ONAPSIS

DISRUPTIVE TECHNOLOGY

HOW DOW CHEMICAL LEVERAGES CYBERSECURITY TECHNOLOGY FOR INTERNAL AUDIT AND COMPLIANCE

BRIAN TREMBLAY
COMPLIANCE PRACTICE LEADER

AGENDA

01. Quick Cybersecurity & Compliance Environment Update

02. Overlap (and challenges) of Managing Cybersecurity & Compliance

03. Common Cyber Technologies and What They Do

04. How Dow Manages Cyber & Compliance

05. Sample Use Cases

LEARNING OBJECTIVES

In this session, participants will:

- Explore technologies used by information security that can deliver value to internal audit.
- Examine the capabilities of these technologies and understand how they can be utilized.
- Hear how Dow Chemical’s information security team leverages these technologies for both security and compliance/audit support.
- Learn what actions internal audit can take to understand and leverage these technologies.

QUICK CYBERSECURITY & COMPLIANCE UPDATE

KEY TAKEAWAY | IT'S COMING FAST, FURIOUS AND WITH A HEAVIER HAND

- Cyber Security – Increasing Expectations
  - 2011: First formal communication from SEC on Cyber Disclosure Guidance
  - 2018: SEC releases interpretive guidance on Cyber
  - 2022: SEC proposes rules on Cyber Disclosures
  - Future: SEC proposes rules on Cyber & ICFR
- Pressure on the auditors:
  - Internal Specialists,
  - 3rd Parties,
  - Technology (both organizations and auditors) including Digital Assets
  - Data, data and more data
- Enforcement actions are on the rise – and so are the costs
  - Accountability is also on the rise
  - FINRA Rule 3310 (2015): CCO liability is now in the news
- Specialized/Technical topics are becoming more frequent in the name of greater transparency
- Organizations will continue to face more specific scrutiny and will need to have technical expertise

OVERLAP (AND CHALLENGES) OF MANAGING CYBER & COMPLIANCE

THE INTERSECTION

- What Threat Actors Want, The Regulators Mandate Be Protected
  - And the regulators know it!

- Example:
  - Cyber defense seeks prevents unauthorized access to systems which is exactly what threat actors do first via provisioning them self high-privileged roles/access
  - So does ITGC for SOX ICFR
  - So does GDPR
  - So does HIPAA

- Access Control Risk and the associated controls is paramount to solving these challenges

- GRC & InfoSec & IT Alignment Critical to success – more to come!

COMMON CYBER TECHNOLOGIES AND WHAT THEY DO

WHAT IS OUT THERE

The list is long and complex……..

- End-point
  - Anti-Virus, Firewall, etc.
- Network
  - VPN, Firewall, Intrusion Detection System, etc.
- Authentication & Access
  - Passwords, Multi-Factor Authentication, etc.
- Encryption
- And more…..

WHAT THEY DO

Interestingly…….some overlap

- End-point
  - Prevention, Threat detection, Detect & Respond, etc.
- Network
  - Prevention, Threat detection, Detect & Respond, etc.
- Authentication & Access
  - Prevention, Detect & Respond, etc.
- Encryption
  - Prevention

GRC PAINS & SOLUTIONS

COMMON CHALLENGES

- Business & Technology Complexity
  - Keeping pace is nearly impossible
- Hiring & Retaining Talent
- Proliferation of Information
- Adhering to Laws & Regulations
  - Illustrating Assurance Activities i.e. are you in compliance
- Manual Nature of the work
- Identifying & Implementing Process & Technology
- Determining a ‘single source of GRC truth’
- Risk Assessment Expertise & Depth
- Timely Identification of Risks Manifesting/Deviations

SOLVABLE TODAY

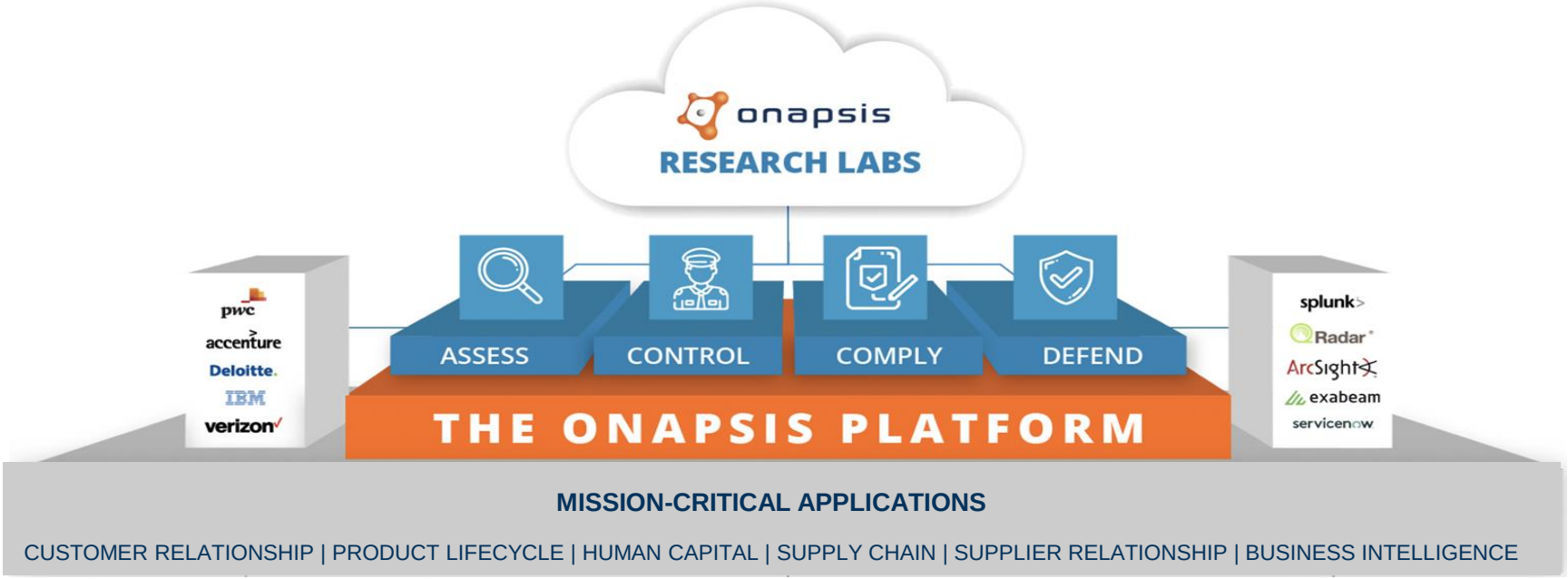
- Aggregating Information in single audit management solutions for a ‘single source of truth’
  - Automation of key administrative tasks (approvals, certifications, etc.)
- Pseudo-automation of compliance activities
  - Also technologies like RPA but that provides as much risk as benefit

Not Widely Solvable (or are they?)

- Continuous Monitoring
- Continuous Auditing
- Managing the testing cycle and doing the work
- Remediation Activities
- Hiring & Retaining Talent

HOW DOW MANAGES CYBER & COMPLIANCE

THE ONAPSIS PLATFORM OVERVIEW

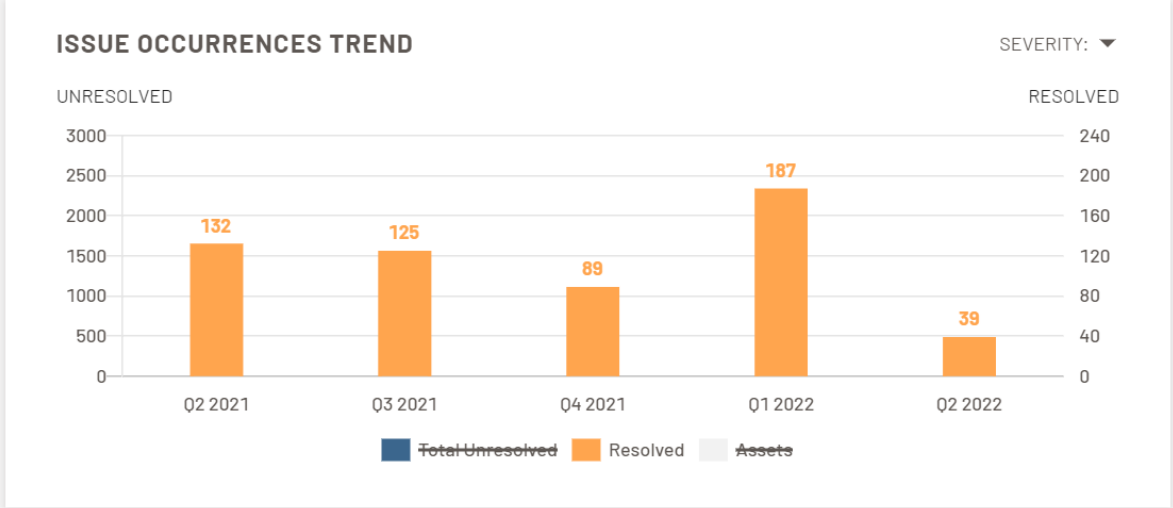


ONAPSIS SECURITY PLATFORM (OSP)

- Vulnerability Scans (Assess)
  - Authorization
  - Configuration
  - Missing Patches
- Compliance Audits (Comply)
- Real-Time Monitoring (Defend)

OSP IN ACTION

226 critical or high vulnerability instances remediated in 2022



ONAPSIS SCOPE

- SAP middleware supporting:
  - SAP BW, ECC, GRC, Solution Manager, and other ERP components
- SAP ABAP & Java NetWeaver
- SAP HANA Databases
  - SAP BW, CDS, and EDH
  - Managed by Dow team in Azure
  - Was previously managed by SAP in HANA Enterprise Cloud (HEC)

Key takeaway – the vast majority of our traditional security teams and toolsets do not operate at this layer

ONAPSIS USE CASES

- Compliance (ICFR/SOX)
  - Patch & Vulnerability Management
  - Default Account/Profile Management
  - Role-based Access Control governance
  - Security Parameter Settings
- Continuous Audit / Monitoring
  - Key controls are monitored in near real-time
    - Integration to SIEM, functional email accounts, etc.
  - Internal/External Audit Reliance
- Business Use Cases
  - Business Controls for other SAP workstreams (pilot for P2P currently underway)
  - Currently partnered with Dow Controllers function and Onapsis to deliver a broader pilot across SAP workstreams

ONAPSIS USE CASES (CONTINUED)

- Cyber Security Threat Detection & Mitigation
  - Alarm profiles alert for active exploits
  - SAP Recon, Log4J, ICMAD
- Assurance for new ERP builds/projects
  - Migration of SAP BW from SAP HEC to Azure
  - New SAP client delivery or future platform upgrades
- Future:
  - SAP Business Controls
  - Move other use cases to the Defend module

IMPACT

- **Proactive Cyber Security Program for ERP**
  - Full-scope vulnerability scans 2x monthly
  - Transparency to SAP Patch & Vulnerability Management data
  - Reduction in vulnerability exposure window
  - Real-time monitoring and notification capability for critical SAP controls
  - Notification of zero-day threats from Onapsis, with detailed security workarounds and monitoring signatures for Onapsis detection
- **Complete, Accurate & Efficient Compliance Efforts**
  - Automation of critical ICFR/SOX Governance Activities
  - Providing continuous control audit/monitoring services
  - Reduction of time/effort for IT, IS, IA, etc.

INTERNAL & EXTERNAL AUDIT RELIANCE

- Dow Internal Audit
  - RBAC Governance: 1,000+ hr. audit reduced to dozens of hours PLUS more complete & accurate results
  - >10 Controls replaced by platform
- External audit reliance of RBAC process for SSAE16 SOC
  - Onapsis ITGC (application and platform)
  - Data Integrity (IPE)
  - Change control
  - Focus on remediation efforts and timeliness
  - Sampling for critical controls

EXAMPLE USE CASES

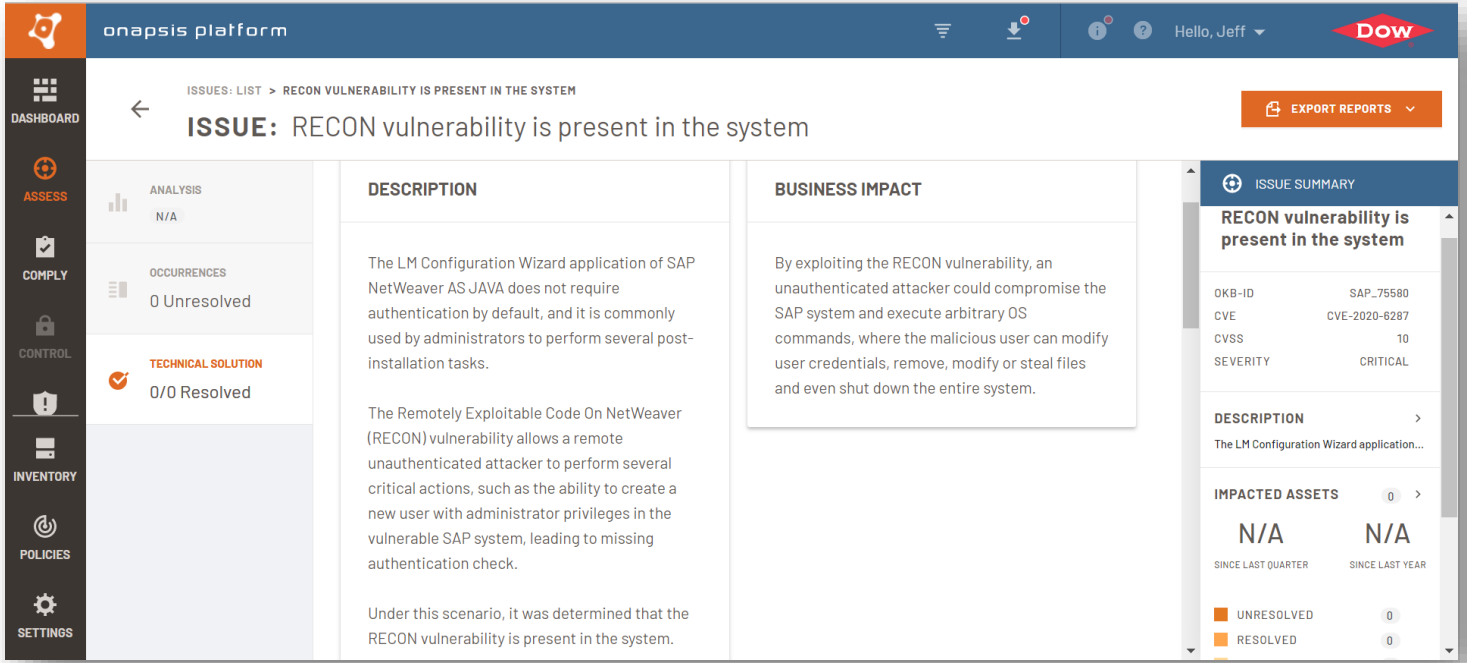
USE CASES

- Zero-day Threat Remediation & Exploit Monitoring (SAP RECON)
- Privileged Access Monitoring
- Self-Provision of Access
- Role-Based Access Governance

SAP RECON

- Remotely Exploitable Code On NetWeaver
- Default component present in every SAP application running NetWeaver JAVA
- CVSS 10.0
- Security Workarounds
  - Deactivating the application aliases
  - Stopping the vulnerable application
  - Enabling authentication for the vulnerable service
- SAP Note 2934135

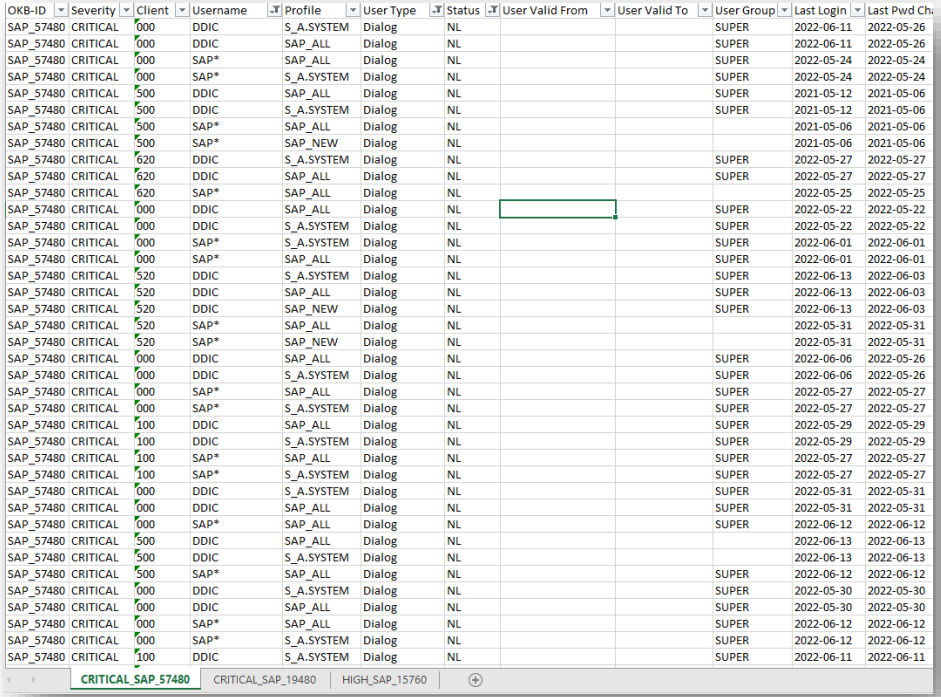
SAP RECON



SAP RECON

- Dow implemented a combination of security workarounds
- Shortly thereafter implemented SAP Note 2934135
- Onapsis Defend incident profiles for exploit detection

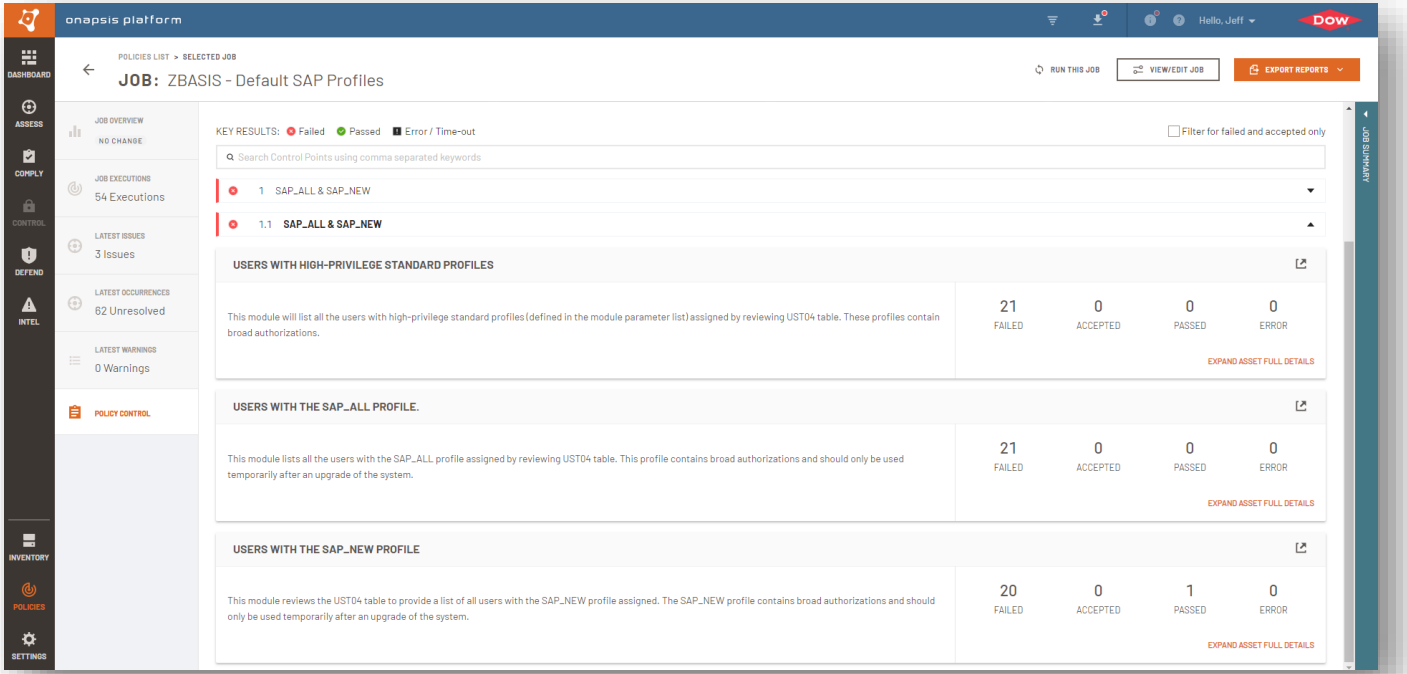
SAP PRIVILEGED ACCESS MONITORING



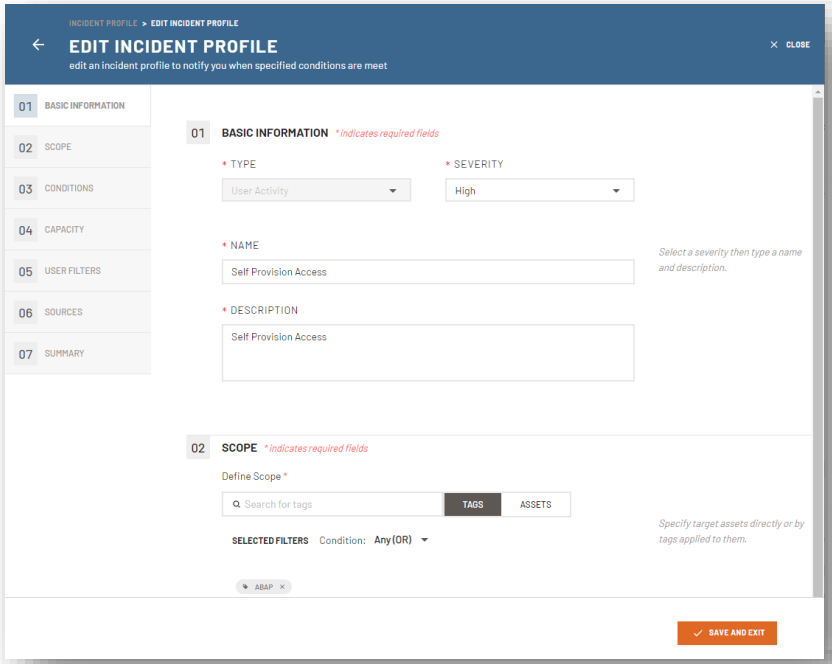
OKB-ID	Severity	Client	Username	Profile	User Type	Status	User Valid From	User Valid To	User Group	Last Login	Last Pwd Ch
SAP_57480	CRITICAL	000	DDIC	S_A.SYSTEM	Dialog	NL			SUPER	2022-06-11	2022-05-26
SAP_57480	CRITICAL	000	DDIC	SAP_ALL	Dialog	NL			SUPER	2022-06-11	2022-05-26
SAP_57480	CRITICAL	000	SAP*	SAP_ALL	Dialog	NL			SUPER	2022-05-24	2022-05-24
SAP_57480	CRITICAL	000	SAP*	S_A.SYSTEM	Dialog	NL			SUPER	2022-05-24	2022-05-24
SAP_57480	CRITICAL	500	DDIC	SAP_ALL	Dialog	NL			SUPER	2021-05-12	2021-05-06
SAP_57480	CRITICAL	500	DDIC	S_A.SYSTEM	Dialog	NL			SUPER	2021-05-12	2021-05-06
SAP_57480	CRITICAL	500	SAP*	SAP_ALL	Dialog	NL				2021-05-06	2021-05-06
SAP_57480	CRITICAL	500	SAP*	SAP_NEW	Dialog	NL				2021-05-06	2021-05-06
SAP_57480	CRITICAL	620	DDIC	S_A.SYSTEM	Dialog	NL			SUPER	2022-05-27	2022-05-27
SAP_57480	CRITICAL	620	DDIC	SAP_ALL	Dialog	NL			SUPER	2022-05-27	2022-05-27
SAP_57480	CRITICAL	620	SAP*	SAP_ALL	Dialog	NL				2022-05-25	2022-05-25
SAP_57480	CRITICAL	000	DDIC	SAP_ALL	Dialog	NL			SUPER	2022-05-22	2022-05-22
SAP_57480	CRITICAL	000	DDIC	S_A.SYSTEM	Dialog	NL			SUPER	2022-05-22	2022-05-22
SAP_57480	CRITICAL	000	SAP*	S_A.SYSTEM	Dialog	NL			SUPER	2022-06-01	2022-06-01
SAP_57480	CRITICAL	000	SAP*	SAP_ALL	Dialog	NL			SUPER	2022-06-01	2022-06-01
SAP_57480	CRITICAL	520	DDIC	S_A.SYSTEM	Dialog	NL			SUPER	2022-06-13	2022-06-03
SAP_57480	CRITICAL	520	DDIC	SAP_ALL	Dialog	NL			SUPER	2022-06-13	2022-06-03
SAP_57480	CRITICAL	520	DDIC	SAP_NEW	Dialog	NL			SUPER	2022-06-13	2022-06-03
SAP_57480	CRITICAL	520	SAP*	SAP_ALL	Dialog	NL				2022-05-31	2022-05-31
SAP_57480	CRITICAL	520	SAP*	SAP_NEW	Dialog	NL				2022-05-31	2022-05-31
SAP_57480	CRITICAL	000	DDIC	SAP_ALL	Dialog	NL			SUPER	2022-06-06	2022-05-26
SAP_57480	CRITICAL	000	DDIC	S_A.SYSTEM	Dialog	NL			SUPER	2022-06-06	2022-05-26
SAP_57480	CRITICAL	000	SAP*	SAP_ALL	Dialog	NL			SUPER	2022-05-27	2022-05-27
SAP_57480	CRITICAL	000	SAP*	S_A.SYSTEM	Dialog	NL			SUPER	2022-05-27	2022-05-27
SAP_57480	CRITICAL	100	DDIC	SAP_ALL	Dialog	NL			SUPER	2022-05-29	2022-05-29
SAP_57480	CRITICAL	100	DDIC	S_A.SYSTEM	Dialog	NL			SUPER	2022-05-29	2022-05-29
SAP_57480	CRITICAL	100	SAP*	SAP_ALL	Dialog	NL			SUPER	2022-05-27	2022-05-27
SAP_57480	CRITICAL	100	SAP*	S_A.SYSTEM	Dialog	NL			SUPER	2022-05-27	2022-05-27
SAP_57480	CRITICAL	000	DDIC	S_A.SYSTEM	Dialog	NL			SUPER	2022-05-31	2022-05-31
SAP_57480	CRITICAL	000	DDIC	SAP_ALL	Dialog	NL			SUPER	2022-05-31	2022-05-31
SAP_57480	CRITICAL	000	SAP*	SAP_ALL	Dialog	NL			SUPER	2022-06-12	2022-06-12
SAP_57480	CRITICAL	500	DDIC	SAP_ALL	Dialog	NL				2022-06-13	2022-06-13
SAP_57480	CRITICAL	500	DDIC	S_A.SYSTEM	Dialog	NL				2022-06-13	2022-06-13
SAP_57480	CRITICAL	500	SAP*	SAP_ALL	Dialog	NL			SUPER	2022-06-12	2022-06-12
SAP_57480	CRITICAL	000	DDIC	S_A.SYSTEM	Dialog	NL			SUPER	2022-05-30	2022-05-30
SAP_57480	CRITICAL	000	DDIC	SAP_ALL	Dialog	NL			SUPER	2022-05-30	2022-05-30
SAP_57480	CRITICAL	000	SAP*	SAP_ALL	Dialog	NL			SUPER	2022-06-12	2022-06-12
SAP_57480	CRITICAL	000	SAP*	S_A.SYSTEM	Dialog	NL			SUPER	2022-06-12	2022-06-12
SAP_57480	CRITICAL	100	DDIC	S_A.SYSTEM	Dialog	NL			SUPER	2022-06-11	2022-06-11

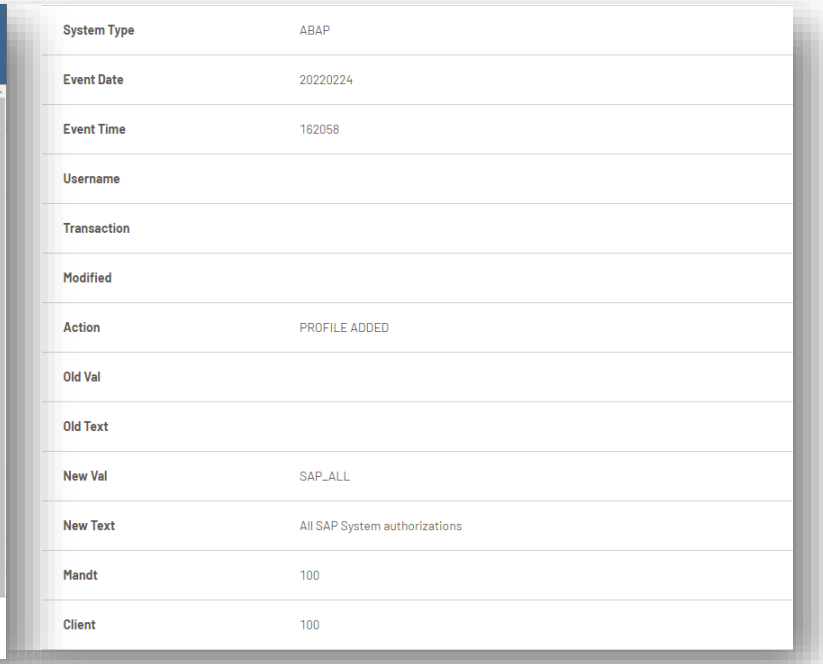
CRITICAL_SAP_57480 | CRITICAL_SAP_19480 | HIGH_SAP_15760

SAP PRIVILEGED ACCESS MONITORING



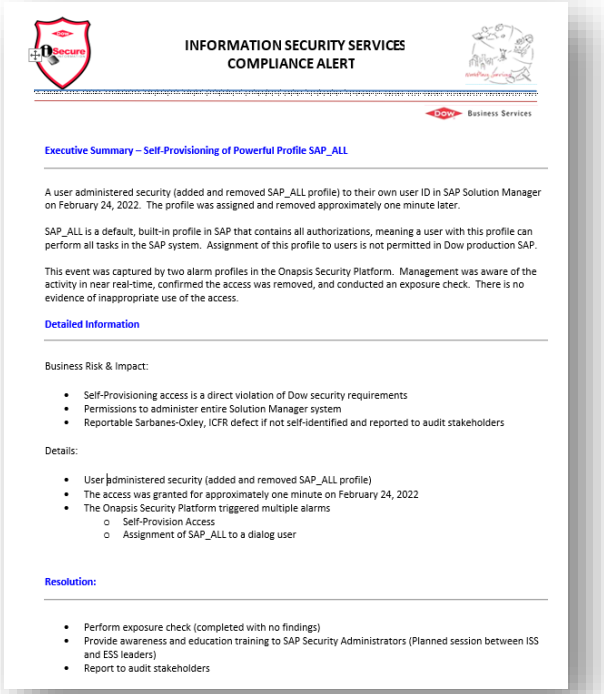
ONAPSIS DEFEND – SELF PROVISION OF ACCESS





REAL-TIME RISK DETECTION

- Detection of administrator elevating privilege
  - Identify
  - Exposure check
  - Avoid ICFR business issue
  - Deter behavior



INFORMATION SECURITY SERVICES
COMPLIANCE ALERT

Dow Business Services

Executive Summary – Self-Provisioning of Powerful Profile SAP_ALL

A user administered security (added and removed SAP_ALL profile) to their own user ID in SAP Solution Manager on February 24, 2022. The profile was assigned and removed approximately one minute later.

SAP_ALL is a default, built-in profile in SAP that contains all authorizations, meaning a user with this profile can perform all tasks in the SAP system. Assignment of this profile to users is not permitted in Dow production SAP.

This event was captured by two alarm profiles in the Onapsis Security Platform. Management was aware of the activity in near real-time, confirmed the access was removed, and conducted an exposure check. There is no evidence of inappropriate use of the access.

Detailed Information

Business Risk & Impact:

- Self-Provisioning access is a direct violation of Dow security requirements
- Permissions to administer entire Solution Manager system
- Reportable Sarbanes-Oxley, ICFR defect if not self-identified and reported to audit stakeholders

Details:

- User administered security (added and removed SAP_ALL profile)
- The access was granted for approximately one minute on February 24, 2022
- The Onapsis Security Platform triggered multiple alarms
  - Self-Provision Access
  - Assignment of SAP_ALL to a dialog user

Resolution:

- Perform exposure check (completed with no findings)
- Provide awareness and education training to SAP Security Administrators (Planned session between ISS and ESS leaders)
- Report to audit stakeholders

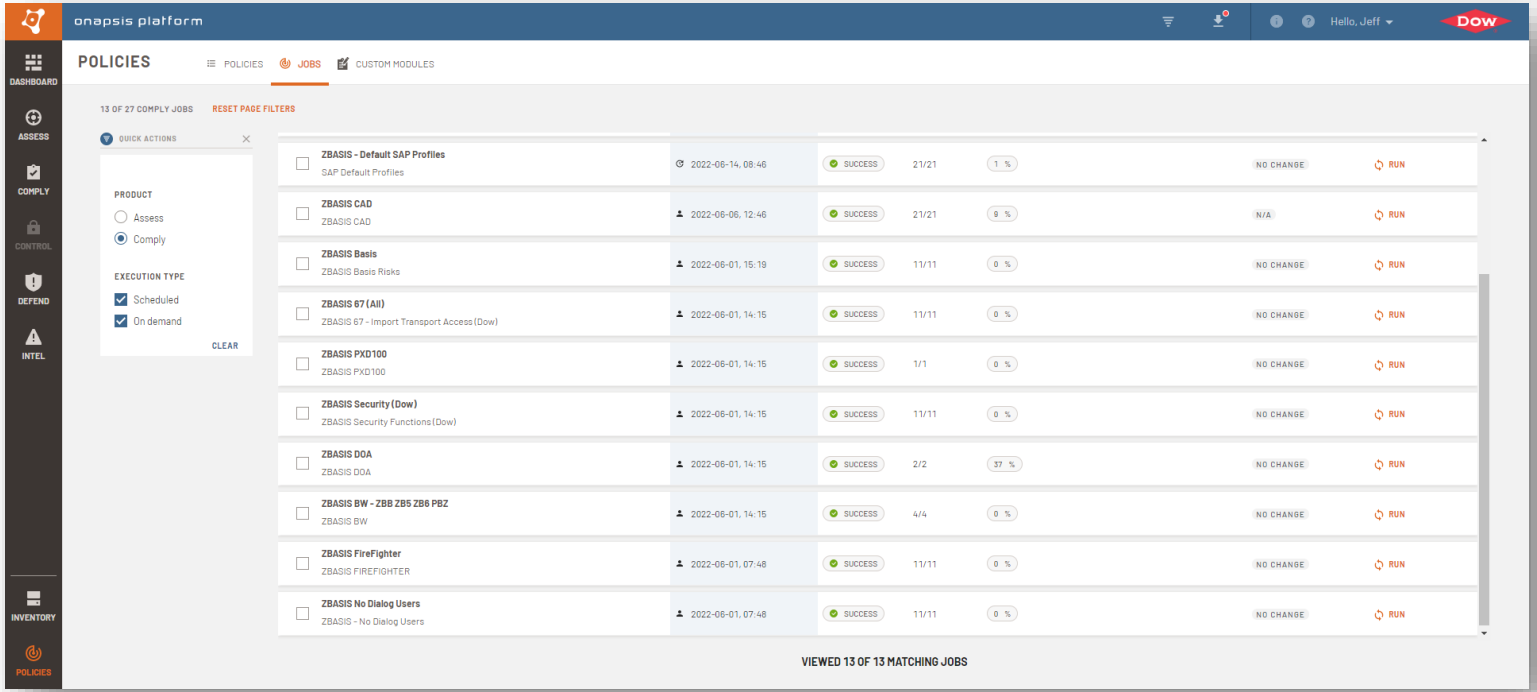
RBAC GOVERNANCE

- Monthly review of appropriateness of SAP role-based, elevated access
- Key internal control for ICFR/SOX compliance (also cyber)
- Previous process leveraged GRC-AC
  - Time consuming, manual effort
  - Error prone
  - Costly
- Onapsis automation and exclusion groups unlock efficiency and effectiveness
- Key Statistics:
  - 15 sap systems (many SAP clients)
  - 37 elevated access conditions
  - 492 unique access reviews
  - 5 SME hours of effort per month

RBAC GOVERNANCE - BEFORE

	ABC	ABC	ABC	ABC	ABC	ABC	ABC	ABC	ABC	ABC	ABC	ABC	ABC	ABC	ABC
SAP_50012340	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50010040	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50009140	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50009240	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50010740	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50010240	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50009340	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50010640	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50009440	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50011540	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50011240	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50012440	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50010340	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50010440	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50010540	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50009540	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50012540	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50012040	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50011640	P	P	P	P	P	P	P	P	P	P	P	ISS-ZB30	ISS-ZB30	P	P
SAP_50012140	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50012640	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50012740	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50011340	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50009640	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50003740	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50012840	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50012940	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50003840	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50013040	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50013140	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50013240	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50013340 - PBZ	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ISS-ZB53
SAP_50013640 - ZBB	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ISS-ZB53	N/A
SAP_50013740 -ZB5	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ISS-ZB53	N/A	N/A	N/A
SAP_50013840 -ZB6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ISS-ZB53	N/A	N/A
SAP_50003940	N/A	N/A	N/A	N/A			N/A	N/A	N/A	N/A	P	P	P	P	P
SAP_50013440 - PRD		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PRM 663 SAP_50013940	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PRM 655 SAP_50014040	N/A	N/A	P	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PRM 654 SAP_50014140	N/A	P	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PRD 500 SAP_50013540	P	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PRM 663 SAP_50014240	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PRM 654 SAP_50014340	N/A	P	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PRM 655 SAP_50014440	N/A	N/A	P	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
SAP_50003040	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SAP_50012240	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A
SAP_50016240	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A
SAP_50016340	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A
SAP_50016440	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A
SAP_50016840	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A
SAP_50016940	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A
	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A
SAP_50016640	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A
SAP_50017040	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A
SAP_50016740	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A
SAP_50011740	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A
SAP_50011840	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A
SAP_50017440	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P	N/A	N/A	N/A	N/A

RBAC GOVERNANCE - AFTER



KEY TAKEAWAYS

- The Regulatory Environment Is Putting a Lot of Pressure – on everyone
- Cybersecurity and Compliance – they aren’t THAT different
- Cybersecurity Technology – some very cool use cases for compliance!
- Enable the 2nd Line to harmonize the two and reap the benefits!

QUESTIONS?

THANK YOU


@onapsis


linkedin.com/company/onapsis

ONAPSIS.COM

ONAPSIS