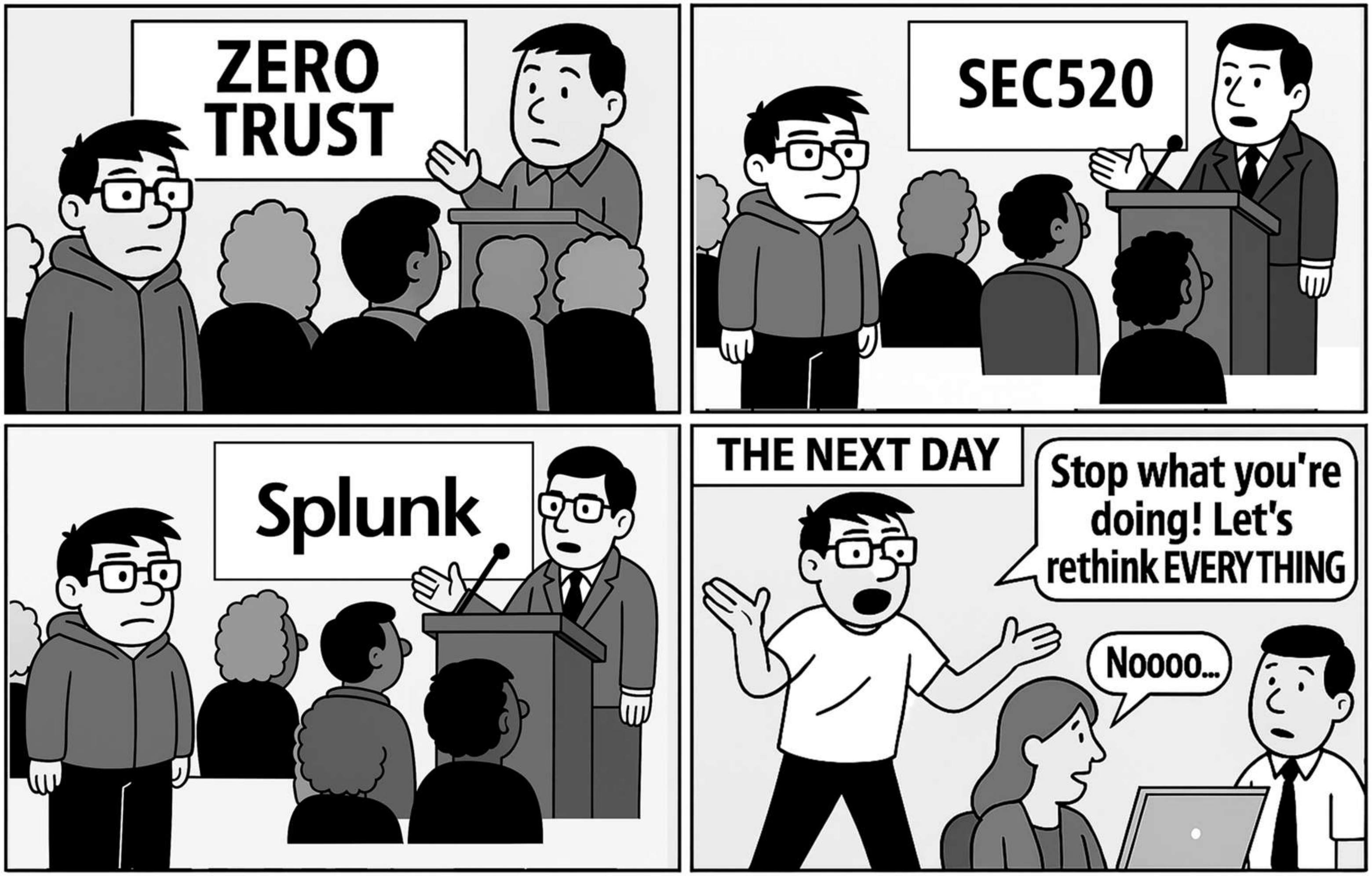
Change in Compliance Directives
Change in Business Process
New Business Initiative, Process, Technology
Change in Third Party Vendor, Partner

Change in User information

List of Top Management, Resigned Staff etc.
Administrator, Roles etc.

MDR Customer Community

New Use cases developed


ZERO TRUST
SEC520
Splunk
THE NEXT DAY
Stop what you're doing! Let's rethink EVERYTHING
Noooo...

Questions?

VIRGINIA IT AGENCY

Atos

VIRGINIA IT AGENCY

For more questions, please contact:
Kevin McLees, Atos Account Executive
Kevin.McLees@atos.net
(804) 301-1430

Atos Group is deploying safe and responsible AI solutions (internal and/or 3rd party based) for the internal use by its employees, collaborators and advisors when developing and delivering products and/or services to its customers as well as when and offering AI based solutions. A specific policy has been deployed across all the Group employees to ensure the protection of the confidentiality and the security of own data and our customers' data through the use of solutions vetted by our legal, security and data protection teams.

Additionally, the Group offers professional services that can help companies to understand requirements, to anticipate legislations applicable to AI, and to be better prepared to achieve compliance with those AI regulations as they are adopted.

Atos