Welcome

DCO COBRA and SOSSEC - CYBER TALK

Presents:
Cloud Hosting Microsoft Capabilities
May 28, 2020

Microsoft Speakers Include:
Andrew Harris – Principal PM, Azure Sovereign Cloud Security
Gladys Rodriguez - Principal Cyber Security Consultant
David Phillips - DOD Director For Cyber Security Services
Stephen Ingerski - Sr. Cyber Delivery Project Manager
“The ethos of being partner led is always going to be in everything we do.”

Satya Nadella
Inspire 2017
The Department’s cyberspace objectives are:

1. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment;
2. Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages;
3. Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident;
4. Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and
5. Expanding DoD cyber cooperation with interagency, industry, and international partners.
BUILD A MORE LETHAL JOINT FORCE;

Accelerate cyber capability development: The Department will accelerate the development of cyber capabilities for both warfighting and countering malicious cyber actors. Our focus will be on fielding capabilities that are scalable, adaptable, and diverse to provide maximum flexibility to Joint Force commanders. The Joint Force will be capable of employing cyberspace operations throughout the spectrum of conflict, from day-to-day operations to wartime, in order to advance U.S. interests.

Innovate to foster agility: The Department must innovate to keep pace with rapidly evolving threats and technologies in cyberspace. We will accept and manage operational and programmatic risk in a deliberate manner that moves from a “zero defect” culture to one that fosters agility and innovation because success in this domain requires the Department to innovate faster than our strategic competitors.

Leverage automation and data analysis to improve effectiveness: The Department will use cyber enterprise solutions to operate at machine speed and large-scale data analytics to identify malicious cyber activity across different networks and systems. The Department will leverage these advances to improve our own defensive posture and to ensure that our cyber capabilities will continue to be effective against competitors armed with cutting edge technology.

Employ commercial-off-the-shelf (COTS) cyber capabilities: The Department excels at creating cyber capabilities tailored for specific operational problems. In addition to these capabilities, we will make greater use of COTS capabilities that can be optimized for DoD use.
Cloud (and Cloud Cyber Security Capabilities) is DoD Imperative of FY20

- Identity and Secure Identity
  - Credential exposure mitigation
  - Hybrid authentication and authorization
- Comply to Connect
- Azure AD implementation
- Cyber driven data platforms
- Cloud migration (inc/O365) with cyber capabilities (Advanced Threat Protection)
- Zero Trust Architectures
Support DoD Telework initiatives; (1.2M Teams users)

- Enable Azure Multi Factor Authentication
- Protect against threats in O365/Teams
- Configure O365 Advanced Threat Protection
- Configure Azure Advanced Threat Protection
- Turn on Microsoft Advanced Threat Protection
- Configure Intune for managed devices
- Enable Azure AD for conditional access
- Require compliant PC’s and conditionally approved devices
- Get started with Cloud App Security
- Continuous monitoring capabilities
Cloud Cyber services benefits the warfighter

Cloud is a cyber security imperative for DoD.

No longer should cyber security be inhibitor to cloud migration but rather an enabler.

The DoD will always need in house technical expertise, however consuming cloud security solutions greatly reduces the underlining requirements from an infrastructure perspective and enables the DoD to better focus on mission priorities.

DoD can focus on consumption of the services and ensuring the services are providing the data the DoD requires to make mission decisions, rather than focusing on installation and maintenance.
What is today’s enterprise perimeter?

Cyber Protection used to be about building a robust network boundary, akin to the castle and moat, to keep the bad guys out and the good guys in.

Remote work, partner resources, disparate networks, cloud environments, and BYOD all open doors to the kingdom.

The modern enterprise cannot be contained in the legacy manner.
Identity is the new security perimeter...

Cloud delivers this faster, more scalable and more effectively

Cloud apps

On-premises apps

Devices

Employees

Partners & customers
Modernizing the security perimeter

Network protects against classic attacks...
...but bypassed reliably with
• Phishing
• Credential theft
+ Data moving out of the network
= Critical to build modern security perimeter based on Identity
  ▪ Identity and Access Management
    Strong Authentication + Monitoring and enforcement of policies
  ▪ Strength from Hardware & Intelligence—
    Auth & Access should consider device status, compromised credentials, &
    other threat intelligence
Why Worry About Identity?

Major Identity Challenges

- Identity system security is critical to all security assurances
- Attackers are actively targeting privileged access and identity systems
- Identity systems are challenging to protect
- Identity attacks like credential theft are difficult to detect and investigate
- Individual accounts have large attack surface across devices and systems
- Network controls do not inherently isolate credentials
- Change in culture and resistance to updating CONOPS/TTPs is hard – this is not an “insert X-Appliance” fix

Securing Identity

Embrace identity as primary security perimeter and protects identity systems, admins, and credentials as top priorities

Elevated protection for privileged access & identity systems
- Strongest protections for identity admins based on top attacks and leading-edge hardware rooted protections
- Advanced detection for identity and credential theft attacks
- Expert analysts to help detect and respond to identity attacks

Industrial Grade Protections for all users
- Hardware protection for credentials on devices
- Leading edge biometrics authentication combining ease of use and high security
- Integration of real time cloud intelligence into identity risk management
Identity is not a new issue to DoD

Reduce and Harden the AD attack surface by implementing a *least privilege* administrative model

Focused on privileged accounts, belonging to humans, but what about the rest?
How Does Identity Relate to DCO?

Access Control: Keep Assets and Data away from Attackers
Enable Risk Based Command Centric Operational Decisions
ZT Principles enhance Operational Effectiveness

1. IT Security is Complex
   • Many Devices, Users, & Connections

2. “Trusted network” security strategy
   • Initial attacks were network based
   • Seemingly simple and economical
   • Accepted lower security within the network

3. Assets increasingly leave the network
   • BYOD, WFH, Mobile, and SaaS

4. Attackers shift to identity attacks
   • Phishing and credential theft
   • Security teams often overwhelmed
If identity is the new perimeter, what data do I need to see?

If I trust nothing, how can I collect all the disparate data?

If I don’t own the environment, how can I trust the data?

If I don’t control all the systems, how can I correlate all the data?
“Zero Trust” has been around for a while

Converged approach gaining significant momentum (though still ‘early days’ of this approach)

Historically slow mainstream adoption for both network & identity models:

- **Network** – Expensive and challenging to implement
  - Google’s BeyondCorp success is rarely replicated

- **Identity** – Natural resistance to big changes
  - Security has a deep history/affinity with networking

**Converged approach gaining significant momentum (though still ‘early days’ of this approach)**
Zero Trust

Security strategy – Treat every access attempt as if it’s originating from an untrusted network.

 Leads to

Access Architecture uses policy to:
1. Explicitly validate trustworthiness
2. Dynamically address insufficient trust:
   • Increase trust
   • Limit access
   • Block access

Mobility & Choice to enable productivity
1. Can work anywhere
   • Applications & Data available anywhere
   • Security protections work anywhere
2. Users can choose any device type

Increases both security and productivity
Conditional Access ➔ Zero Trust Model

**User**
- Groups/Role
- Location
- Privileges
- Session risk
- User Risk

**Device**
- Managed or BYOD
- Health & compliance
- Device risk
- Type and OS version
- Encryption status

**Security & Compliance Policy Engine**
- Microsoft Azure AD
- Microsoft Defender ATP
- Microsoft Intune

**Microsoft Cloud**
- Microsoft Cloud App Security

**Microsoft Information Protection**
- Cloud SaaS apps

**On-premises & web apps**

Azure Sentinel
Zero Trust User Access

Conditional Access to Resources

- **User Threat/Risk Signals**
  - Azure ATP
  - Cloud App Security
- **User/Session Risk**
  - **Azure AD Identity Protection**
    - Leaked cred protection
    - Behavioral Analytics
  - **Hello for Business**
    - Azure MFA
- **Device Threat/Risk Signals**
  - [IsCompliant](#)
  - Microsoft Intune
- **Approved Apps**

Policy is evaluated when:
- Initial Access Request
- Change in posture (AADIP signal)

**Conditional Access**

- **Azure Active Directory (Azure AD)**
- **Azure AD B2B**

**Remediate** Leaked Credential (Requires MFA)

**Approved Apps**

**Legend**

- Green: Full access
- Dashed: Limited access
- Orange: Risk Mitigation
- Blue: Remediation Path

**Microsoft Applications**
- Office 365
- Dynamics 365

**Cloud Infrastructure**
- Azure Portal
- Linux Login

**Modern Applications**
- [Google](#)
- [Salesforce](#)
- [AWS](#)
- [SAM](#)

**SaaS Applications**
- AWS
- [Google](#)
- [Salesforce](#)
- [AWS](#)

**Legacy Apps**
- Secure VPN Replacement

**Documents**
- [PDF](#)
- [Word](#)

**Mobile Apps**
- Android
- [iOS](#)

**Intelligent Security Graph (ISG)**
- 8 Trillion Signals/Day

**Signal**
- to make an informed decision

**Decision**
- based on organizational policy

**Enforcement**
- of policy across resources
Managing Information\Cyber Risk

Zero Trust

Modern SOC

Organizational Leadership
Board
- Organizational & Risk Oversight

Management
- Business Model and Vision
- Organizational Risk Appetite

Active Governance
- Policy Authoring/Approval
  - Enable Productivity
  - Protect Mission
- Monitor & Remediate Risk

Information Risk Management
- Refresh policy regularly with changes to threat environment, technology, regulations, business model, and more
- Supply Chain Risk

Identify

Detect

Respond

Recover

Threat Intelligence
- Strategic Threat Insight/Trends

Modern SOC

Critical Partner Team
Security Reference Architecture

Legend
- Event Log Based Monitoring
- Investigation & Proactive Hunting

Improve & Learn by Measuring:
Responsiveness - Mean time to Acknowledge (MTTA)
Effectiveness - Mean Time to Remediate (MTTR)

Case Management

Classic SIEM
- Anomaly
- Radar
- Splunk

SOC Analyst

Security & Network
- Provide actionable security alerts, raw logs, or both
- Carbon Black
- Symantec
- Fortinet
- Sophos
- zscaler
- PureEye
- Cybereason
- Lookout
- Duo
- Check Point

Raw Logs
- Security & Activity Logs

Hybrid Infrastructure and Apps
- Logstash
- Splunk
- Monitor

Identity & Access Management
- LDAP
- Okta
- CRAM
- SAML
- Security

Endpoint & Mobile
- Office 365
- Bloomberg
- Slack
- SAML
- Security

Modern & SaaS Applications
- Salesforce
- MS Office
- Google
- SAML
- Security

Information
- Amazon
- AWS
- Azure
- Microsoft
- IBM
- Oracle
- SAML
- Security
Security Reference Architecture

Legend
- Event Log Based Monitoring
- Investigation & Proactive Hunting

Improve & Learn by Measuring:
Responsiveness - Mean time to Acknowledge (MTTA)
Effectiveness - Mean Time to Remediate (MTTR)

Case Management

Classic SIEM
- ArcSight
- Splunk

Alert Integration - Graph Security API

Security & Network
- Carbon Black
- Symantec
- Fortinet
- Sophos
- Zscaler

Raw Logs
- Security & Activity Logs

Hybrid Infrastructure and Apps

Identity & Access Management
- Okta
- Oracle

Endpoint & Mobile
- Office 365

Modern & SaaS Applications
- G Suite

Information

Outsourcing
Effectiveness Improvement – Microsoft Experience

**Enforce Quality + Apply Technology**

---

**Detect**

- 8 trillions of signals per day

- Machine Learning (Artificial Intelligence)

- Behavioral Analytics (UEBA) (User and Entity)

- 10\textsuperscript{th} of thousands of alerts

---

**Respond**

- Enforce 93% true positive on alert feeds

- Formally 28% suspicious logins to 0.001%

- MTTA – 15 minutes

- 96% manual incidents handled within 1hr

---

Focus on time to acknowledge and remediate

Security Orchestration, Automation, and Remediation (SOAR)

Hundreds of investigations
ZTA Integration using the **Graph Security APIs**

- Easier to connect with solutions from Microsoft and partners.
- Readily realize and enrich the value of these solutions.
- Use one of the following approaches:
  - **Write code** in C#, Java, NodeJS, and more.
  - **Connect using scripts** – Find PowerShell samples.
  - Use [Microsoft Graph Security connectors](https://docs.microsoft.com/en-us/graph) for Azure Logic Apps, Microsoft Flow, and PowerApps.
  - **Get data into reports and dashboards** – Use the [Microsoft Graph Security connector](https://docs.microsoft.com/en-us/graph) for Power BI.
  - **Connect using Jupyter notebooks** – Find [Jupyter notebook samples](https://docs.microsoft.com/en-us/graph).

https://docs.microsoft.com/en-us/graph
Microsoft Intelligent Security Association (MISA)
Graph Benefits Overview

**Customer**
- Less bandwidth and storage requirements
  - Reduction of need to centralize alerts/logs
- Less time interconnecting and maintaining
  - No manual verifications to maintain
  - Reduction in troubleshooting custom workflows
- Better verifications
- Vendor provided interconnection and SOAR
- Reduction of False Positives
- Faster MTTA and MTTR

**Partners**
- Enrich the value of products and services
  - Product Features
  - Reporting and Analytics
- Development Services
- Expert Services
  - Cyber Operations
  - Implementation
- Readiness
- Processes, Governance
Risk: Adversary gets access to your resources by sending a phishing email (which delivers remote control malware).

Goal: Rapidly find and clean all malicious emails and malware infections (before adversary can spread farther).

Phishing Email (Internal or External)

- **Risk:** Adversary gets access to your resources by sending a phishing email (which delivers remote control malware).
- **Goal:** Rapidly find and clean all malicious emails and malware infections (before adversary can spread farther).

- **Search all mailboxes and remove attachment**
- **Block/quarantine the attachment**
- **Office 365 ATP**
  - Sends malicious email attachment
  - Remediate other infected locations
- **Intelligent Security Graph**
  - Shared security signals
- **Microsoft Defender ATP**
  - Remediate other infected end-points
<table>
<thead>
<tr>
<th>Incident name</th>
<th>Severity</th>
<th>Category</th>
<th>Active alerts</th>
<th>Status</th>
<th>Assigned to</th>
<th>Impacted entities</th>
<th>Detection source</th>
<th>First activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential theft phishing campaign</td>
<td>High</td>
<td>Credential theft, Suspicious activity + 2 more</td>
<td>10/10</td>
<td>Active</td>
<td>Dan Smith</td>
<td>2 devices, 2 users, 2 mailboxes</td>
<td>Microsoft Defender ATP, Office 365 ATP</td>
<td>3/7/2019</td>
</tr>
<tr>
<td>Unwanted software installed on high value systems</td>
<td>High</td>
<td>Malware</td>
<td>5/6</td>
<td>Active</td>
<td>Unassigned</td>
<td>4 devices, 3 users</td>
<td>EDR, Antivirus</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>Possible credential theft and defense evasion</td>
<td>High</td>
<td>Execution, Defense evasion + 2 more</td>
<td>7/7</td>
<td>Active</td>
<td>Unassigned</td>
<td>4 devices, 3 users</td>
<td>Azure ATP, EDR, Custom detection</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>Multi-stage attack linked to malicious IP address</td>
<td>High</td>
<td>Initial access, Execution, Discovery + 2 more</td>
<td>11/11</td>
<td>Active</td>
<td>Unassigned</td>
<td>2 devices, 2 users, 2 mailboxes</td>
<td>Microsoft Defender ATP</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>User and endpoint compromise from phishing</td>
<td>High</td>
<td>Initial access, Execution, Discovery + 2 more</td>
<td>3/3</td>
<td>Active</td>
<td>Unassigned</td>
<td>2 devices, 2 users, 2 mailboxes</td>
<td>Office ATP, Antivirus, EDR</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>Impossible travel and suspicious activity</td>
<td>Medium</td>
<td>Suspicious activity</td>
<td>2/2</td>
<td>Active</td>
<td>Unassigned</td>
<td>core-joraw... Jonathan Wel...</td>
<td>MCAS, EDR</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>incident #50534</td>
<td>Medium</td>
<td>Persistence</td>
<td>2/2</td>
<td>Active</td>
<td>Unassigned</td>
<td>Client-1 Daniel Ben</td>
<td>Azure ATP</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>incident #50555</td>
<td>Medium</td>
<td>Malware download</td>
<td>12/12</td>
<td>Active</td>
<td>Unassigned</td>
<td>2 devices, 2 users</td>
<td>Microsoft Defender ATP</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>incident #50575</td>
<td>Medium</td>
<td>Suspicious activity</td>
<td>1/3</td>
<td>Active</td>
<td>Unassigned</td>
<td>core-avamaci...</td>
<td>Microsoft Defender ATP</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>incident #50590</td>
<td>Medium</td>
<td>Lateral movement</td>
<td>45/46</td>
<td>Active</td>
<td>Unassigned</td>
<td>4 devices, 3 users</td>
<td>Microsoft Defender ATP</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>incident #50536</td>
<td>Medium</td>
<td>Lateral movement</td>
<td>3/4</td>
<td>Active</td>
<td>Unassigned</td>
<td>4 devices, 4 users</td>
<td>Microsoft Defender ATP</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>incident #50519</td>
<td>Medium</td>
<td>Malware download</td>
<td>2/3</td>
<td>Active</td>
<td>Unassigned</td>
<td>3 devices, 2 users</td>
<td>Microsoft Defender ATP</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>incident #50524</td>
<td>Medium</td>
<td>Malware</td>
<td>1/2</td>
<td>Active</td>
<td>Unassigned</td>
<td>core-danilie... Daniel Ben</td>
<td>Microsoft Defender ATP</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>Incident #50550</td>
<td>Medium</td>
<td>Reconnaissance</td>
<td>2/2</td>
<td>Active</td>
<td>Unassigned</td>
<td>core-mckid... Mike Pearson</td>
<td>Microsoft Defender ATP</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>incident #50517</td>
<td>Medium</td>
<td>Credential stealing</td>
<td>1/1</td>
<td>Active</td>
<td>Unassigned</td>
<td>Core-mckid... Mike Pearson</td>
<td>Microsoft Defender ATP</td>
<td>3/2/2019</td>
</tr>
<tr>
<td>Incident #50521</td>
<td>Low</td>
<td>Suspicious activity</td>
<td>4/4</td>
<td>Active</td>
<td>Unassigned</td>
<td>3 devices, 2 users</td>
<td>Microsoft Defender ATP</td>
<td>3/2/2019</td>
</tr>
</tbody>
</table>
Incident queue > Credential theft phishing campaign

11/11 Active alerts
8 MITRE attack categories

2 impacted devices
2 impacted users
2 impacted mailboxes

Incident details
Incident status: Active
First activity: Nov 4, 2019 06:32 AM
Last activity: Nov 4, 2019 06:53 AM
Classification: Not set
Determination: Not set
Assigned to: Not assigned

Evidence and pending actions
23 evidence found
Evidence remediation status
## Incident queue > Credential theft phishing campaign

<table>
<thead>
<tr>
<th>Title</th>
<th>Severity</th>
<th>Status</th>
<th>Linked by</th>
<th>Category</th>
<th>Impacted entities</th>
<th>Detection Source</th>
<th>Risk activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious behavior by Microsoft word was observed...</td>
<td>Medium</td>
<td>Resolved</td>
<td>2 reasons</td>
<td>Initial access</td>
<td>cont-mikebarden</td>
<td>Microsoft Defender ATP</td>
<td>Nov 4, 2019 06:32 AM</td>
</tr>
<tr>
<td>Suspicious PowerShell commandline</td>
<td>Medium</td>
<td>Active</td>
<td>Proximate time</td>
<td>Execution</td>
<td>cont-mikebarden</td>
<td>Microsoft Defender ATP</td>
<td>Nov 4, 2019 06:35 AM</td>
</tr>
<tr>
<td>Suspicious access to LSASS service</td>
<td>Medium</td>
<td>Active</td>
<td>Proximate time</td>
<td>Credential access</td>
<td>cont-mikebarden</td>
<td>Microsoft Defender ATP</td>
<td>Nov 4, 2019 06:36 AM</td>
</tr>
<tr>
<td>Security principal reconnaissance (LOAP)</td>
<td>Medium</td>
<td>Active</td>
<td>2 reasons</td>
<td>Discovery</td>
<td></td>
<td>Azure ATP</td>
<td>Nov 4, 2019 06:38 AM</td>
</tr>
<tr>
<td>Pass the ticket attack</td>
<td>High</td>
<td>Active</td>
<td>Proximate time</td>
<td>Lateral movement</td>
<td>contoso-CRM-EU-O1</td>
<td>Microsoft Defender ATP</td>
<td>Nov 4, 2019 06:41 AM</td>
</tr>
<tr>
<td>Suspicious WMI process creation</td>
<td>High</td>
<td>Active</td>
<td>2 reasons</td>
<td>Lateral movement</td>
<td>EU-PRIMARY+DC</td>
<td>Microsoft Defender ATP</td>
<td>Nov 4, 2019 06:41 AM</td>
</tr>
<tr>
<td>Suspected identity theft (pass-the-ticket)</td>
<td>High</td>
<td>Active</td>
<td>2 reasons</td>
<td>Credential Access</td>
<td>2 devices</td>
<td>Azure ATP</td>
<td>Nov 4, 2019 06:41 AM</td>
</tr>
<tr>
<td>Remote code execution attempt</td>
<td>Medium</td>
<td>Active</td>
<td>2 reasons</td>
<td>Lateral Movement</td>
<td></td>
<td>Azure ATP</td>
<td>Nov 4, 2019 06:41 AM</td>
</tr>
<tr>
<td>Suspicious additions to sensitive groups</td>
<td>Medium</td>
<td>Active</td>
<td>2 reasons</td>
<td>Persistence</td>
<td>EU-Primary-Dc Jonathan Wolcott</td>
<td>Azure ATP</td>
<td>Nov 4, 2019 06:45 AM</td>
</tr>
<tr>
<td>Email message containing malware removed after…</td>
<td>Informal</td>
<td>Active</td>
<td>2 reasons</td>
<td>Initial access</td>
<td><a href="mailto:mike.barden@contoso.com">mike.barden@contoso.com</a></td>
<td>Office 365 ATP</td>
<td>Nov 4, 2019 06:53 AM</td>
</tr>
</tbody>
</table>
### Incident queue > Credential theft phishing campaign

<table>
<thead>
<tr>
<th>ID</th>
<th>Status</th>
<th>Detection source</th>
<th>Impacted entities</th>
<th>Start date</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>27956c</td>
<td>Remediated</td>
<td>MDAATP</td>
<td>cont-mikebarden</td>
<td>Nov 4, 2019 10:32 AM</td>
<td>5 min</td>
</tr>
<tr>
<td>27281</td>
<td>Remediating</td>
<td>Avere ATP</td>
<td>cont-mikebarden</td>
<td>Nov 4, 2019 00:33 AM</td>
<td>3 min</td>
</tr>
<tr>
<td>27956c</td>
<td>Remediated</td>
<td>Office 365 ATP</td>
<td>2 inboxes</td>
<td>Nov 4, 2019 01:33 AM</td>
<td>5 min</td>
</tr>
<tr>
<td>40</td>
<td>Remediated</td>
<td>RDR</td>
<td>cont-mikebarden</td>
<td>Nov 4, 2019 01:32 AM</td>
<td>5 min</td>
</tr>
<tr>
<td>191e</td>
<td>Remediated</td>
<td>Office 365 ATP</td>
<td><a href="mailto:mike.barden@contoso.com">mike.barden@contoso.com</a></td>
<td>Nov 5, 2019 07:31 AM</td>
<td>5 min</td>
</tr>
</tbody>
</table>
Credential theft phishing camp... 🙇 Security principal reconnaissance (LDAP)

Security principal reconnaissance (LDAP)
Investigation #27221 is Pending analyst approval

Investigation details
Status
Pending approval
Immediate actions require review and approval
Alert severity
Medium
Category
Discovery
Detection source
Azure ATP

Investigation graph
Alerts (2)  Devices (1)  Users (7)  Key findings (2)  Entities (25)  Pending actions (2)  Log (48)

- Devices (5)
  - cont-mukabezden

- Entities analysed (2497)
  - 7 User activities
  - 2 Malicious
  - 184 Users
  - 288 Services
  - 396 Drivers
  - 3 IP Addresses

- Threats found (1)
  - 2 Threats found

- User (7)

- Pending approval (2)
  - Mark user as compromised
  - Waiting for action approval (3ms)
Entities analyzed (2.5K)

- 7 User activities
  - 2 Malicious
- 1692 Files
- 134 Processes
- 265 Services
- 396 Drivers
- 3 IP Addresses
Credential theft phishing camp... Security principal reconnaissance (LDAP)

Security principal reconnaissance (LDAP)
Investigation #27261 is Pending analyst approval

Investigation details

<table>
<thead>
<tr>
<th>Status</th>
<th>Alert severity</th>
<th>Category</th>
<th>Detection source</th>
<th>Azure ATP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Verdict</th>
<th>User</th>
<th>Name</th>
<th>AAD ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious</td>
<td><a href="mailto:johnathan.wolcott@contoso.com">johnathan.wolcott@contoso.com</a></td>
<td>Jonathan Wolcott</td>
<td>efb4b7ec-b297-99de-4d4b-2b938e438b734</td>
</tr>
<tr>
<td>Malicious</td>
<td><a href="mailto:mike.barden@contoso.com">mike.barden@contoso.com</a></td>
<td>Mike Barden</td>
<td>2f4b979c-d2f4-464b-8d97-3d9b38e438b734</td>
</tr>
<tr>
<td>Clean</td>
<td><a href="mailto:tracie.huber@contoso.com">tracie.huber@contoso.com</a></td>
<td>Tracie Huber</td>
<td>lj7mb94-b297-2b938e4386867</td>
</tr>
<tr>
<td>Clean</td>
<td><a href="mailto:Jacob.gall@contoso.com">Jacob.gall@contoso.com</a></td>
<td>Jacob Gall</td>
<td>mdkhyrne-b297-2b938e438b734</td>
</tr>
<tr>
<td>Clean</td>
<td><a href="mailto:hailey.stevens@contoso.com">hailey.stevens@contoso.com</a></td>
<td>Hailey Stevens</td>
<td>efb4b7ec-b297-99de-4d4b-2b938e438b734</td>
</tr>
<tr>
<td>Clean</td>
<td><a href="mailto:casandra.hersley@contoso.com">casandra.hersley@contoso.com</a></td>
<td>Casandra Hersley</td>
<td>efb4b7ec-b297-99de-4d4b-2b938e438b734</td>
</tr>
<tr>
<td>Clean</td>
<td><a href="mailto:sadieb@contoso.com">sadieb@contoso.com</a></td>
<td>Sadie Bentley</td>
<td>efb4b7ec-b297-99de-4d4b-2b938e438b734</td>
</tr>
</tbody>
</table>
## Security principal reconnaissance (LDAP)

Investigation #27261 is Pending analyst approval

### Investigation details

<table>
<thead>
<tr>
<th>Investigation graph</th>
<th>Alerts (2)</th>
<th>Devices (1)</th>
<th>Users (7)</th>
<th>Key findings (2)</th>
<th>Entities (25)</th>
<th>Pending actions (2)</th>
<th>Log (48)</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Malicious</td>
<td><a href="mailto:jonathan.wolcott@contoso.com">jonathan.wolcott@contoso.com</a></td>
<td>Jonathan Wolcott</td>
<td>efb8b9cf-b297-5bf6-f44b-b297-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Malicious</td>
<td><a href="mailto:mike.barden@contoso.com">mike.barden@contoso.com</a></td>
<td>Mike Barden</td>
<td>hy8b9cf-5bf6-f44b-b297-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Clean</td>
<td><a href="mailto:tracie.huber@contoso.com">tracie.huber@contoso.com</a></td>
<td>Tracie Huber</td>
<td>jk7mb6-f5bf-4b6f-b297-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Clean</td>
<td><a href="mailto:Jacob.gall@contoso.com">Jacob.gall@contoso.com</a></td>
<td>Jacob Gall</td>
<td>mksdyf-5bf6-f44b-b297-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Clean</td>
<td><a href="mailto:haley.stevens@contoso.com">haley.stevens@contoso.com</a></td>
<td>Haley Stevens</td>
<td>kfb8c8f-5bf6-f44b-b297-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Clean</td>
<td><a href="mailto:casandra@contoso.com">casandra@contoso.com</a></td>
<td>Cassandra Hersley</td>
<td>efb8b9cf-5bf6-f44b-b297-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Clean</td>
<td><a href="mailto:sadieb@contoso.com">sadieb@contoso.com</a></td>
<td>Sadie Bentley</td>
<td>efb8b9cf-5bf6-f44b-b297-2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### User details

- **Verdict**: Compromised
- **Name**: Jonathan Wolcott
- **AAD ID**: efb8b9cf-b297-5bf6-f44b-b297-2
- **User name**: Jonathan Wolcott
- **SID**: S-1-5-2198076486876530875-1

[Open user page] [Mark user as compromised]
Azure Sentinel collects security data at cloud scale from all sources across your enterprise.

- **Pre-wired integration** with Microsoft solutions
- **Connectors** for many partner solutions
- **Standard log format** support for all sources

Proven log platform with more than 10 petabytes of daily ingestion.
Detect threats and analyze security data quickly with AI via *Azure Sentinel*

ML models based on **decades of Microsoft security experience and learnings**

Millions of signals filtered to few **correlated and prioritized incidents**

Insights based on vast **Microsoft threat intelligence** and your own TI

Reduce alert fatigue by up to 90% through ML
Converging Tools & Data
Engineering a single seamless system with automation, extending Zero Trust

- Single Portal Experience
- Playbook Automation
  Ensure Automation runs across all systems
- Semantics and Meaning
  Correlation, prioritization, orchestration, etc.
- Unified entity definitions
  Reputation for Users, machines, email, IPs, etc.
- Signal sharing
- Intelligent Capabilities
  High Quality Detection and Data
Converging Tools & Data
Engineering a single seamless system with automation, extending Zero Trust

- **Single Portal Experience**
- **Playbook Automation**
  
  *Ensure Automation runs across all systems*
- **Semantics and Meaning**
  
  *Correlation, prioritization, orchestration, etc.*
- **Unified entity definitions**
  
  *Reputation for Users, machines, email, IPs, etc.*
- **Signal sharing**
- **Intelligent Capabilities**
  
  *High Quality Detection and Data*

---

**Microsoft Threat Protection (MPT) Suite**

*Incidents, investigations, threat hunting, threat analytics*

- **Protect**
- **Investigate**
- **Remediate**

---

**Roadmap**

**Bring your own Threat Intel!**

---

**Including non-MSFT sources (Linux, syslog, AWS, Firewall, DNS, etc.)**
How it works (with **MSP/Partner opportunities**)

<table>
<thead>
<tr>
<th>Collect</th>
<th>Integrate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>now. ServiceNow</td>
</tr>
<tr>
<td>Apps, users, infrastructure</td>
<td>Other tools</td>
</tr>
<tr>
<td>Public Clouds</td>
<td>Community</td>
</tr>
</tbody>
</table>

### Visibility
- Dashboard

### Analyze & Detect
- Machine learning, UEBA

### Investigate & Hunt
- Pre-defined Queries, Azure Notebook

### Automate & Orchestrate Response
- Playbooks

### Enrichment
- Data Ingestion
- Data Repository
- Data Search

**Azure Monitor**
Investigate threats with AI and hunt suspicious activities at scale

Get prioritized alerts and automated expert guidance

Visualize the entire attack and its impact

Hunt for suspicious activities using pre-built queries and Azure Notebooks

Easily consume 3rd party, Non-MSFT data, normalize the data and further enrich your investigations

Democratize the SOC analyst
Ok great, how do we do this...

DoD has complex tiered, hierarchical and distributed structure

Assets can move (deployed), align to different commands/sub-commands at various times, etc.

This requires above/beyond management capabilities. Ideally centralized, across clouds and inclusive of on-premises and existing datacenters
Management in a complex and Tiered environment

- **Management Groups**
  - *Cross*-Subscriptions in same Tenant (centralized policy)

- **Azure Lighthouse**
  - *Cross*-Tenancy (Managed Solution Provider; MSP)

- **Azure Arc**
  - **Multi-cloud, hybrid**: IaaS, Containers (includes physical on-premises systems!), extend Azure Policy and RBAC (DevOps, SecOps models, etc.) to you.

Complemented via **Microsoft Cloud App Security (MCAS)** which provides PaaS and SaaS defense capabilities. In addition, *any solution YOU bring to the table will benefit from these centralized management capabilities*.
Management Groups

- **Root Management Group (Group of Subscriptions)** – Enterprise-wide Policies, Permissions, & Tags

  - **Core Services**
    - Shared Services (Edge Security)
  - **Additional Segment(s) / Subscriptions**
    - Development Stage Segments
      - Segment 3
      - Segment 4
      - Segment 5

- **Enterprise Tenant 2**

- **Intra-Tenant**

- **Azure Enrollment**
- **Identity**
- **Management Groups**
- **Segmentation Strategy**

- **Subscriptions**
  - Resource Groups & Resources
  - Virtual Networks
Without Azure Lighthouse, MSPs need to access every customer’s Tenant, individually.

MSP can perform CRUD (Create, Read, Update, Delete) operations at scope.
Azure Lighthouse

- **Azure Enrollment**
  - **Identity**
  - **Management Groups**
  - **Segmentation Strategy**
    - Subscriptions
    - Resource Groups & Resources
    - Virtual Networks

- **Enterprise Tenant**
  - **Identity**
  - **Management Groups**
  - **Segmentation Strategy**
    - Subscriptions
    - Resource Groups & Resources
    - Virtual Networks

- **Root Management Group (Group of Subscriptions)**
  - Enterprise-wide Policies, Permissions, & Tags

---

**Tenant 2 explicitly declares, for this scope, delegates privileges to...**

---

**Inter-Tenant**
With Azure Lighthouse

The secret sauce to Azure delegated resource management lies in being able to project customer resources into the partners environment

Customer resources projected into MSP tenant to be managed by authorized MSP users

MSP can perform CRUD (Create, Read, Update, Delete) operations at scope

- MSP tenant
- MSP directory
- MSP user group

Customer directory

Customer-1 Subscription
- Customer resources

Customer-2 Subscription
- Customer resources

Customer-3 Resource group
- Customer resources

Customer-4 Resource group
- Customer resources
Azure Delegated Resource Management creates logical (control plane) access to customer’s environment for the service provider.

1. MSP initiates an action for customer resource.
2. ARM validates the request is from a partner tenant and calls Managed Service Resource Provider (RP).
3. Managed service RP provides MSPs precise RBAC access.
4. MSP completes the action on customer resource.

Control plane:
- Tags
- RBAC
- ARM Templates
- Locks
- Policy
- Activity Log

Managed Services RP:
- AAD

Existing 200+ Azure services:
- Storage
- Compute
- Networking
- PaaS services

Access methods:
- CLI
- PowerShell
- HTTP request
- Azure Portal
Azure Arc

Overview
A large financial institution has sprawling server-based IT systems deployed in corporate datacenters, hosts and cloud. In addition, new DevOps practices result in an unknown number of servers that are connected to the corporate networks but are running outside of identity and governance systems. The sprawl is overwhelming, and it is impossible to apply consistent governance across the environment and meet compliance needs.

Business requirements
• Manage a mix of bare metal, Windows and Linux servers
• Visibility across locations, OS flavors and disparate systems
• Enable IT to apply at scale governance and security policies across all servers
• Enable application owners to apply and audit to meet their own requirements
• Measure and remediate compliance at scale and down to the individual workload/server
Govern your environment, across clouds, including on-premises:

- Asset organization and inventory with a **unified view** in the Azure Portal
- **Universal** governance anywhere through **Azure Policy**
- Built-in server compliance rules
- **Central compliance** view across all servers
- Server owners can view and remediate to meet their compliance
- **MSPs** can implement governance for their customer’s environment
Bringing it all together
Microsoft Intelligent Security Association (MISA)

Enrich your security products
Leverage Microsoft security products to extend solution capabilities and share threat intelligence.

Execute your go-to-market strategy
Members enjoy a broad range of co-marketing opportunities like speaking engagements, product roadmap updates, and special events.

Connect with customers
Help customers find, try, and buy security solutions that work with their digital environments.

Make integration easier
Get additional access to product teams to speed up integration and better differentiate your solution.

Already in our Customer Experience and Partners Channel?
https://aka.ms/CxeGovPartners

- Services partner ecosystem development
- Product partner ecosystem identified

Contact Dave:
DoD Cybersecurity Services contact
David Phillips, davidphi@microsoft.com
Thank you!
SOSSEC Membership is Required for Award on PEO EIS, DCO
Cyberspace Operations Broad Responsive Agreement (COBRA)
Other Transaction Agreement (OTA)

Benefits of Joining the SOSSEC Consortium

✓ Opportunity to perform work under seven (7) OTAs for the Air Force, Army and National Geospatial-Intelligence Agency
✓ Opportunity to build members’ business base by applying their technologies/expertise to meeting urgent DoD requirements
✓ Simple, streamlined process to compete for DoD work
✓ Average 60 days from requirements definition to award
✓ Flexible treatment of intellectual property
✓ OTA access to any DoD user with approval of OTA customer

Go to [www.sossecinc.com](http://www.sossecinc.com) and click on the JOIN NOW Tab to access the membership application. The process is simple and rapid. There is no joining fee, and the membership fee is $500 per year. Membership is open to Industry (traditional, nontraditional, small business), not for profit and academic institutions that share the values of the SOSSEC Consortium.

Questions about SOSSEC COBRA OTA contact: eaguirre@sossecinc.com