CLOUDNATIVE SECURITYCON

NORTH AMERICA 2023

Mapping Motives Tells a Story:

Analysis of 2,000 Enterprise Cloud Detections

DAVID WOLF
Security Innovation Researcher

JOSHUA SMITH
Security Content Engineer

Session Content

- About Devo SciSec and Innovation
- Research Methods and Scope
- Research Findings by Theme
    1. Automated SOC
    2. Augmented Analyst
    3. Alert Management
- Takeaways from Research

About Devo SciSec and Innovation

MISSION:

Conduct security research on emerging threats and customer security problems to drive the delivery of high quality and novel security use cases.

RESEARCH THEMES:

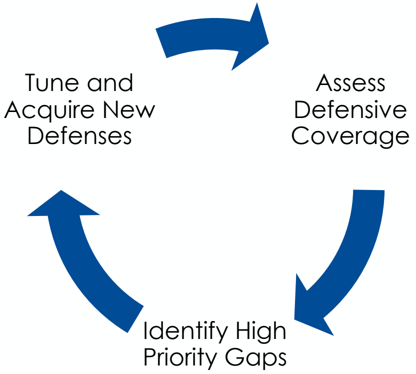
1. **Automated SOC Controls**
   - Detective
   - Corrective
   - Preventative
2. **Augmented Analyst**
   - Empowered
   - Enabled
   - Educated
3. **Alert Management***
   - Customizable
   - Reusable
   - Across vendor products

** Reported #1 analyst pain point from Devo annual SOC Performance Report*

RESEARCH PROCESS:

ATT&CK™ Adversarial Tactics, Techniques & Common Knowledge

- Assess
- Prioritize gaps
- Tune defenses


Assess Defensive Coverage
Identify High Priority Gaps
Tune and Acquire New Defenses

About Devo SciSec Research Lab

- Team
  - Detections Engineers
  - ML/AI Data Scientists
  - Security Researchers
  - QA
- Technology
  - Detections (product content)
  - ML models
  - Test infrastructure (vendor products)
  - Cloud providers (AWS, GCP, Azure)

DEVO

Research Methods and Scope

Methods

Devo SciSec security researchers:

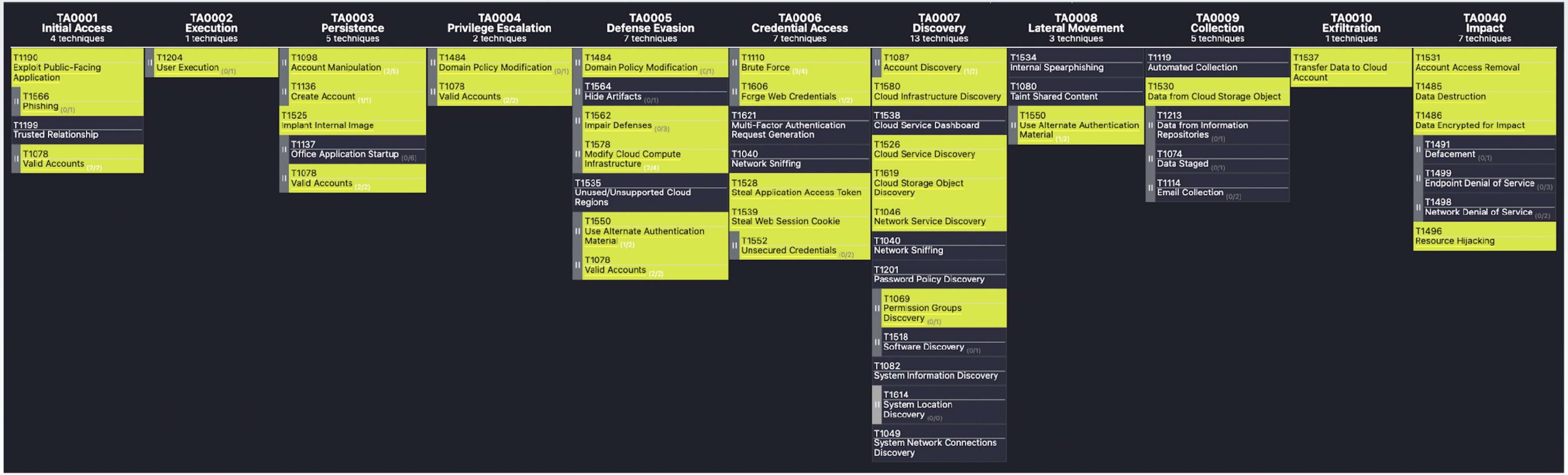
- Analyzed cloud SIEM detections from more than 300 enterprises and MSPs that have active, firing alerts.
- Applied novel machine learning (ML) and natural language processing (NLP) to alert metadata in order to map detections to MITRE ATT&CK® and Zero Trust Architecture.
- Explored further ML and NLP methods to analyze cloud alert metadata as a corpus in order to map attacker motives and stories using semantic relationships.

Scope

- 6035 alerts used in analysis (15141 alerts in sample)
  - Sample period: 1 August-31 December 2022
- 398 SIEMs (Devo domains) with out-of-the-box (OOTB) alerts deployed
- Enterprises span industries, including:
  - MSSPs, financial services, retail, technology, education, and operational technology (manufacturing, hospitals, transportation, etc.)
  - Federal and defense-related detections are not in scope

Scope: MITRE ATT&CK® Cloud Matrix: Infrastructure and Workspace Controls

The cloud alerts used in this research mapped to MITRE ATT&CK® Cloud Matrix Tactics and Techniques

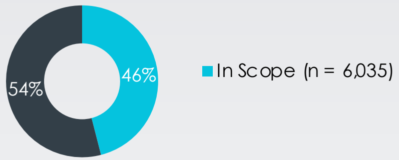


TA0001 Initial Access 4 techniques	TA0002 Execution 1 techniques	TA0003 Persistence 5 techniques	TA0004 Privilege Escalation 2 techniques	TA0005 Defense Evasion 7 techniques	TA0006 Credential Access 7 techniques	TA0007 Discovery 13 techniques	TA0008 Lateral Movement 3 techniques	TA0009 Collection 5 techniques	TA0010 Exfiltration 1 techniques	TA0040 Impact 7 techniques
T1190 Exploit Public-Facing Application	T1204 User Execution (0/1)	T1098 Account Manipulation (2/5)	T1484 Domain Policy Modification (0/1)	T1484 Domain Policy Modification (0/1)	T1110 Brute Force (3/4)	T1087 Account Discovery (1/2)	T1534 Internal Spearphishing	T1119 Automated Collection	T1537 Transfer Data to Cloud Account	T1531 Account Access Removal
T1566 Phishing (0/1)		T1136 Create Account (1/1)	T1078 Valid Accounts (2/2)	T1564 Hide Artifacts (0/1)	T1606 Forge Web Credentials (1/2)	T1580 Cloud Infrastructure Discovery	T1080 Taint Shared Content	T1530 Data from Cloud Storage Object		T1485 Data Destruction
T1199 Trusted Relationship		T1525 Implant Internal Image		T1562 Impair Defenses (0/3)	T1621 Multi-Factor Authentication Request Generation	T1538 Cloud Service Dashboard	T1550 Use Alternate Authentication Material (1/2)	T1213 Data from Information Repositories (0/1)		T1486 Data Encrypted for Impact
T1078 Valid Accounts (2/2)		T1137 Office Application Startup (0/6)		T1578 Modify Cloud Compute Infrastructure (2/4)	T1040 Network Sniffing	T1526 Cloud Service Discovery		T1074 Data Staged (0/1)		T1491 Defacement (0/1)
		T1078 Valid Accounts (2/2)		T1535 Unused/Unsupported Cloud Regions	T1528 Steal Application Access Token	T1619 Cloud Storage Object Discovery		T1114 Email Collection (0/2)		T1499 Endpoint Denial of Service (0/3)
				T1550 Use Alternate Authentication Material (1/2)	T1539 Steal Web Session Cookie	T1046 Network Service Discovery				T1498 Network Denial of Service (0/2)
				T1078 Valid Accounts (2/2)	T1552 Unsecured Credentials (0/2)	T1040 Network Sniffing				T1496 Resource Hijacking
						T1201 Password Policy Discovery				
						T1069 Permission Groups Discovery (0/1)				
						T1518 Software Discovery (0/1)				
						T1082 System Information Discovery				
						T1614 System Location Discovery (0/0)				
						T1049 System Network Connections Discovery				

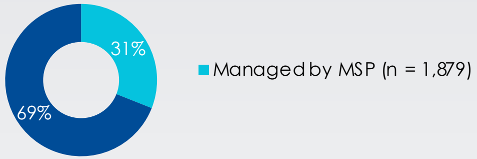
DEVO

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

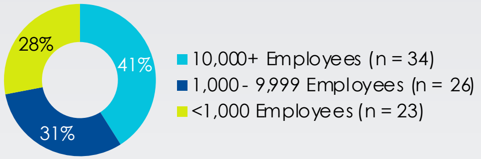
Scope in Graph Form



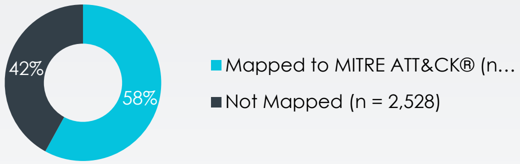
Detections used in final analysis vs removed from sample



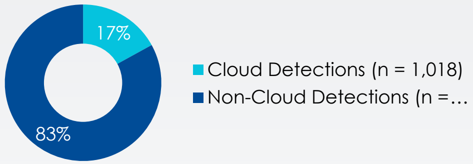
Detections by alert management responsibility



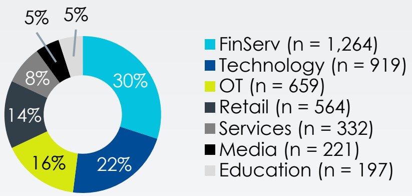
Number of employees per enterprise (excludes MSSPs)



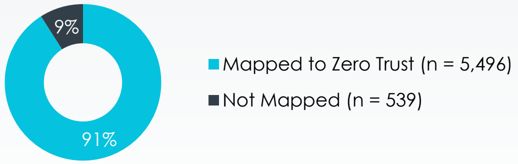
Detections mapped to MITRE ATT&CK® framework



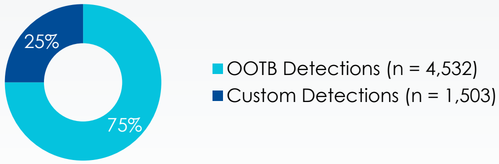
Detections based on cloud providers vs traditional enterprise detections



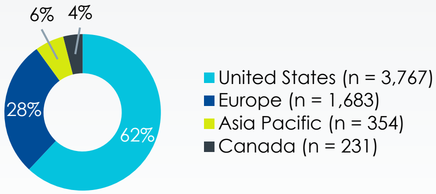
Detections per enterprise vertical (excludes MSPs)



Detections mapped to Zero Trust Architecture framework



Out-of-the-box detections vs custom-crafted detections

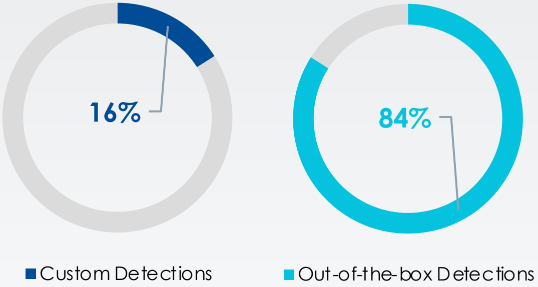


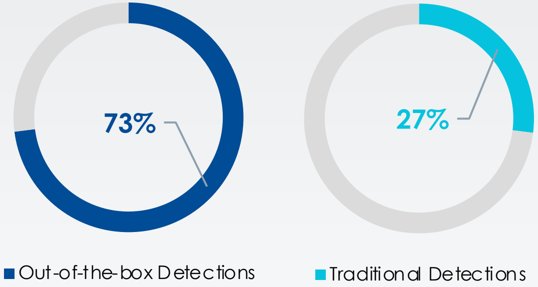
Detections per enterprise location

1. Automated SOC

Automated SOC: OOTB Key to Cloud Control

Cloud SOC defenders are relying on out-of-the-box detections (84%)
and only 60% as likely to build custom SIEM alerts compared to enterprise defenders

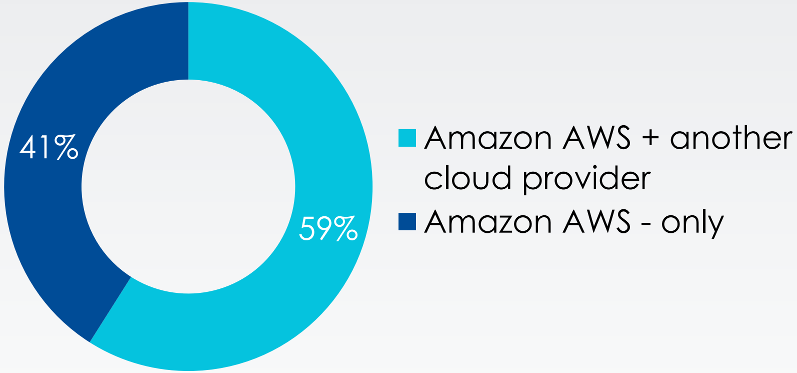




Source: *2022 Devo State of the Cloud SOC* Detections Report

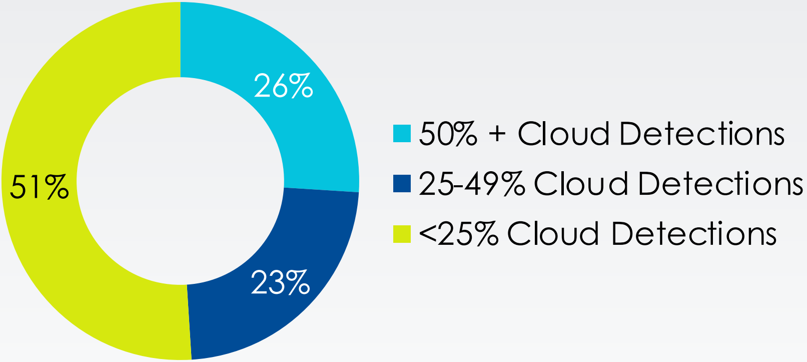
Automated SOC: Cloud Control Coverage

Enterprise SOCs with Amazon AWS are often defending another cloud (59%)



Source: 2022 Devo State of the Cloud SOC Detections Report

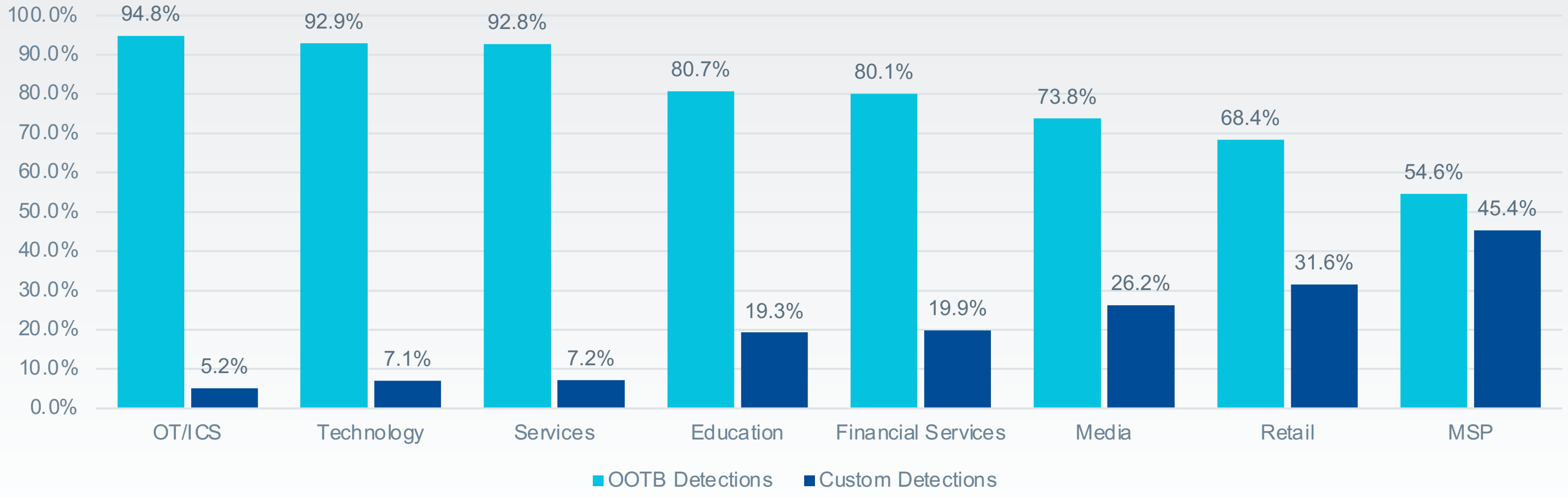
For 1 in 4 enterprise SOCs defending cloud assets, cloud detections comprise a majority (50%+) of the SIEM detection stack



Source: 2022 Devo State of the Cloud SOC Detections Report

Automated SOC: OOTB vs Custom SIEM Alerts

Managed Security Service Providers (MSSPs) are more likely than enterprises to craft custom detections. Overall, 84% of enterprise detections are OOTB, compared to only 55% of MSSP detections.



Automated SOC

TOP TAKEAWAYS:

1. Out-of-the-box detections are the key to cloud SOC automation
2. Cloud is a major control area and often a majority of automated SIEM alerts

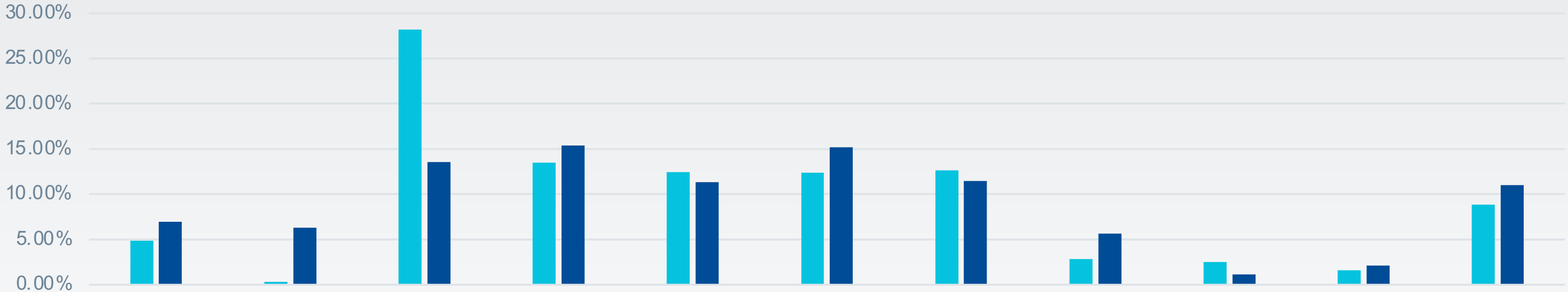
2. Augmented Analyst

DEVO

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Augmented Analyst: Mitre ATT&CK Visibility

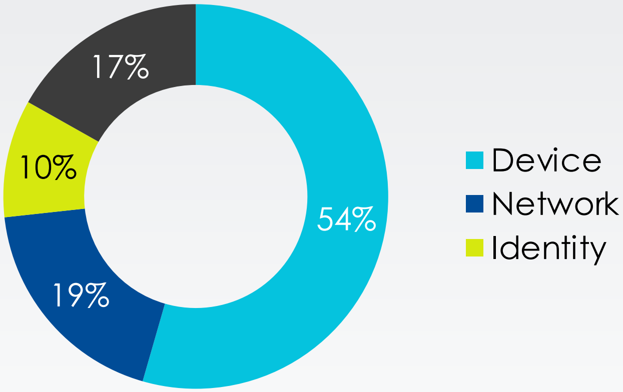
Cloud SOC analysts have less visibility at the start and end of the MITRE ATT&CK® chain compared to enterprise defenders **(12.1% vs 22.1%)**



	TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0008** Lateral Movement	**TA0009** Collection	**TA00010** Exfiltration	**TA00040** Impact
Cloud Detections	4,87%	0,29%	28,17%	13,47%	12,45%	12,35%	12,61%	2,84%	2,51%	1,58%	8,87%
Enterprise Detections	6,97%	6,29%	13,54%	15,39%	11,34%	15,16%	11,46%	5,65%	1,12%	2,10%	10,98%

Augmented Analyst: Zero Trust

Most SOC detections focus on **Zero Trust Device and Network activity (74%)** with far fewer controls based on **User Identity, Application Workloads, and Data**



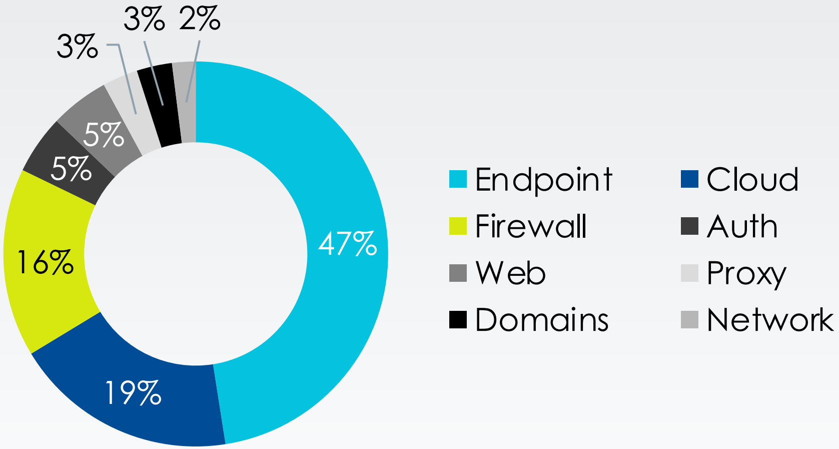
Source: *2022 Devo State of the Cloud SOC* Detections Report

DEVO

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Augmented Analyst: Device Protection

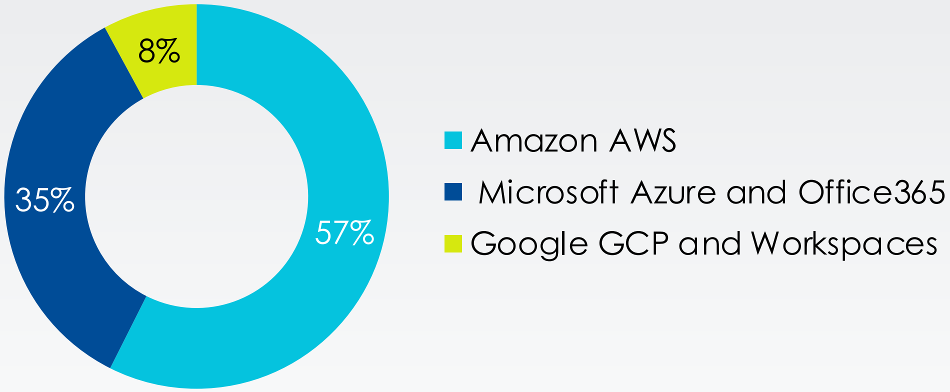
Detections based on endpoint device protection, cloud logs, and firewall solutions are the basis for most enterprise SOC controls (83% of detections from the top 10 technology control areas)



Source: *2022 Devo State of the Cloud SOC* Detections Report

Augmented Analyst: Cloud controls

Cloud SOC defenders are focusing most detective controls on AWS (58%)



Source: *2022 Devo State of the Cloud SOC* Detections Report

Augmented Analyst

TOP TAKEAWAYS:

1. Cloud SOC analysts need support via specialized detections to defend multiple clouds, especially for enterprises on AWS
2. Cloud SOC analysts need more visibility at the start and end of the MITRE ATT&CK® chain

3. Alert Management

DEVO

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Alert Management: Current Auditing Options by Cloud Vendor

Amazon Web Services (AWS)

- Logging and events
- Visibility and alerting
- Automation
- Secure storage
- Custom

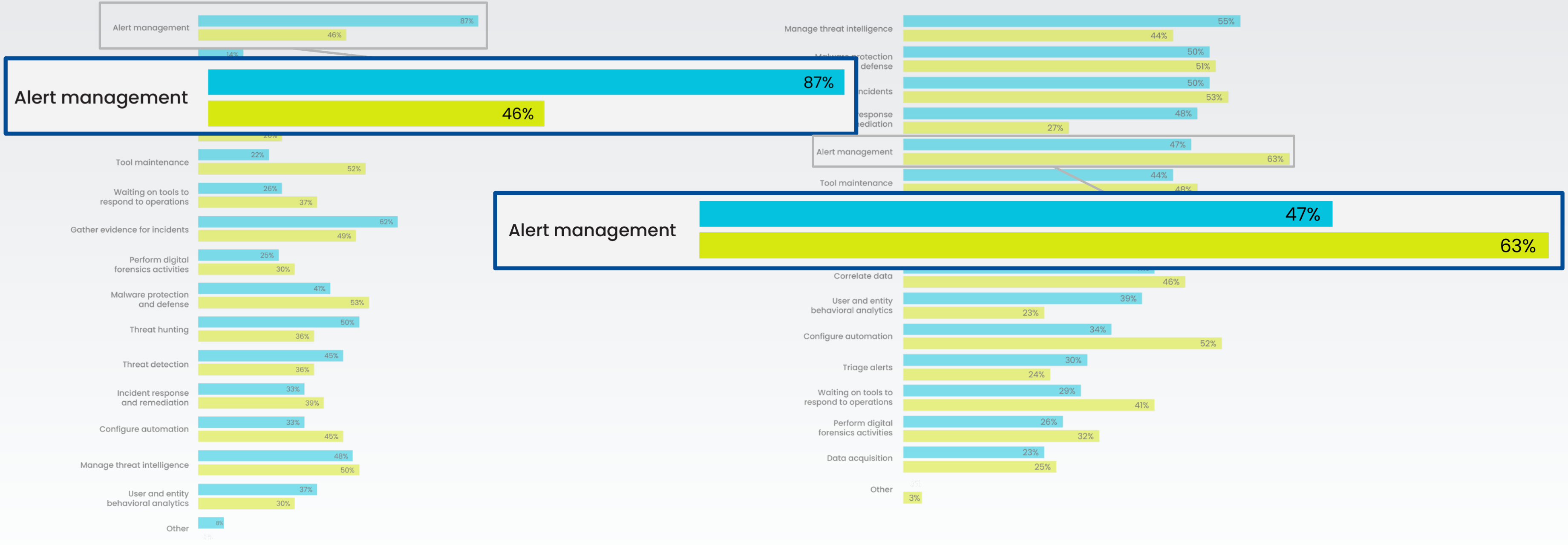
Google Cloud Provider (GCP)

- Admin Activity audit logs
- Data Access audit logs
- System Event audit logs
- Policy Denied audit logs

Microsoft Azure

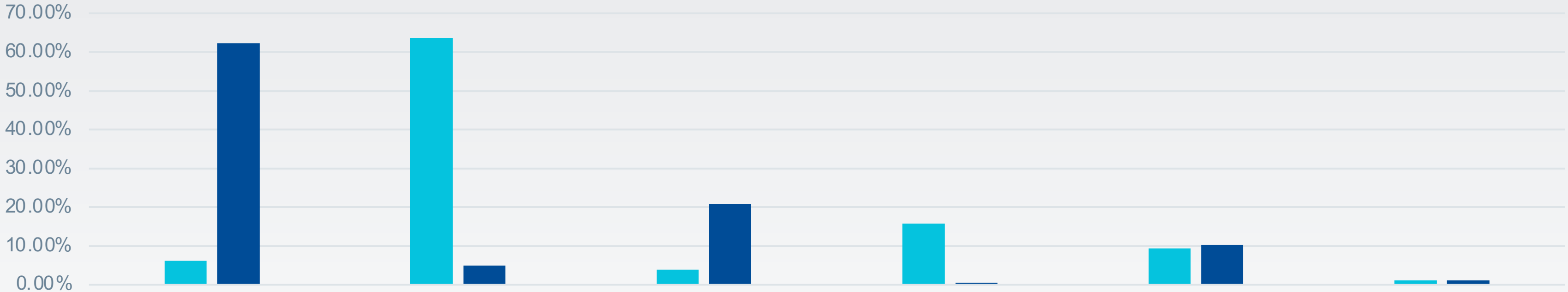
- Activity logs
- Azure Resource logs
- Azure Active Directory reporting
- Virtual machines and cloud services
- Azure Storage Analytics
- Network security group (NSG) flow logs
- Application insight
- Process data / security alerts

Alert Management: Devo SOC Performance Report



Alert Management: Zero Trust

Most Cloud SOC detections focus on **Zero Trust Visibility and Workloads (79%)**
while traditional Enterprise SOC detections are focused on **Device and Network activity (83%)**

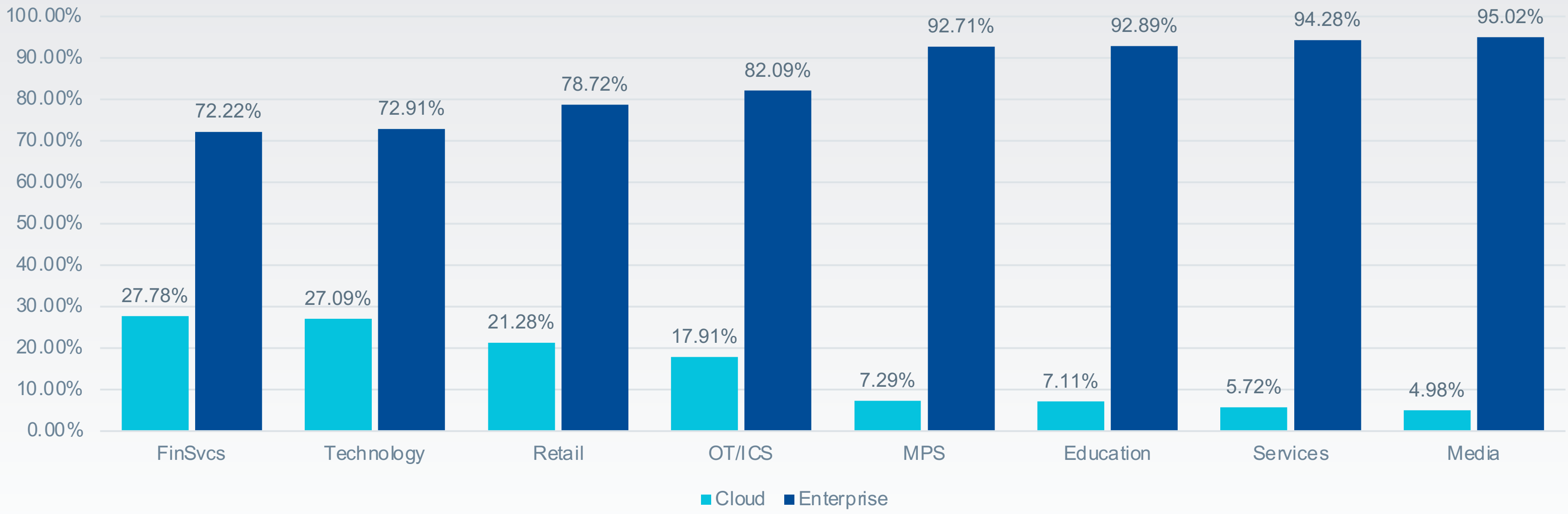


	Device	Visibility	Network	Workload	Identity	Data
Cloud Detections	6,23%	63,58%	3,94%	15,75%	9,43%	1,07%
Enterprise Detections	62,29%	4,91%	20,82%	0,57%	10,33%	1,09%

Source: *2022 Devo State of the Cloud SOC* Detections Report

Alert Management: Cloud Detections Matter

Cloud is most prominent as a ratio of detections in **Financial Services and Technology (27%)**



Source: *2022 Devo State of the Cloud SOC* Detections Report

Alert Management

TOP TAKEAWAYS:

1. Out-of-the-box detections are the key to cloud SOC automation
2. Cloud is a major control area and often a majority of automated SIEM alerts

Lessons Learned:

1. Cloud is a big part of the enterprise detection stack, and enterprises are increasingly defending multiple cloud infrastructure and workspace providers
2. Analysts need alerts that are augmented with rich metadata like MITRE ATT&CK tactics and techniques
3. Help analysts by mapping alerts to a control area: cloud, network, device, identity, application, data
4. Cloud controls are different – OOTB strategy is the way to go

THANK YOU