# CES
# Security Operations Center

**801-422-7788**

**cessoc@byu.edu**

# CES
# Security Operations Center

**BYU-OIT slack instance**

**#comm-cessoc  (public channel)**

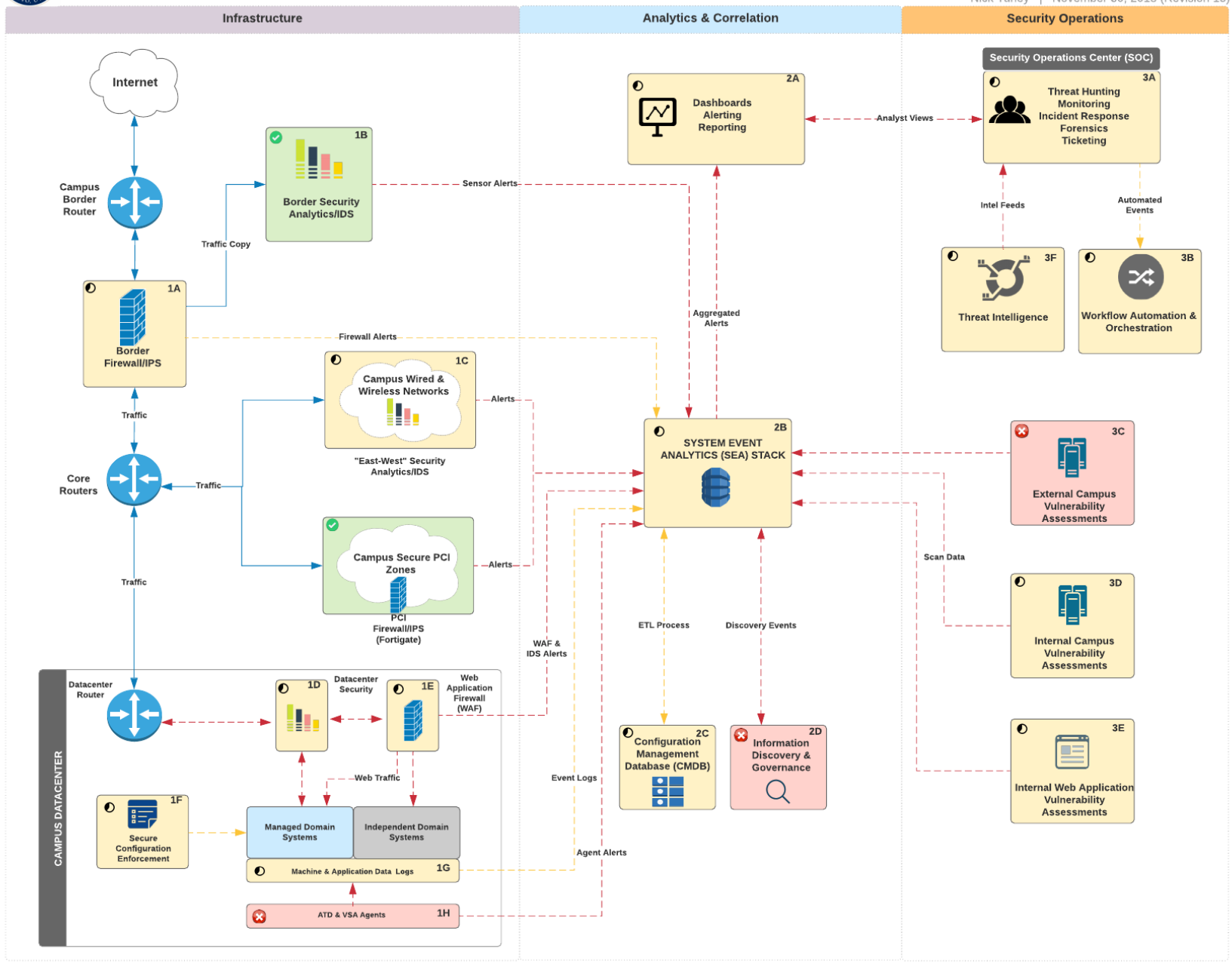
**#cessoc-csr  (private channel)**

# CES Security Operations Center

- SOC director
  - John Payne
- 4 FT analysts
  - Sam Moses
  - Mike Watson
  - 2 soon to be opened slots
    - Jerry Sell & TJay Humphries are retiring
- 6 Student analysts
- SOC architect
  - Nick Turley
- 3 FT engineers
  - John Clawson
  - Dallin Warne
  - Logan Miller
- 4 student engineers

# BYU CAMPUS SECURITY ECOSYSTEM

Nick Turley | November 30, 2018 (Revision 15)




Fully Implmented
Partially Implemented/Need Enhancement
Not Implemented/Need Visibility
Data Stream Not Implemented
Data Stream Partially Implemented

ATD = Advanced Threat Detection
ETL = Extract, Transform, Load
IDS = Intrusion Detection System
IPS = Intrusion Prevention System
VRF = Virtual Routing and Forwarding
VSA = Vulnerability Scan Agents
WAF = Web Application Firewall

**1A - Enhancements:**
- Update firewall rules to restrict dangerous protocols/services
- Block common application level attacks
- Improve SEA stack alerting with WildFire and custom alerts
- Extend IPS rules to block additional attacks

**1B - Implemented:**
- Border IDS that provides incident response/ticketing workflow, deep packet inspection and kill chain analytics
- Correlates with internal campus IDS sensors providing network "end-to-end" security view

**1C - Need implementation/Visibility:**
- Deploy sensors across campus locations for "east-west" monitoring

**1D - Need Implementation/Visibility:**
- Deploy sensor for ingress/egress traffic monitoring of the datacenter with Deep Packet inspection, kill chain analysis and campus IDS correlation
- Ideally, solution is next generation firewall with IPS. Alternate solution is to deploy IDS sensor

**1E - Partially Implemented:**
- Deploy WAF to monitor and block specific attacks against web applications (e.g. SQL injection, Cross-site scripting)
- Provides detailed visibility of web traffic and forensics (especially for encrypted HTTPS, not blocked by border Palo Alto)

**1F - Need Implementation/Visibility:**
- Deploy configuration management and enforcement system providing technical application and maintenance of security policy on systems, applications and network devices

**1G - Need Implementation/Visibility:**
- Deploy agents to collect machine and application log data for ingestion into the SEA stack for analytics (e.g. PeopleSoft application logs)

**1H - Need Implementation/Visibility:**
- Deploy Advanced Threat Detection agents to augment anti-virus agents and improve end-point threat visibility
- Deploy local vulnerability scanning agents to improve end-point vulnerability detection

**2A - Need Implementation/Visibility:**
- Build situational awareness dashboards and real-time alerting/reporting framework using aggregated events from SEA

**2B - Partially Implemented:**
-Managed Domain systems are currently sending logs to SEA. Logging profiles need enhancement.
- Add additional security data streams (e.g. vulnerability scans, Sophos, IDS/IPS, application logs, host firewalls)
- Integrate with CMDB (e.g. inventory, data classifications, locations, CSR contacts)

**2C - Partially Implemented:**
- Need asset inventory and asset metadata
- Need asset data classifications and risk levels
- Security ETL of inventory/data classifications for reporting and incident response prioritization

**2D - Need Implementation/Visibility:**
- Implement data discovery and data management solution for identifying and reporting on sensitive or protected sources of data on campus

**3A - Need Implementation:**
- Establish Security Operations Center (SOC) for coordinated incident response, 24/7 monitoring and security workflow orchestration

**3B - Need Implementation:**
- Framework handles security workflow automation by integrating with infrastructure systems to conduct various operations and reduce response times for security analysts

**3C - Need Implementation/Visibility:**
- Establish external vulnerability scanners to test BYU's external defenses and security posture
- Integrate with SEA stack to provide real-time reporting of external security posture

**3D - Enhancements:**
- Implement full authenticated scans for OIT assets
- Implement policy compliance' scans for OIT assets
- Implement web application scans
- Implement targeted unting scans
- Integrate with SEA stack to provide real-time reporting of system security postures

**3E - Partially Implemented:**
- Deploy new vulnerability assessment tools that specifically focus on web application assessments and penetration testing

# CES Security Operations Center – Services Catalog

## Available
2018/2019

- ❑ Incident Management
- ❑ Security Event Monitoring & Management
- ❑ Security Assessment & Consultation
- ❑ Network Security Monitoring/IDS
- ❑ Firewall/IPS (Palo Alto)
- ❑ Basic Vulnerability Management

## In Development
2019/2020

- ❑ Advanced Vulnerability Management
- ❑ Threat & Federated Intelligence
- ❑ Cloud Security (PaaS/IaaS)
- ❑ Metrics & Reporting

## Pending
2021+

- ❑ Data Security
- ❑ System Security
- ❑ Security Awareness & Training

**What can we see?**

**What do we do with the information we gather?**

# Border Traffic Protections

**Using the Palo Alto firewall**

# Palo Alto

- **Virus and other malicious traffic patterns**

# Palo Alto

- Virus and other malicious traffic patterns
- **How do sites get blocked?**

# Palo Alto

- **Virus and other malicious traffic patterns**
- **How do sites get blocked?**
  - https://it.byu.edu/byu/form.do?form=ef61f2cb0a0a3c0e500eb07ce67dca7c

    aka
  - **https://go.byu.edu/unblock**

# Palo Alto

- Virus and other malicious traffic patterns
- How do sites get blocked?
  - https://it.byu.edu/byu/form.do?form=ef61f2cb0a0a3c0e500eb07ce67dca7c
- Other Palo Alto Protections
  - RDP
  - Patterns of attack

# East/West Campus traffic

**Bro (Zeek) & Corelight**

# East/West Campus traffic

- **We can currently see ~70% of the traffic flow between subnets on campus**
  - **Most of the focus is on plaintext and traffic patterns**
  - **We struggle to understand some encrypted traffic**

# East/West Campus traffic

- We can currently see ~70% of the traffic flow between subnets on campus
  - Most of the focus is on plaintext and traffic patterns
  - We struggle to understand some encrypted traffic
- **We currently maintain 30 days of traffic metadata, which helps us understand when problems started, if we catch them fast enough**

# East/West Campus traffic

**SOC Dashboards**

# Penetration Tests

# Vulnerability Management

**Qualys**

# Let’s talk about Qualys

# Security special interest group (SIG) meetings

# Security SIG
# Vulnerability Management

**July 9th**

**2pm**

**ITB 1010 suite**

# Phishing and other email issues

# Latest phishing campaign
# May 14 – May 22

- 28 impersonations
- 606 emails sent to 402 recipients
- 91 people replied to the email, some had a number of replies
- 4 confirmed victims ($500 each)

# Minimizing the impact of  phishing and other malicious email

- The sooner we get a report and validate it as non-legitimate, the sooner we can block the fake email account, links in an email, etc.
  - There is also the option of doing a search & destroy for the email in Exchange, that work is time intensive right now
  - We don’t have the ability to do anything if the email is forwarded off campus and/or opened remotely

# Minimizing the impact of  phishing and other malicious email

- The sooner we get a report and validate it as non-legitimate, the sooner we can block the fake email account, links in an email, etc.
  - There is also the option of doing a search & destroy for the email in Exchange, that work is time intensive right now
  - We don’t have the ability to do anything if the email is forwarded off campus and/or opened remotely

**abuse@byu.edu**

# Minimizing the impact of  phishing and other malicious email

- The sooner we get a report and validate it as non-legitimate, the sooner we can block the fake email account, links in an email, etc.
  - There is also the option of doing a search & destroy for the email in Exchange, that work is time intensive right now
  - We don’t have the ability to do anything if the email is forwarded off campus and/or opened remotely

**abuse@byu.edu**

**phishing@byu.edu**

**phishtank@byu.edu**

**spam@byu.edu**

# Upcoming capabilities

# Upcoming capabilities

- Advanced Vulnerability Management
- Threat & Federated intelligence
- Cloud security visibility & tools
- Security Awareness & Training

# Capabilities that are a bit further out

- Data security
- Endpoint protection

# What can CSRs do to help?

# CSRs and the SOC

- CMS hygiene, WebApps, Admin consoles

# CSRs and the SOC

- CMS hygiene, WebApps, Admin consoles
- Understand where data resides in your environment
  - Clean out of sensitive data types that you don’t want, need, or use

# CSRs and the SOC

- CMS hygiene, WebApps, Admin consoles
- Understand where data resides in your environment
  - Clean out of sensitive data types that you don’t want, need, or use
- If you see something, say something.

# CSRs and the SOC

- CMS hygiene, WebApps, Admin consoles
- Understand where data resides in your environment
  - Clean out of sensitive data types that you don’t want, need, or use
- If you see something, say something.
- Network scanning

# CSRs and the SOC

- CMS hygiene, WebApps, Admin consoles
- Understand where data resides in your environment
  - Clean out of sensitive data types that you don’t want, need, or use
- If you see something, say something.
- Network scanning
- Help us understand the landscape

# CSRs and the SOC

- CMS hygiene, WebApps, Admin consoles
- Understand where data resides in your environment
  - Clean out of sensitive data types that you don't want, need, or use
- If you see something, say something.
- Network scanning
- Help us understand the landscape
- If you have any concerns with how the SOC is communicating with you – skill, details provided, or anything else – please ask for me or reach out to me privately

# Security Metrics

# Security Metrics

- We really aren’t yet good at creating meaningful, useful metrics about the security incidents and cyber security work being done on this campus

# Security Metrics

- We really aren’t yet good at creating meaningful, useful metrics about the security incidents and cyber security work being done on this campus

- What KPIs and other metrics would be useful?

# Other InfoSec stuff

**IT Security Standards**

**Application Inventory updates**

# IT Security Standards

- https://infosec.byu.edu/node/158

# IT Security Standards

- https://infosec.byu.edu/node/158
- Minimum controls for systems with sensitive data types

# IT Security Standards

- https://infosec.byu.edu/node/158
- Minimum controls for systems with sensitive data types
- Todd Brown can be contacted if there are concerns or questions about the published standards

# IT Security Standards

- https://infosec.byu.edu/node/158
- Minimum controls for systems with sensitive data types
- Todd Brown can be contacted if there are concerns or questions about the published standards
- This is currently in a ‘soft release’, you should hear from your deans & directors soon, if you haven’t already, about the need to meet the standards by mid-2020

# Security SIG
# IT Security Standards

**September 24th**

**2:30pm**

**ITB 1010 suite**

# Application Inventory updates

- Ryan Bird will be sending your application inventory data to you looking for an update
- If there are no changes, just indicate that and return it.
- If there are changes, please make those minor modifications and we will process them

# CES
# Security Operations Center

**801-422-7788**

**cessoc@byu.edu**